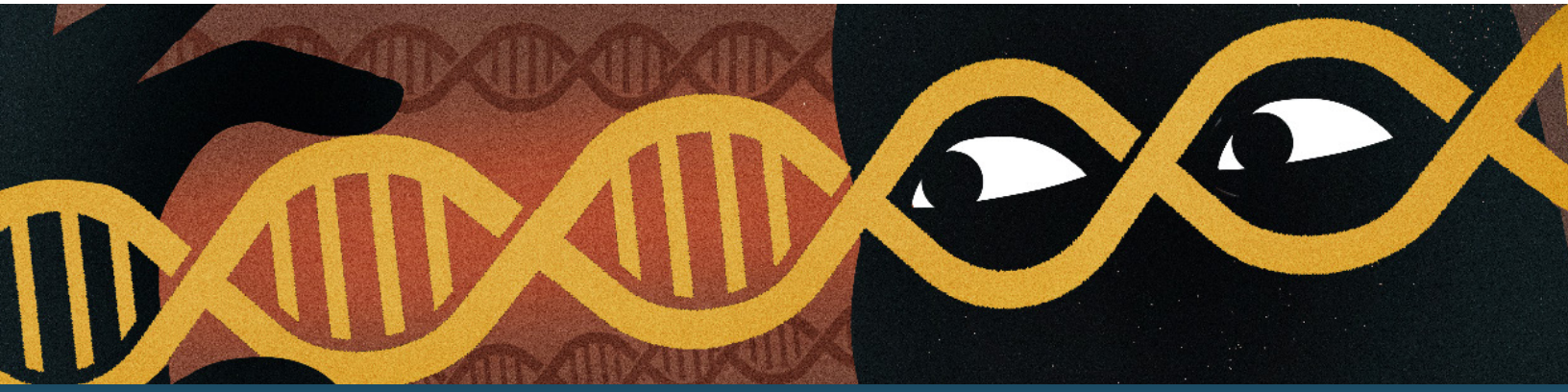
PUBLIC POLICY BRIEF

Protecting Your DNA From Government Fishing Expeditions

Authored by Michael Melendez
Director of Policy

LIBERTAS INSTITUTE



SUMMARY

Should police officers be able to conduct mass searches in privately owned or crowd-sourced DNA databases? At first glance, it might seem that this is a helpful new tool to identify suspects in pursuit of justice.

But unlike with a fingerprint or other biometric information, our DNA reveals our personal medical information, ethnic heritage, and connections to a family tree of relatives. Police officers using this data are not merely capable of matching DNA to a single individual; they are also able to uncover a person's family connections—a violation of the Fourth Amendment.

These massive databases are an understandable temptation for law enforcement officials who want to generate leads. Nonetheless, they should be restricted in being able to do so, just as the Utah Legislature has—in the name of privacy—limited law enforcement's use of drones, mobile tracking devices, license plate readers, body cameras, digital data snooping and other emerging technologies.

Innocent people should be protected against mass searches by law enforcement in DNA databases.

Melodic sounds filled a Centerville, Utah, chapel of The Church of Jesus Christ of Latter-day Saints late on November 17, 2018, as 71-year-old Margaret Orlando practiced the organ. She was suddenly interrupted with loud pounding on the chapel's locked door. About half an hour later, a person attacked her from behind and began choking her, forcing her to lose consciousness.[1]

Orlando did not see her attacker, and there was no video evidence to help reveal the person's identity. Detectives later found three drops of blood on a broken window sill. If law enforcement could match the blood's DNA to a suspect, that would help secure justice for Orlando. But they ran into a dead end with traditional DNA testing when the Utah State Crime Lab did not find a match in the FBI's national DNA database.

They did not have any leads. What, then, were detectives to do?

As it turns out, the attack and investigation happened right at a pivotal moment in DNA technology. As millions of Americans send their saliva to genetic testing companies in return for information about their family heritage and health, it becomes that much easier for anyone to use that information to find relatives through their shared DNA.

These databases have become a target-rich environment for law enforcement agencies and the companies that assist them in trying to generate leads using DNA samples of unknown individuals. Known as genetic genealogy, the process involves providing a data file of a person's DNA to explore how that DNA might match against potential relatives in these large databases. Once connections are made, law enforcement can back-trace their way to a suspect by investigating the person's family tree.

