Security Risks of DNA Testing

Isabella Forman
Comp 116: Security
December 12, 2018

Abstract

A popular trend emerging in recent years is sending in a sample of one's DNA to companies for the purpose of testing for genetic disorders or discovering one's ancestral information. These services should be regarded with caution. DNA is the most personal information a person possesses; is it safe to give this information to companies, who may do with it what they will, and to store this information in databases, which could be vulnerable to hacking? There have been several instances of hacking sensitive genetic information, at genealogy companies MyHeritage and Ancestry. Additionally, companies may sell clients' genetic information for profit. This paper examines the security risks associated with DNA testing, covering the de-anonymization of DNA, the genealogy companies' privacy and security policies, the effectiveness of such methods, and strategies to securely store DNA data. Participating in DNA testing services, although it may seem like a harmless, compelling way to learn about oneself and one's family, presents many security risks about which people should be very concerned.

Introduction

As technology advances and we become willing and capable of analyzing more and more personal data, our concern over what happens to this personal data must increase as well. One example of this is analyzing DNA. DNA testing began in 1985.[1] At that time, DNA testing was used primarily for forensic purposes. Police and prosecutors used DNA as evidence to convict criminals and to exonerate wrongly convicted people. More recently, DNA testing has been used to determine paternity, identify human remains, discover predisposition to genetic diseases, and discover ancestry.[1] Genetic tests can be performed in a clinical setting, or can even be done at home without any medical persona present.[2] Companies such as Ancestry, 23andMe, MyHeritage, and Helix offer genealogy tests as a business. These take-home genetic tests have become increasingly popular, especially for the purpose of discovering one's ancestry. As of February 2018, more than 12 million people had done DNA ancestry testing with consumer services (see Figure 1).[3] Different types of genealogical DNA tests include autosomal DNA tests, mitochondrial DNA tests, and Y-chromosomal DNA tests (for males only).[4]

The process of genealogical DNA testing through a consumer service is alarmingly simple. The process involves ordering a kit online, taking a saliva sample and putting it into a tube, mailing the saliva collection tube to the company for analysis, and logging into an online account to access test results.[5, 6] Some companies require a cheek swab instead of a saliva sample, but the rest of the process is the same. All reports are accessed simply through a password-protected account created on the company website.[5, 6]

The juxtaposition between the importance of DNA and the simplicity of giving this precious information to a company to be analyzed is cause for concern. Not only are results accessed through an online account, which is vulnerable to hacking, but individual genetic data is also stored long-term in online databases. Additionally, although these companies test DNA for the purpose of discovering genealogy, they find out much more information about a person besides genealogy in the process. They run single nucleotide polymorphism (SNP) tests that test "hundreds of thousands of markers, even though they may be only looking for a couple of hundred markers".[7] These tests can reveal genetic diseases and health information, much beyond the scope of one's genealogy – this is sensitive information that a customer may not want to be stored in company's database indefinitely. Although genealogy testing is the primary focus of this paper, when medical DNA testing is included as well, there are currently over 100

DNA databases online, and most of these databases are publicly accessible.[8] This raises the questions, how securely is people's DNA protected, and why does it matter?

To the Community

People gaining access to DNA data is cause for concern in many ways. First, even if the DNA data is stored without a person's name or other personal information as an identifier, it is easy to de-anonymize DNA. Carnegie Mellon University professors Bradley Malin and Latanya Sweeney used a program called CleanGene to use health data profiles to determine the identifiability of DNA from a database.[8] 98-100% of the DNA was able to be identified, using data from hospital visits and genetic disease diagnoses.[8] In a later experiment, at Harvard University's Data Privacy Lab, Professor Latanya Sweeney (now the lab director), was able to identify 42% of people who had donated their DNA to the Personal Genome Project.[9, 10] Approximately half of the DNA donors had also provided their zip code, date of birth, and gender. Using these three pieces of information, Sweeney was able to identify people through public records and was then able to link the names of specific individuals to their DNA. The DNA profiles included information such as "medical conditions including abortions, illegal drug use, alcoholism, depression, sexually transmitted diseases, medications and their DNA sequence," meaning that Sweeney was able to discover the personal medical history of these people who she had easily identified.[9, 10] In this case, people were identified based off the information that they had provided along with their DNA rather than solely based off their genomic data. Regardless of the method of identification though, this project showed the effortlessness of matching specific people to sensitive genomic data. When people send in DNA testing kits to 23andMe and other DNA testing services, they also provide their name, birthdate, address, and contact information, and it is not unreasonable to imagine that this data may be stored along with their DNA in the company databases.

