

# How to Protect Your DNA Data Before and After Taking an at-Home Test



Mail-in genetic tests offer a wealth of information about your ancestry and insight into medical risks — in exchange for a lot of data. Here’s where that data goes, and how to delete it.

By Eric Ravenscraft

• June 12, 2019

Consumer DNA testing kits like those from [23andMe](#), [Ancestry.com](#) and [MyHeritage](#) promise a road map to your genealogy and, in some cases, information about what diseases you’re most susceptible to. They also ask for a lot of trust with your DNA information — trust that, in some ways, may not be earned. Here’s how to protect and delete your data if you use any of these services.

Home DNA testing kits usually involve taking a cheek swab or saliva sample and mailing it off to the company. In that little sample is the most personal information you can share: your genetic code. Some companies [share that data with law enforcement](#), and most [sell your DNA data to third parties](#), after which it can become difficult to track. For some people who work for small companies or serve in the military, it can affect insurance premiums and [even the ability to get insurance at all](#).

While DNA testing has been used in medical and scientific contexts for decades, direct-to-consumer testing kits are still relatively new and legal policies that govern the private use of consumer data are still being developed.

According to Dr. James Hazel, a postdoctoral fellow at the Center for Genetic Privacy and Identity in Community Settings, there are fewer protections for your data with consumer DNA testing kits than there would be if you were taking a medical test. If a doctor takes a DNA sample, that sample is protected by the [Health Insurance Portability and Accountability Act](#) and there are limits on how it can be shared.

“In the United States, if you’re talking about genetic data that’s generated outside of the health care setting, there’s a relatively low baseline of protection,” Dr. Hazel said. “And that’s provided generally by the by the Federal Trade Commission. So the Federal Trade Commission, although it’s not specific to genetic data, has the ability to police unfair and deceptive business practices across all industries. Other than that, there are really no laws in the United States that apply specifically.”

In other words, if you want to make sure your data is safe, you’re going to have to do the unthinkable: read the company’s privacy policy. That policy will tell you what data the company collects, how it’s used and what control you have over it. If a company deceptively violates its own policy, the F.T.C. can step in. Beyond that, though, you’ll have to read a company’s policy carefully before signing up.

## Go for the big names

For most DNA testing companies, the best way to protect your data is to not hand it over in the first place. In 2017, Dr. Hazel’s team [studied 90 DNA testing companies](#) and found most of their privacy policies wanting. Some companies only had policies governing use of their website, while others failed to indicate whether they strip away personally identifiable information from a sample before sending it off for testing. A few of the larger companies may have acceptable policies, but Dr. Hazel said you probably shouldn’t trust smaller testing companies that you haven’t heard of.

“When we looked in 2017, we found that 40 percent of companies appear to have no written policy that specifically mentioned genetic data,” Dr. Hazel said. “We saw these smaller companies that you might not have heard of had privacy policies that were a paragraph long, a couple paragraphs long, and really didn’t provide any information whatsoever.”

The more well-known testing companies are safer bets — perhaps because they’re so well-known. “And so when we have larger companies that are constantly sort of in the public spotlight, I think the result has been that these companies are generally more accountable,” Dr. Hazel said. “And their privacy policies are generally much more comprehensive.”

Three of the biggest names in home DNA tests are 23andMe, Ancestry.com and MyHeritage. You can find their privacy policies and specific instructions on how to delete data from each of them below. [Wirecutter](#), the product review website owned by The New York Times Company, [evaluated 15 DNA testing kits](#) and recommended [AncestryDNA](#) or [23andMe](#).

## What to watch for before you sign up

When you first set up a new smartphone, you might be asked to give a company permission to track your location or share data about how you use your phone. In

the same way, once you've picked a DNA test to try, there are a few things to watch out for. DNA testing companies tend to ask a lot of questions that may strike you as boring, but if you want to protect your data, you'll want to read them all carefully.

Consumers "want to look at what choices they have, in terms of the activities that they can opt into, or opt out of," Dr. Hazel said. Some companies like 23andMe have a separate agreement asking permission to use your DNA data in research studies. This data is stripped of identifying labels like your name or address that tie it to you specifically, but that's not always guaranteed to protect your privacy.

In some cases, Dr. Hazel said, companies use what's called "de-identified aggregate data," which is relatively safe. This kind of data might include summaries that don't specifically call out individuals, like [what percentage of people have a certain ancestry](#).

"But these companies also use what's called de-identified individual-level data, where there is, you know, always a risk that a person can be re-identified from that data," Dr. Hazel said. This kind of data might describe your unique genetic makeup without using your name. While it may be unlikely that this information could be linked back to you, [researchers have shown it is possible](#). Law enforcement famously used crime-scene DNA that was shared with a genealogical research site to [track down a suspect in the Golden State killer case](#), even though he never used a DNA test himself, demonstrating that even anonymized data can be used to identify people.

If you give a company permission to share your data with another research organization, you can revoke that permission later. However, it will be difficult or impossible to delete your data from third parties that have already received it. It's also hard to guarantee that those third parties won't also share your data with yet another company or research organization down the road. "Once that data has been shared with a third party, it's really difficult to control further sharing," Dr. Hazel said. That doesn't mean you shouldn't share data with researchers, but you should know the risks going in.

You may also be asked for permission to allow the DNA testing company to store your sample, meaning that it can go back and test it again if more advanced techniques are developed in the future. Some sites also offer a family finder feature that lets potential relatives contact you if your DNA matches. All of these can be very personal permissions to give. Reputable companies will make sure to inform you as much as possible, but be sure to read everything you're presented with before you click "Agree."

## How to delete your data from the Big Three

Each company has its own steps for deleting your data. We'll cover the steps for each of the Big Three companies below, as well as what deleting your data with that company entails.

## 23andMe

To delete your 23andMe data, head to [your account settings page](#) and find the "Delete Your Data" option under "23andMe Data." You can download any or all of your data before you destroy it. If you agreed to have your sample saved, it will also be physically destroyed.

However, 23andMe uses a laboratory that must follow regulations under the [Clinical Laboratory Improvement Amendments](#), or CLIA. This means that some data, including your DNA, sex and date of birth will be retained in order to comply with these regulations. The company will no longer use that information, though. You can read more about [the company's deletion process here](#).

## Ancestry

To delete data from Ancestry, [sign into your account](#), click the "DNA" tab and choose "Your DNA Results Summary." From there, click "Settings" and choose "Delete Test Results." You'll have to enter your password again to confirm that you want to delete your information.

This process will delete your DNA data, as well as prevent you from appearing in any family finder results. You can also [delete your entire Ancestry account](#). As with 23andMe (and any federally compliant DNA-testing company), your DNA information will be retained for regulatory compliance purposes, but nothing else, according to Ancestry's privacy policy.

## MyHeritage

To delete data from MyHeritage, [log into your account](#), click your name in the upper-right corner, and choose "Account Settings." From there, scroll to the bottom of the page and click "Delete Account." You can also choose to [delete your Family Tree Builder projects or sites](#) without deleting your entire account, but this will not necessarily delete your data. Since MyHeritage labs are CLIA-certified, they will also retain some information about you.

---

DNA testing companies have improved their methods for deleting your data over the years. However, since the United States government requires these companies to retain DNA information in order to comply with [quality control guidelines](#), it's never really possible to delete it forever. Before you sign up for a testing kit, always

make sure you know what you're agreeing to and that you're comfortable signing that permission away.