Unsurprisingly, law enforcement is elated with this new technological breakthrough and the opportunity to perform mass searching in private and public databases to find leads. Many initially find the possibilities of these searches exciting—after all, who does not want justice for Orlando and others like her?

But as important as it is to secure justice by identifying perpetrators, the use of these databases profoundly violates individual privacy and constitutes a warrantless search that lacks individual suspicion. It is, therefore, a violation of the Fourth Amendment. The good that might come from access to these genetic databases cannot outweigh the harms it involves; law enforcement should not be able to perform mass searches in databases with such sensitive information.

Biometric Databases

Information about each of us resides in a large number of databases, both private and public. Our e-commerce orders, grocery store rewards program purchases, Netflix viewing history, emails, texts, and phone call logs are all stored in private databases maintained by the companies we interact with. The government also has a number of databases to track births, welfare, driver licenses, pharmaceutical prescriptions, and so much more. Those subjected to the criminal justice system have had their mugshots, physical details, and biometric information, such as fingerprints and DNA, logged by the government.

Mass searching of genetic databases is a profound privacy violation and lacks particularized suspicion as required by the Fourth Amendment.

Supplying our data to many of these databases is a trade-off—a choice made by individuals who decide to share data about themselves in exchange for a product or service. And while in some cases the database entries are mandatory, as in the case of a criminal record, these are still a consequence of a person's own behavior.

Unlike a person's shopping history, phone calls, and other behavioral information stored in databases, biometric information uniquely identifies a specific person. Things like fingerprints, retinal scans, and especially our DNA, are private information that should be protected from government access.

A person's biometric data can obviously be useful for identification. Imagine a crime scene where a fingerprint is found; law enforcement will obtain and preserve this evidence so that they can match it against the suspect to determine if he or she was present at the scene of the crime. This process is well known and constitutionally sound, as a fingerprint merely confirms a person's identity but reveals nothing more about the person, let alone other people.

Storing information like this in a database, under limitations and with due process, is justifiable when

necessary. But DNA adds a whole new twist to this warehousing of data; as this brief will later explain, DNA is unlike other biometric data in that it reveals information about—and therefore exposes—other people as well. Government access to DNA databases presents a significant privacy problem.

Searches and Warrants

Personal privacy is a fundamental right that is guaranteed by the Fourth Amendment. As that clause of the Constitution states, the government may encroach upon this privacy once a warrant has been obtained, based upon probable cause that "particularly describe[s] the place to be searched, and the persons or things to be seized."[2] What this means, in plain language, is that a law enforcement officer must have strong reasons to suspect a person for violating the law before the officer can violate that person's privacy in an effort to find evidence of the crime.

What is especially relevant in the context of biometrics, especially DNA, is the "particularity" requirement, born of the colonists' rejection of broad warrants that allowed British authorities to engage in "general, exploratory rummaging in a person's belongings."[3] Thus, with particularity, a warrant to search a residence must be specific to a single living unit, rather than an entire apartment complex full of other innocent people, or a whole neighborhood. This requirement ensures "that the scope of every governmental intrusion is limited only to that for which there is probable cause."[4] Mass searching is therefore constitutionally problematic.

Of course, law enforcement would solve many more cases in a surveillance society, but the American tradition has squarely rejected that trade-off. Making it easier to catch suspects at the expense of individual privacy is not a valid objective.

Orlando was attacked at this chapel in Centerville, Utah.

Databases full of information—either maintained by the government, or accessible to it—present a complication by centralizing the access to information and making it easy to identify and surveil individuals. In the context of DNA databases, one judge noted:

> *In our age in which databases can be mined in a millisecond using super-fast computers, in which extensive information can, or potentially could, be gleaned from DNA… and in which this data can easily be stored and shared by governments and private parties worldwide, the threat of a loss of privacy is real…*[5]

This emergent concern about the combination of conveniences afforded to the government by warehousing our biometric data and the very revealing nature of one's DNA has led another judge to poignantly state that government searching through DNA

> *represents an alarming trend whereby the privacy and dignity of our citizens [are] being whittled away by imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of man's life at will.*[6]

The typical response to privacy concerns such as these would be to require a warrant, but as this brief will later explore, that requirement is not sufficient to allow mass searching in genetic databases.