While people can be easily connected to their own DNA, relatives of DNA donors can also be identified through a family member's DNA. The Y-chromosome is passed from fathers to sons, as last names have traditionally been passed down as well. Thus, there is a correlation between DNA on the Y-chromosome and family last name.[11, 12] Because of this information, genealogists have created databases that store Y-chromosome genetic information according to family last name. These databases are accessible by the public. Using this information, researchers at the Whitehead Institute for Biomedical Research in Massachusetts worked on a project to show that individuals and their relatives can be identified from one person's DNA, even if the DNA is stored in a de-identified form.[11, 12] They queried the Y-chromosome database with DNA data donated by volunteers to past genomic studies. Looking in the Y-chromosome database, they were able to match last names with the DNA. This process is called "surname inference".[11, 12] Once the Whitehead team had last names, they were able to use other records on the internet such as obituaries and public demographic data to identify the specific individuals. This project was eye-opening because it showed that "the posting of genetic data from a single individual can reveal deep genealogical ties and lead to the identification of a distantly-related person who may have no acquaintance with the person who released that genetic data".[11] Even if one man did not ever donate or submit his DNA to a company or research group, he could be identified through a (paternal) relative who had submitted DNA.

There are many reasons why people should care about keeping their DNA private.[13, 14] For example, a discovery of genetic diseases in one's DNA could lead to insurance rejection. Employers could refuse to hire people based off their predisposition for certain diseases found in their DNA. Careers of people running for political office could be demolished if it came out that they would be afflicted with genetic diseases several years down the road. The Genetic Information Nondiscrimination Act (GINA) is a law from 2008 that prohibits genetic discrimination by insurance companies and employers, but more exhaustive laws are necessary.[15] There are numerous ways in which people could be discriminated against, if their DNA fell into the wrong hands.[13, 14] Additionally, sperm or egg donors who

wish to remain anonymous could be discovered and contacted by their biological children because their DNA was unwillingly made public. In another vein, DNA can be used for forensic purposes.[13] Police can search DNA from crime scenes against DNA in genealogy databases. Through the genealogy databases, they can find relatives who had uploaded their DNA, and then police can use the family tree of the relatives to find the culprit.[16] This is how the alleged Golden State Killer was found. Law enforcement had generated a profile of the killer's DNA from crime scenes, and they uploaded it to GEDMatch, which is an open-source genealogy website. Through the GEDMatch database, they found a partial match, and used this relative to track down the criminal.[17] This process raises many ethical and privacy issues. Essentially, uploading one's DNA to the internet through genealogy services could cause the incrimination of one's relative in the future.

Genealogy Companies' Security Practices

The primary companies that offer genetic testing as a consumer service claim to protect their customers' DNA data, but they offer vague explanations for how, and they may retain more information long-term than people are aware of. Helix, which offers DNA testing for the purpose of ancestry but also for optimizing workouts, losing weight, and being aware of nutrition, asserts on the Data Security section of its privacy page that the company "use[s] strong SSL/TLS ciphers and strict policies to help keep your information private and safe".[18] This does not provide a lot of specific information. They should certainly be using SSL/TLS to encrypt network traffic; that is the bare minimum. However, that tells us nothing about how they secure the databases in which they store customers' DNA. Additionally, the Helix website states, "We also expect our partners to meet the standards that we established when it comes to privacy, security, control, and experience".[18] This statement comes across as ludicrous. Helix can *expect* their partners to meet the Helix security standards, but there is no guarantee of what the partners will *actually do*. If the partners are not a subsidiary of Helix, then Helix does not have control over how the partners will actually handle the DNA data, regardless of what Helix may hope. Also, Helix communicates that when someone purchases a DNA product, "You also allow us to share some basic details about you, like your age, sex, and contact information".[18] As shown earlier in the project at Sweeney's Data Privacy lab, just someone's age, sex, and contact information was exactly enough information to identify people by name and connect them with their DNA.

