Weekly Write-Up #1

In this day and age, DNA testing is not all that uncommon and is no longer something only used by researchers and forensic scientists. It’s actually fairly accessible to individuals thanks to the rise in popularity of genetic testing companies that sell home-testing DNA kits. When they send in a DNA testing kit, consumers understand that these companies are storing their data, in order to trace their lineage and provide ancestry information. This information is extremely personal and therefore expected to be kept private, between the consumer and company. Family Tree DNA, although protective of customers’ information when it comes to selling or trading it with third parties, is reportedly giving the federal government access to their databases for the purpose of solving crimes (Hernandez, 2019). They are allowing law enforcement to create accounts using collected DNA, to then have access to the same information that their paying customers can view.

Instead of just openly giving the FBI access to their databases, they are making agents use the front-end system by submitting the DNA they have (presumably from a crime scene). This ensures that the company’s privacy terms are technically not being breached, even though these agents are not paying customers, nor are they using the site as is intended for everyone else. However, when customers send in their kits, they’re not giving informed consent for their DNA to be used in such a way – they consent to their information being stored in a database and used for genetic testing, but unknowingly also contribute their information to be used in criminal investigations. This secondary use of their genetic information for crime solving – which does not align with the primary, originally-intended ancestral discovery use – raises the question about whether or not it was okay for Family Tree DNA to enter into such a partnership with the FBI.
On one hand, it may seem like an invasion of privacy to the paying customers that the FBI can just look through their ancestry and genetic tree. It can feel like a threat to your privacy because your information is essentially being released to a third-party without your authorization. It feels dishonest to me that because agents are accessing the data in the same way paying customers would, side-stepping privacy terms because such use technically is not considered to be third-party sharing. The news of this agreement between the company and the FBI is also not clearly conveyed to the customers, those whose information they already had were not even notified (Hernandez, 2019). People should be able to opt-out of the database the FBI is given access to, as opposed to the forced choice of either letting the government access your DNA or just removing your kit and losing the option to use the DNA matching option. On the other hand, this is a massive advancement in law enforcement, and is a powerful new use of DNA. This could help find new leads on cases gone cold long ago, and ultimately should not be detrimental to innocent relatives of the criminal whose DNA is put into Family Tree DNA’s databases. The company was careful to not give them any more access than the regular customer would have access to and that seems fair.

Personally it seems to me as though this agreement between Family Tree DNA and the FBI raises questions about the ethics behind this partnership that are not easily brushed off just because it may make solving certain crimes easier. People have a right to control how their information is being used, and in this context the customers who use or have used Family Tree’s services deserve better than the blurred picture they’re getting of what is happening to the information they submit.

References