Genetic Databases and Consent

Today's society, "quite unlike any we have seen," is changing in large part due to technology. Both private companies and public organizations are crowd-sourcing large databases of individuals' genetic information. Cumulatively, these databases could be used to make most everyone identifiable. A 2018 study published in *Science* revealed that a full 90% of Americans with European ancestry will be identifiable from their DNA by the end of 2020—even if they never provided their DNA to anyone.[7] Eventually—and rather soon—*everyone* will be identifiable.

Should the companies and organizations who maintain these databases be required to allow law enforcement to conduct a search of people's familial connections to find an unknown individual (or their relatives) within their DNA database? Because a fishing expedition of this nature is obviously not based on particularized suspicion, this approach violates a person's constitutional privacy protections.

Does consent change this scenario? Should not law enforcement be able to access a database of genetic information—whether public or private—if the people who contributed their DNA profiles consented to their use by the government? After all, a person waives their right to privacy if they voluntarily share private information; a secret document posted online for anyone to access, for example, cannot be hidden from government view.

This question shines a light on how the traditional model of consent is upended by the very nature of DNA. Consider this: a company requests your retinal scan to gain access to its facility. You read the agreement, give your consent, and now the company has your retinal scan. This decision implicates only you, because your retinal scan is unique to you.

DNA works differently. Imagine that a certain person is very privacy conscious and does not want to provide his revealing genetic information to anyone for any purpose. But his mother is a curious person who loves doing family history research, so she provides her saliva to Ancestry or 23andMe, and uploads her resulting genetic information to a database to find relatives. She just exposed her son against his wishes. He had no say in the matter. Because of today's DNA technology, he is now, in effect, in the database.

In response to privacy concerns, some companies and organizations have stated that law enforcement can only gain access to data for which the DNA owner has given consent. But those who consent to this genetic probe by the government are also explicitly exposing their siblings, parents, cousins, relatives they have never met, and even future generations of their family. Giving the government information about a person's entire family tree does not fit within a traditional consent framework; while a person can consent to waive their own privacy, their so-called "consent" cannot be construed to also waive the privacy interests of hundreds of relatives.

Industry Response

Several of the large DNA testing companies understand the sensitive nature of the data they are processing. Ancestry and 23andMe, two of the larger companies, are part of a coalition to protect DNA privacy.[8]

One coalition member was later removed for its violation of the standards. FamilyTreeDNA agreed to provide the FBI with warrantless access to its DNA database of 1.5 million people, marking "the first time a prominent private company has agreed to voluntarily provide law enforcement with routine access to customers' data." The agreement "is out of step with consumer expectations," the coalition added, noting that "when users send in their DNA to learn more about their health or heritage, they do not expect their genetic data to become part of an FBI genetic lineup."[9]

Even more concerning is GEDmatch, a website where consumers can upload their DNA profiles that were generated by a genetic testing company to compare with other profiles to find relatives. The public database now contains over a million records,[10] offering law enforcement a tempting opportunity to do mass searching to identify possible suspects (and their relatives).

This is precisely how the attacker in Centerville was discovered; the blood sample was processed into a DNA profile and uploaded to GEDmatch, in violation of the company's terms of conditions and without notice to consumers, after a detective from Utah persuaded the company's owner.[11] The search revealed a distant relative of the suspect. Investigators learned that someone related to the person in GEDmatch lived in Centerville: a 17-year-old high school student. A police officer at the school watched the young man during lunch and later collected the juice box he threw away in the garbage. DNA extracted from the saliva on the straw was a match for the blood from the crime scene evidence.

In reaction to public scrutiny from cases such as this, GEDmatch changed their policy in May 2019 to only allow law enforcement to use a portion of the database where users have consented to their genetic information being searched by law enforcement—a positive step, though still a problematic one since consent for DNA is not a valid basis to expose innocent relatives.

Mass Searches of Genetic Databases

The law enforcement community is excited about this new technological tool. As one officer explained, "'most of the work we do is pretty boring,' but when coupling genetic

genealogy with the mass searches of a genetic database, 'it did feel pretty exciting, new and cutting edge.'"[12] The prospect of solving cold cases and finding unknown suspects is a hopeful one for those whose profession is judged based on holding criminals accountable.

