DNA Donors Must Demand Stronger Privacy Protection

Posted on **June 14, 2018** by **masonmarks**

By Mason Marks and Tiffany Li

An earlier version of this article was published in STAT.

The National Institutes of Health wants your DNA, and the DNA of one million other Americans, for an ambitious project called All of Us. Its goal — to "uncover paths toward delivering precision medicine" — is a good one. But until it can safeguard participants' sensitive genetic information, you should decline the invitation to join unless you fully understand and accept the risks.

DNA databases like All of Us could provide valuable medical breakthroughs such as identifying new disease risk factors and potential drug targets. But these benefits could come with a high price: increased risk to individuals' genetic data privacy, something that current U.S. laws do not adequately protect.

Last month, the NIH announced it was throwing open the doors to enrollment in All of Us. This comes at a time when genetic data privacy is in the public eye. Earlier this month, the popular genealogy site MyHeritage.com revealed that 92 million user accounts were breached. In late April, California police caught the alleged "Golden State Killer" by using an online DNA database called GEDmatch. In mid-May, the same database was used to help solve a double homicide committed in Washington state in 1987. Notwithstanding the benefits to law enforcement, these and other revelations are eroding public trust in genealogy websites like 23andMe and Ancestry.com. Without trust, it will be difficult for programs like the All of Us initiative to succeed.

Far more complex than fingerprints, a genetic profile is the single most identifiable characteristic people have. Such profiles contain a treasure trove of information about individuals and their health such as predispositions for cancer, neurodegenerative disease, and mental illness. It's not only genetic data that the All of Us Program will obtain. The project aims to collect biospecimens and data about donors' medical histories, lifestyles, families, and psychological health. It will also solicit data from their wearables like FitBits and Apple Watches.

Our current health privacy laws were created before genetic privacy became an issue, and they don't adequately protect it. For example, the Health Insurance Portability and Accountability Act (HIPAA), the primary U.S. health privacy law, does not apply to companies like GEDmatch, 23andMe, or Ancestry.com. Nor does it apply to the All of US Program, its corporate partners, or new forms of medical data gathered from sources like websites, apps, and wearables. HIPAA applies only to what it calls "covered entities" — individuals and organizations traditionally associated with health care, such as doctors, hospitals, insurance companies, and their business associates. HIPAA holds covered entities to

a high standard of care, requiring that they maintain the confidentiality of patient data and penalizing them in the event of a data breach. In many cases, the All of Us Program may have more sensitive information about you than your doctor. But the program is not your physician and is not subject to the duties imposed on healthcare providers by HIPAA and other regulations such as state medical licensing laws.

Beyond HIPAA, few laws prohibit police from accessing genetic data stored in public or private databases. There are even fewer restrictions on government access to genetic data if national security is at risk. That means contributing DNA to genealogy services could expose users and their families to law enforcement scrutiny. For example, if your relative's DNA is found at a crime scene, you could be dragged into an investigation due to your kinship. Even a distant relative's data could provide probable cause for law enforcement to conduct a search or interrogation.

Theft is also a concern. Consider what could happen if hackers stole genetic data from the All of Us database or a consumer genealogy site. Once it has been disseminated, it would be impossible to retrieve and conceal again. Hackers could hold the data for ransom or sell it to third parties such as data brokers or unscrupulous employers.

DNA databases can also be sold. In 1997, Iceland and a company called DeCODE Genetics launched a national database, which now contains DNA from nearly half the Icelandic population. In 2012, the pharmaceutical corporation Amgen bought the database and now profits from the insights gleaned from it. The All of US program will share data with its corporate partners including Google's life sciences division Verily.

We urge legislators to consider expanding HIPAA's definition of covered entities to include app developers, websites, and other companies that collect and analyze health data, including genetic information. In 2014, California passed a law that treats all companies that handle medical information as health care providers under the state's Confidentiality of Medical Information Act. To protect consumer genetic data, other states could follow California's lead. Even better, Congress could amend HIPAA to bring all companies that handle health data into its definition of covered entities. In that case, genealogy sites would be required to use the same privacy standards as doctors and hospitals.

At the same time, organizations and companies that collect genetic information, from 23andMe to the NIH, must be clearer and more straightforward about conveying how they protect individuals' genetic data. Current contract law governs the protection of genetic data through the agreements users sign when providing genetic information. These agreements are notoriously vague and difficult to understand, and they can give companies nearly limitless rights to use an individual's genetic information (and to change their policies at any time without consent). To protect consumer privacy, genetic testing entities must create privacy policies that prioritize clarity. They should also allow users to opt-out of data sharing that does not directly benefit the public or contribute to user test results.

To create laws that better govern both public and private genetic data collection and DNA databases, courts and lawmakers should draw from the concept of information fiduciaries, coined by Jack Balkin, a professor at Yale Law School, to describe the special relationship of trust between consumers and entities that collect their personal or sensitive information, Treating DNA databases like information fiduciaries would impose on them legal duties of care, confidentiality, and loyalty. They would be obliged

to act reasonably toward users, safeguard their data, and avoid conflicts of interest that could exploit them.

Public and private DNA databases have the potential to produce great social benefits, from improving cancer treatment to catching serial killers. But these benefits shouldn't come at the risk of exposing individuals' private genetic data. Before donating their DNA to private or public databases, individuals should ask hard questions — and read the fine print — to make sure their genetic information will remain private and protected.

Erosion of trust will discourage people from contributing their DNA and diminish the scientific benefits of programs like All of Us. To benefit fully from DNA databases, we must create and enforce fair industry standards, reform existing health laws to account for new sources of medical data, and create laws that protect genetic privacy rights.

This entry was posted in **Biospecimens**, **Biotechnology**, **Conflicts of Interest**, **Genetics**, **Health Information Technology**, **Health Law Policy**, **Law**, **Mason Marks**, **Medical Privacy** and tagged **Genetics**, **Health Law**, **health law policy**, **HIPAA**, **Privacy** by **masonmarks**. Bookmark the **permalink [https://blogs.harvard.edu/billofhealth/2018/06/14/dna-donors-must-demand-stronger-privacy-protection/]** .

About masonmarks

Mason Marks is a Visiting Fellow at the Information Society Project at Yale Law School. His research focuses on health law, privacy, and intellectual property. He is particularly interested in the application of artificial intelligence to clinical decision making in healthcare, emerging issues in health data privacy, and comparative privacy law. Mason's legal and technology writing has been featured in WIRED, the NYU Journal of Legislation and Public Policy, and Harvard Law School's Bill of Health where he is a regular contributor. Mason has been invited to speak at Yale Law School, Yale Medical School, Harvard Law School, Harvard Medical School, Arizona State College of Law, Seton Hall Law School, and the Yale Whitney Humanities Center. Mason received his J.D. from Vanderbilt Law School. He is a member of the California Bar and practiced intellectual property law in the San Francisco Bay Area. Prior to law school, he received his M.D. from Tufts University and his B.A. in biology from Amherst College.

View all posts by masonmarks →