23andMe is another genealogy testing company that also offers vague information about how they secure their DNA databases and protect customers' sensitive genetic data. On the security page of the 23andMe website, the company states that "access to genetic and account information is enforced through different policies and encryption keys".[5] Additionally, they "use state of the art intrusion detection and prevention measures to stop any potential attacks against its networks" and have a program where people can report vulnerabilities that they find in exchange for a potential reward.[5] They also state that "personal information and genetic data are stored in physically separate computing environments".[5] It is unclear what this truly means– are they simply stored in separate databases but with an identifying number to connect the personal and genetic information, or is there really no link between the types of data? Finally, the website also states, "External firewalls restrict unauthorized connections to our databases".[5] I also sent an email to 23andMe to ask for more detailed information about their security practices, especially with regards to their databases. See Figure 2 for the reply received.

There were no significant differences in the statements on security from Ancestry, yet another genealogy testing service, either. This company does provide more information on how they store the DNA information, "Your AncestryDNA results are stored in a secured database, which employs a number of security measures. As well as protecting the information from unauthorized access from those outside of AncestryDNA, we strictly limit access to this database from within the company".[6] Of course, it is possible that there may be malicious intent from inside the company. Customers are able to download their raw DNA data from their account at any time, meaning that if someone gained access to a customer

account, they would gain access to that customer's DNA data. See Figure 3 for an email from Ancestry, in response to my email asking for more specific information about their security practices.

Effectiveness of the Methods of Security Used by These Companies

The methods of security that the genealogy companies described using were all necessary, first-line-of-defense methods. TLS/SSL, used by several companies, is used to keep a connection secure. It works through encryption of data sent back and forth between the user and the server. Secure Sockets Layer (SSL) is a part of the Transport Layer Security (TLS). Most systems use a combination of symmetric and asymmetric encryption. The SSL protocol is prevalently used; it is a basic first step to securely handling a customer's data and interactions with a website.[19] However, TLS/SSL do not encrypt metadata, such as IP and MAC addresses and protocols being used to send and receive information, which can reveal critical network information.[20] Additionally, the TLS/SSL certificates usually rely upon a third party, which could be compromised and could lead to a man-in-the-middle attack.[20] TLS/SSL is susceptible to its own vulnerabilities as well. Several known vulnerabilities and attacks from the past few years include POODLE (CVE-2014-3566), BEAST (CVE-2011-3389), CRIME (CVE-2012-4929), BREACH (CVE-2013-3587), and Heartbleed (CVE-2014-0160).[21] Some of the companies also mentioned encrypting their customers' passwords, which, like using a secure network connection, should be a given at this point in time. However, passwords can be cracked from their hashes using brute force or wordlist approaches, albeit this is not the most time-efficient way to gain access to a system. Also, it is predicted that quantum computers will be able to break encryption in approximately five years.[22]

Firewalls, which 23andMe asserted that it uses as defense, regulate which packets are allowed to enter a network. Agai, they are a good first line of defense against hackers or malicious packets. Current networks have many entry points, though, so one cannot rely solely on firewalls to defend against attacks.[23] There also still exist vulnerabilities with regard to firewalls. They cannot protect against insider attacks, only against attacks from outside the network.[24] In a strategy called "tunneling," or port forwarding, hackers can bypass the firewall by sending their malicious message in another message format, so that it looks like a public data packet when it is actually private.[24] Also, if the firewall does not perform deep packet inspection and only checks the source and destination IP addresses, it may miss threats that are in the payload of the packet.[24]

Both 23andMe and Ancestry mentioned that they store customers' genetic information separately from their personal information. This means that there is an attempt to anonymize the raw DNA data in their databases. However, no information was provided about how these companies actually protect their DNA databases. All three major companies' security pages described mostly how they secured their website and how they secured their customers' personal information. There was not much transparency about the security measures they put in place to safeguard the most valuable information – the genetic data.