And with over 15 million people so far surrendering their (and portions of their relatives') DNA to genetic testing companies,[13] Jay Henry, director of Utah's crime lab, says that he is likewise "excited" by the ability to use these databases. "We might be on the cusp of a new revolution in forensic genealogy, the next big leap."[14]

But when presented with privacy concerns about the process, law enforcement individuals, and Henry specifically, have been dismissive. "If [genetic database companies are] being up front with people, I don't see how that really is an invasion of everybody's privacy," he said. "People are so willing to share their profiles… people are interested in helping solve crime—they're wanting to do it. That really gives me a good feeling."[15]

This perspective is shared by the US Department of Justice. In their guidelines for conducting mass searches of genetic databases, they tell federal officials to only do mass searching if the database owner has "provide[d] explicit notice to their service users and the public that law enforcement may use their service sites to investigate crimes."[16] Mere notice is construed to constitute consent—not just for those uploading their DNA, but for their entire family.

GEDmatch, for its part, has modified the notice they give to their users and has also allowed users to opt in to allowing government searches of their familial data. In response, some investigators have decided to pursue a warrant to try and access GEDmatch's entire list of users and all their data. In July 2019, a Florida judge authorized just such a warrant to do mass searching using their full database. The detective who obtained the warrant later announced to colleagues at an international police conference that he had obtained a warrant to "penetrate" the database and search over a million users.[17] The judicial request overrode the website's privacy settings and the wishes of its users in order to have unrestricted access to the data.

A person cannot consent on behalf of all their family members to share their private DNA with law enforcement to conduct mass searches.

What About a Warrant?

Obtaining a warrant does not work for mass searches of genetic databases, as there is no suspect. Instead, law enforcement is looking to generate leads and compel innocent people to surrender their DNA privacy to assist them.

With the recent Florida warrant, law enforcement hopes that it is the start of even bigger fishing expeditions. The detective who obtained the warrant hoped for eventual access to Ancestry and 23andMe's massive databases. "You would see hundreds and hundreds of unsolved crimes solved overnight," he said. "I hope I get a case where I get to try."[18]

The judge in this case was wrong to authorize a warrant; because there is no suspect, the particularity requirement of the Fourth Amendment cannot be satisfied. Instead, this tactic of using genetic databases inherently involves mass searching of innocent people who have not given their consent and indeed do not know the search is even taking place. It is akin to police hoping to identify a suspect by forcibly entering the homes of everyone in a certain city. Such a request would be preposterous for a warrant.

The Third Party Doctrine

Some proponents of mass searches of genetic databases have suggested that law enforcement access can be justified based on the so-called "third party doctrine," an exception to the Fourth Amendment created by the US Supreme Court suggesting that a person has a reduced expectation of privacy in information that has been provided to a third party.

But technology has radically altered the third party landscape; it is quite impossible to interact digitally at all—even directly with another person—without providing information to third party intermediaries. In part due to this change in recent decades, the US Supreme Court stepped in a new direction in the 2018 *Carpenter* case, showing a new trend likely to be expanded in the future.

In that case, the government's tracking of a person's location using

their cell phone—using third party data held by the phone provider—was deemed unconstitutional. The Court's observation that the previous case law did not properly protect individual rights in light of new technological developments is equally relevant with DNA, especially because, as with Carpenter's location data, people's DNA data is involuntarily exposed, without their knowledge and not necessarily with their consent.

We need not wait years—or decades—for case law to develop on mass searches of genetic databases; it is within the purview of the Legislature to restrict state officials from engaging in this practice. Indeed, this has been the case with the third party doctrine and the Utah Legislature. In early 2019, legislators unanimously supported House Bill 57, sponsored by Representative Craig Hall, which eliminated the third party doctrine exception for law enforcement and requires a warrant, with probable cause and particularity, for access to a person's digital data.[19]

What's the Harm?

In 2014, law enforcement officials in Idaho used Ancestry's database to try and solve a murder case from two decades before.[20] A strong match was found in the Usry family, suggesting that DNA taken from the crime scene belonged to a relative. The match honed in on Michael Usry, a New Orleans man who had contributed his DNA to a project sponsored in part by The Church of Jesus Christ of Latter-day Saints years earlier. The project collected over 100,000 DNA samples before the data was sold to Ancestry in 2007.[21]

Usry did not fit the age profile of the suspected attacker, so law

Michael Usry holds a photo of his son.

enforcement turned to his son, a filmmaker who they discovered had once spent time in Idaho and who had created a short film about murder. Six hours of interrogation later, the son was then held in suspense for over a month before later being cleared of the murder suspicion after his DNA was revealed to not be a match.

The risk of false positives, interrogations, and investigations that result from mass searching in DNA databases are just one form of harms caused by mass searches of genetic databases. A 2014 study revealed that just 17% of familial genetic searches "resulted in the identification of a relative of the true offender," suggesting substantial inaccuracy that broadly targets innocent people.[22]

Those accused falsely of committing heinous crimes often see their careers destroyed, marriages jeopardized, and reputations ruined simply by being publicly connected to an egregious crime.

People who contribute their DNA profiles consensually are harmed through mass searches of genetic databases by having their information searched for a purpose they did not intend or know about when sharing the data. Further, they are made a suspect merely because of a genetic connection to another person. Law enforcement inquiry into the DNA contributor may reveal private information that was intended to remain secret. Police may also scrutinize the past conduct of the contributor during their investigation that may reveal conduct not connected to the crime, but which may provide a prosecutor with leverage to coerce compliance against their relatives. This targeting—again due to their DNA and nothing more—may result in increased stress, lost time, and wasted money on legal fees.

Finally, reliance on DNA for generating leads may enable the prosecution of innocent people who were once present at the scene of the crime. Forensic labs can now identify people using DNA from a few of the roughly 400,000 skin cells the human body sloughs off per day.[23] Innocent people accused of egregious crimes, whether due to misplaced DNA[24] or exposure from their relatives' sharing of the family DNA in a database, may lack ironclad defenses, alibis, and financial resources to successfully fight the charges.

DNA can also exonerate innocent people; like any tool, there are both good and bad uses. But the new world of mass searches of genetic databases, though exciting for law enforcement, inherently violates privacy and undermines consent. While mass searching in genetic databases is tempting for police to exploit, it simply cannot square with the particularity requirement of the Fourth Amendment. We allow law enforcement to use mass searches of genetic databases at the peril of substantially undermining the most fundamental pillars of personal privacy and due process.

PROPOSAL: PROHIBIT MASS SEARCHES OF GENETIC DATABASES

DNA can be a tremendous tool for law enforcement investigations and prosecution of crime. When law enforcement has probable cause to believe that a person has committed a crime and their DNA is needed to confirm an existing DNA sample, law enforcement should have the ability to obtain and use it. Without particularized suspicision, however, this extremely private and revealing data should be out of the government's reach; mass searching of innocent people who have not given consent or notice should be disallowed.