Instances of DNA Data Breaches

Over the past few years, there have been a couple of significant security breaches in DNA testing companies. In December 2017, Ancestry suffered a large data breach. A file containing usernames, passwords, and email addresses of 300,000 customers was exposed via the Ancestry RootsWeb server.[25] According to the security report released by Ancestry after the incident, "RootsWeb is a free community-driven collection of tools that are used by some people to host and share genealogical information".[26] All of this information was then posted online in plaintext for anyone to see and use. Of those 300,000 login credentials, some of them were for RootsWeb alone and some were for both RootsWeb and Ancestry. Approximately 7,000 of the username/password/email info belonged to currently active Ancestry accounts.[25] In the security update written by Ancestry, the company stated that they believed the data breach was caused because "someone was able to create the file of older RootsWeb

usernames and passwords as a direct result of how part of this open community was set up".[26] More information beyond this vague statement was not provided. In response to this data breach, the company locked all of their affected customers' accounts, forcing them to change their passwords, and temporarily took RootsWeb offline.[26] Although this data breach did not leak peoples' DNA data directly, it is concerning because it leaked customers' login information to the site where they could view their DNA results. Thus, anyone could have logged in to the 7,000 active accounts and gained access to each customer's DNA through their account. Furthermore, by gaining access to the DNA directly through the customer's account, the DNA was not anonymized at all; the DNA was connected to all kinds of personal information.

More recently, in June 2018, MyHeritage was affected by a much larger data breach. The email addresses and encrypted passwords of 92.3 million users were exposed.[27] The company stated that the breach had actually taken place in October 2017, and anyone who had created an account up through that time was affected. It is fortunate that the passwords were hashed rather than stored in plaintext; however, it is still possible to recover the passwords from their hashes. A Bloomberg article reporting on the data breach claims, "But even if hackers were able to get into a customer's account, it's unlikely they could easily access raw genetic information, since a step in the download process includes email confirmation".[27] People tend to use the same passwords for many accounts, though, so one could imagine, that if a hacker were able to crack the password for the 23andMe account, the hacker could also gain access to the target's email account using the same password. In the statement that MyHeritage released after the incident, the company stated that the DNA information should still be safe because "DNA data are stored by MyHeritage on segregated systems, separate from those that store the email addresses, and they include added layers of security".[28] After this incident, MyHeritage hired a cybersecurity firm to conduct forensic reviews, sped up their work on a two-factor authentication feature, and forced users to change their passwords.[28]

Action Items

Both genealogy companies and customers can take several steps to protect DNA data. First, genealogy companies should be very careful about to whom they give access of the DNA databases. The 1996 law Health Insurance Portability and Accountability Act (HIPAA) allows medical companies to sell medical data if it has been anonymized.[29, 30] Genetic companies can take advantage of this and capitalize off the genetic data that their customers give to them. 23andMe has already sold access to their databases to at least 13 pharmaceutical firms. As was mentioned earlier, once sole ownership of the database by the genealogy company is relinquished, there is no guarantee how the data will be used or secured. Also, as already established, it is not difficult to de-anonymize the DNA data. Thus, selling access to the DNA databases presents one of the biggest security risks. Genealogy companies should be cautious about selling their customers' data. Ideally, they should not sell it at all, but realistically, they should take legal measures and sign contracts to regulate how outside companies will use and protect the data. In terms of protecting their DNA databases, it is difficult to know what to suggest without knowing what security measures are already in place. Decoupling DNA from customers' personal information in the databases is a good start. Other important basic security measures to protect a database include encrypting the information in the database, segmenting the database with varying levels of access granted to different people (and granting access to as few people as possible), requiring credentials to access the database, and using a firewall.[31] Monitoring the database closely, tracking accesses, is also essential.

Several academic papers have also investigated the privacy risks regarding storing DNA and have proposed methods to ensure greater security. Xiaosan Lei et al. at Xidian University and Anhui University in China looked at preserving the privacy of paternity tests, another type of genetic test that involves the whole DNA sequence.[13] They propose a "privacy-preserving genetic paternity test scheme in the cloud," using the asymmetric RSA encryption algorithm.[13] There are four parties involved: the users provide their

genomic data; the Certification Authority generates the public/private keys and generates pseudonyms for the users; the Certified Institution processes the DNA, divides the genomic data into smaller units, encrypts these individual units, and uploads the data to the cloud; and the Cloud Service Provider provides cloud storage for the data.[13] The authors then show how this method of storage can resist attacks form the Cloud Service Provider and other users who have submitted their own DNA.[13] This method of encryption could be used on genealogy DNA data as well. Mustafa Canim et al. proposed securely storing biomedical data using symmetric encryption on the data, and then using asymmetric cryptography to encrypt the symmetric encryption key.[32]