Endnotes

1. Annie Knox, "Police: Intruder attacked organist, 71, in Centerville chapel late Saturday," *Deseret News*, November 18, 2018, accessed December 7, 2019, https://www.deseret.com/2018/11/18/20659142/police -intruder-attacked-organist-71-in-centerville-chapel-late-saturday.
2. U.S. Const. amend. IV.
3. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).
4. Martha Applebaum, "Wrong But Reasonable: The Fourth Amendment Particularity Requirement After United States v. Leon," 16 Fordham Urb. L.J. 577 (1987), 588
5. 379 F.3d 813. 842 (9th Cir. 2004).
6. Ibid, 851.
7. Heather Murphy, "Most White American's DNA Can Be Identified Through Genealogy Databases," *New York Times*, October 11, 2018, accessed December 7, 2019, https://www.nytimes.com/2018/10/11/science /science-genetic-genealogy-study.html.
8. FPF Staff, "Future of Privacy Forum and Leading Genetic Testing Companies Announce Best Practices to Protect Privacy of Consumer Genetic Data,' Future of Privacy Forum, July 31, 2018, accessed December 7, 2019, https://fpf.org/2018/07/31/future-of-privacy-forum-and-leading-genetic-testing-companies-announce- best-practices-to-protect-privacy-of-consumer-genetic-data/.
9. FPF Staff, "FamilyTreeDNA Agreement with FBI Creates Privacy Risks," Future of Privacy Forum, February 6, 2019, accessed December 7, 2019, https://fpf.org/2019/02/06/familytreedna-agreement-with-fbi- creates-privacy-risks/.
10. Peter Aldhous, "We Tried To Find 10 BuzzFeed Employees Just Like Cops Did For The Golden State Killer," Buzzfeed News, April 9, 2019, accessed December 7, 2019, https://www.buzzfeednews.com/article/peteraldhous/golden-statekiller-dna-experiment-genetic-genealogy.
11. Peter Aldhous, "The Arrest Of A Teen On An Assault Charge Has Sparked New Privacy Fears About DNA Sleuthing," BuzzFeed News, May 14, 2019, accessed December 7, 2019, https://www.buzzfeednews.com/ article/peteraldhous/genetic-genealogy-parabon-gedmatch-assault.
12. Megan Rowe, "Murder trial highlights growing use of genetic genealogy to solve cold cases." *Spokeseman-Review*, March 27, 2019, accessed December 7, 2019, https://www.spokesman.com/ stories/2019/mar/27/your-dna-could-crack-the-next-cold-case/.
13. Murphy, "Most White Americans' DNA Can be Identified Through Genealogy Databases."
14. Mark Shenefelt, "Open-souce DNA: an unprecedented crime buster or privacy nightmare?" *Standard-Examiner*, October 13, 2019, accessed December 7, 2019, https://www.standard.net/police-fire/ open-source-dna-an-unprecedented-crime-buster-or-privacy-nightmare/article_64b2e44a-6c63-51a5-99cf-8af66bd490dd.html.
15. Ibid.
16. "Interim Policy, Forensic Genetic Genealogical DNA Analysis and Searching," United States Department of Justice, accessed November 25, 2019, https://www.justice.gov/olp/page/file/1204386/download.
17. Kashmir Hill and Heather Murphy, "Your DNA Profile is Private? A Florida Judge Just Said Otherwise," *New York Times*, November 5, 2019, accessed December 7, 2019, https://www.nytimes.com/2019/11/05 /business/dna-database-search-warrant.html.
18. Ibid.
19. Molly Davis, "Utah Just Became a Leader in Digital Privacy," Wired, March 22, 2019. Accessed December 7, 2019. https://www.wired.com/story/utah-digital-privacy-legislation/.
20. Jennifer Lynch, "How Private DNA Data Led Idaho Cops on a Wild Goose Chase and Linked an Innocent Man to a 20-year-old Murder Case," EFF, May 1, 2015, accessed December 7, 2019, https://www.eff.org/ deeplinks/2015/05/how-private-dna-data-led-idaho-cops-wild-goose-chase-and-linked-innocent-man-20.
21. Associated Press and Jessica Chia, "Man became suspect in murder and rape case after DNA his father donated to Mormon genetic research was sold to Ancestry.com and then tested by police," *Daily Mail*, March 26, 2016, accessed December 7, 2019, https://www.dailymail.co.uk/news/article-3510568/Law- enforcement-investigators-seek-private-DNA-databases.html.
22. "Familial searching: A specialist forensic DNA profiling service utilising the National DNA Database® to identify unknown offenders via their relatives—The UK experience," *Forensic Science International: Genetics*, vol. 8, no. 1, January 2014, Pages 1-9.
23. Katie Worth, "Framed for Murder by His Own DNA," Wired, April 19, 2018, accessed December 7, 2019, https://www.wired.com/story/dna-transfer-framed-murder/.
24. Suzanna Ryan, "Touch DNA. What is it? Where is it? How much can be found? And, how can it impact my case?" Ryan Forensic, accessed December 7, 2019, http://ryanforensicdna.com/touchdna/.
25. Ibid.

PUBLIC POLICY BRIEF

Protecting Your DNA From Government Fishing Expeditions

LIBERTAS INSTITUTE

FREQUENT RECURRENCE TO FUNDAMENTAL PRINCIPLES IS ESSENTIAL TO THE SECURITY OF INDIVIDUAL RIGHTS

UTAH CONSTITUTION
ARTICLE I, SEC 27

2183 W Main Street, Suite A102, Lehi, UT 84043 | 801.901.0310 | LibertasUtah.org