In another approach to protecting the confidentiality of medical data such that even if the system is hacked, the data will be difficult to understand, Zhen Lin et al. from the Department of Genetics at the Stanford University School of Medicine proposed using data binning.[33] They designed an all-purpose algorithm to anonymize all kinds of medical data, by "generaliz[ing] data upwards in hierarchies until the values of records are shared by a user-specified number of records, called the *bin size*".[33] A larger bin size means that more patients' records are stored together, meaning that it becomes more difficult to connect data to the specific individual from whom it came.[33] They handle genomic data by representing it according to the genomic location of the SNPs (genetic variation) in the DNA.[33] However, it is unclear how this method would be implemented to store the comprehensive raw DNA data collected for genealogy testing, rather than just being concerned about the SNPs in the DNA.

At an individual level, customers should use strong passwords that are different than their passwords for email and other accounts. Using a unique, complicated password decreases the chance that their account could be accessed and their raw DNA data could be downloaded, if there is another data breach and password hashes are leaked. Taking a step back, customers should consider thoroughly the implications of handing over their DNA forever to these genealogy companies, before they buy the DNA testing kits. Purchasing a DNA testing kit from a genealogy company means giving your raw DNA data to the world, for the genealogy company to use and to sell to other companies. Once you give away your DNA, it is out of your control what happens to it and who gains access to it. Furthermore, submitting one's DNA can affect one's relatives far into the future. Thus it is not just a personal decision; one must consider the ethical implications of how it will affect all blood relatives.

Conclusion

DNA is highly sensitive information, and access to one's DNA has serious implication both for oneself and for one's biological relatives. When people buy genealogical testing services, they relinquish sole control over their DNA data and place it in the trust of large companies. Additionally, these companies may then sell the DNA to other companies for profit or hand it over for use in research. Although genealogical companies claim to ensure the security of their systems, there have already been a few instances of data breaches, and it is not unlikely that there will be more in the future. Genealogical companies must emphasize up-to-date security in their databases and servers, and customers must do their part to use strong, unique passwords. Researchers at universities around the world are currently working on schemes for more secure protection of DNA and other biomedical data. Essentially, people should be aware of the security and privacy risks before purchasing genealogical testing. It is exciting that our biological sciences and technology have advanced such that these services are readily available, but the tradeoffs of giving away such personal information must be considered. As the extent to which we rely on technology to hold more sensitive information increases, we must ensure that the rate of progress in cybersecurity increases as well.

Figures

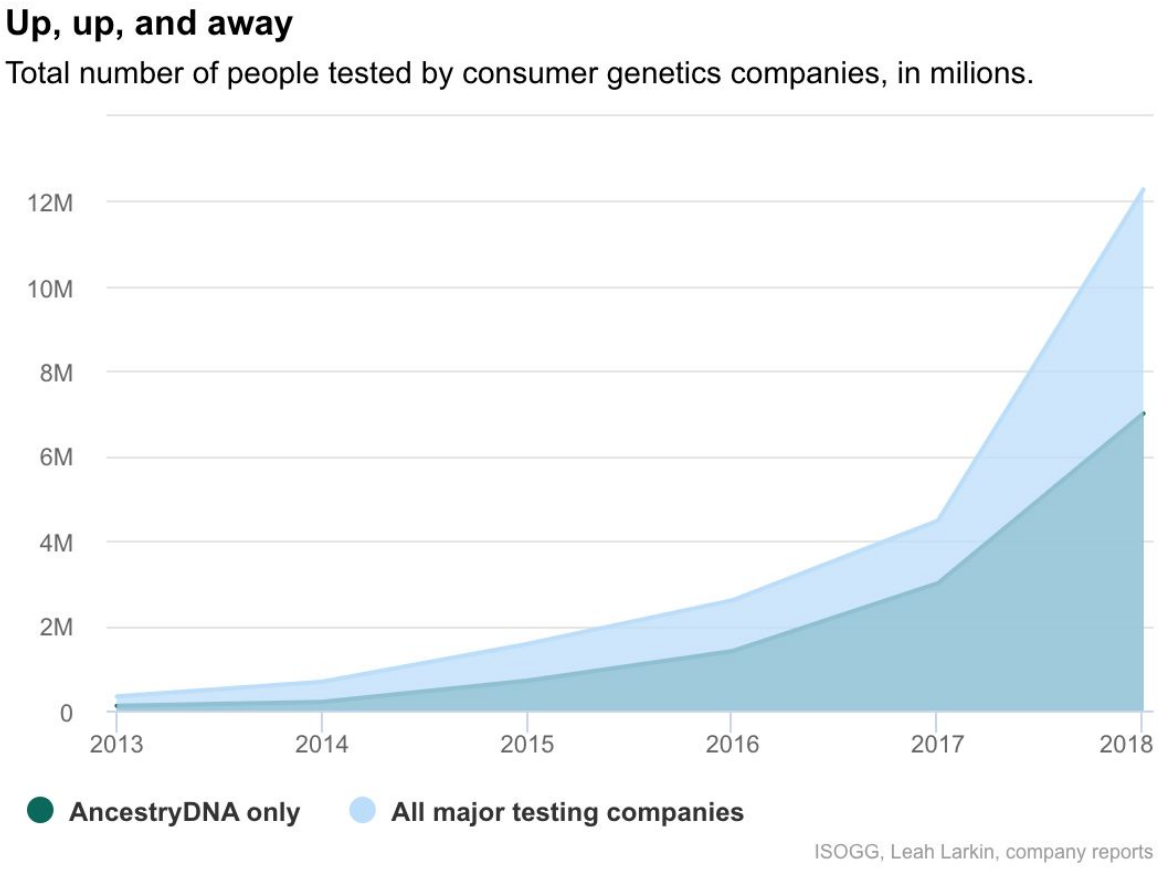
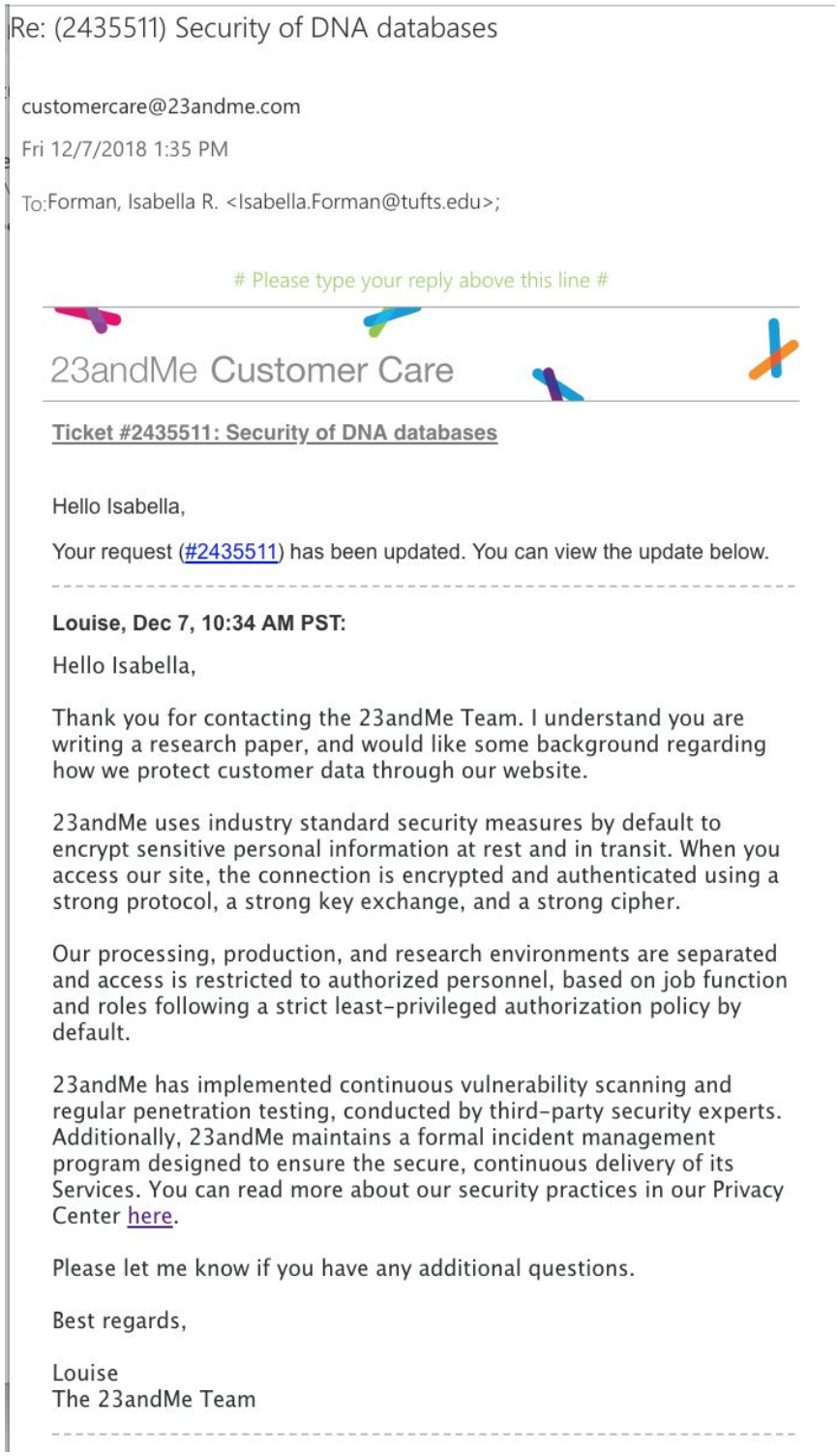


Figure 1



Re: (2435511) Security of DNA databases

customercare@23andme.com

Fri 12/7/2018 1:35 PM

To:Forman, Isabella R. <Isabella.Forman@tufts.edu>;

Please type your reply above this line

23andMe Customer Care

Ticket #2435511: Security of DNA databases

Hello Isabella,

Your request (#2435511) has been updated. You can view the update below.

Louise, Dec 7, 10:34 AM PST:

Hello Isabella,

Thank you for contacting the 23andMe Team. I understand you are writing a research paper, and would like some background regarding how we protect customer data through our website.

23andMe uses industry standard security measures by default to encrypt sensitive personal information at rest and in transit. When you access our site, the connection is encrypted and authenticated using a strong protocol, a strong key exchange, and a strong cipher.

Our processing, production, and research environments are separated and access is restricted to authorized personnel, based on job function and roles following a strict least-privileged authorization policy by default.

23andMe has implemented continuous vulnerability scanning and regular penetration testing, conducted by third-party security experts. Additionally, 23andMe maintains a formal incident management program designed to ensure the secure, continuous delivery of its Services. You can read more about our security practices in our Privacy Center here.

Please let me know if you have any additional questions.

Best regards,

Louise
The 23andMe Team

Figure 2

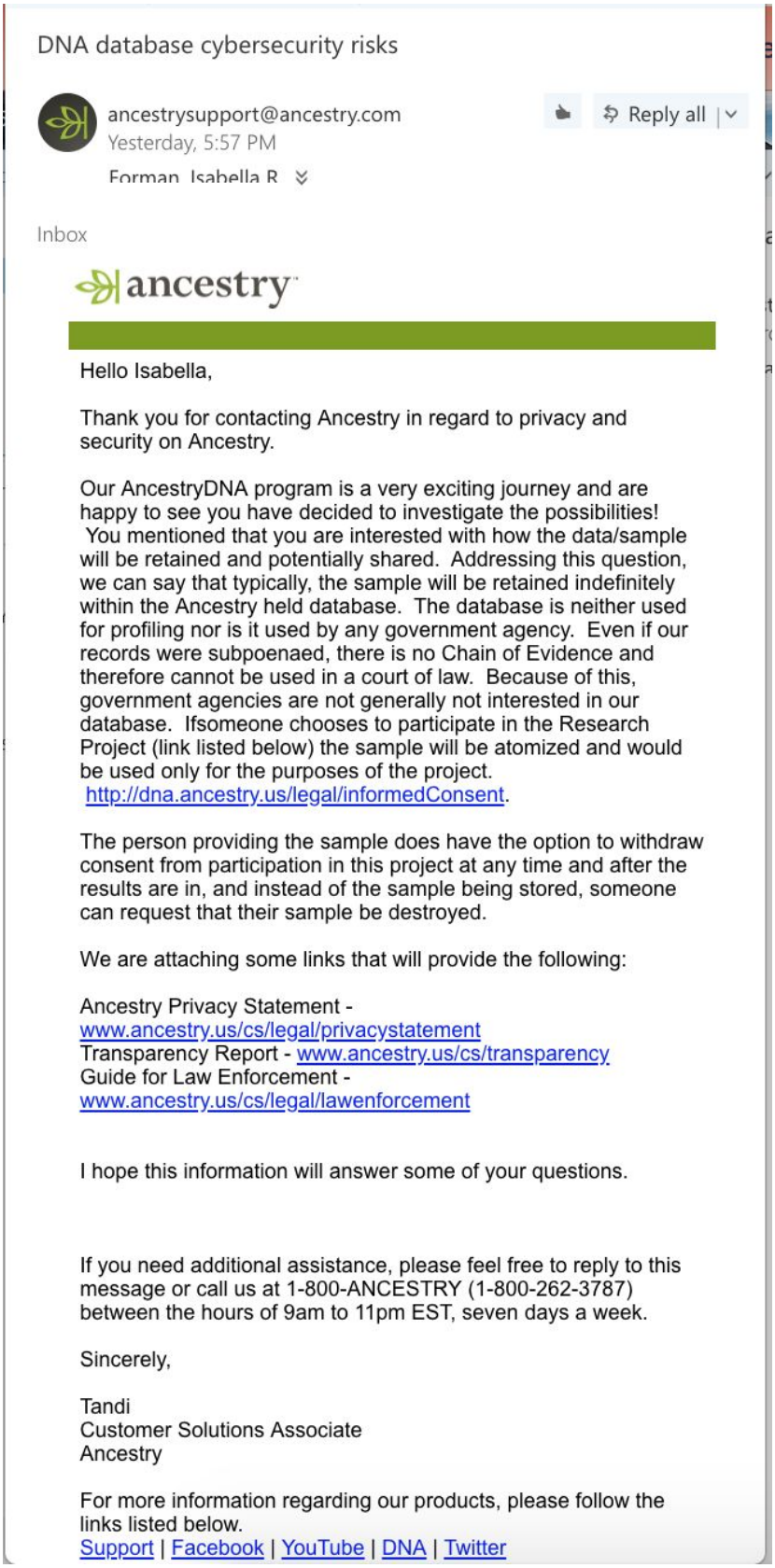

DNA database cybersecurity risks
ancestrysupport@ancestry.com
Yesterday, 5:57 PM
Forman, Isabella R
Reply all
Inbox
ancestry
Hello Isabella,
Thank you for contacting Ancestry in regard to privacy and security on Ancestry.
Our AncestryDNA program is a very exciting journey and are happy to see you have decided to investigate the possibilities! You mentioned that you are interested with how the data/sample will be retained and potentially shared. Addressing this question, we can say that typically, the sample will be retained indefinitely within the Ancestry held database. The database is neither used for profiling nor is it used by any government agency. Even if our records were subpoenaed, there is no Chain of Evidence and therefore cannot be used in a court of law. Because of this, government agencies are not generally not interested in our database. Ifsomeone chooses to participate in the Research Project (link listed below) the sample will be atomized and would be used only for the purposes of the project.
http://dna.ancestry.us/legal/informedConsent.
The person providing the sample does have the option to withdraw consent from participation in this project at any time and after the results are in, and instead of the sample being stored, someone can request that their sample be destroyed.
We are attaching some links that will provide the following:
Ancestry Privacy Statement - www.ancestry.us/cs/legal/privacystatement
Transparency Report - www.ancestry.us/cs/transparency
Guide for Law Enforcement - www.ancestry.us/cs/legal/lawenforcement
I hope this information will answer some of your questions.
If you need additional assistance, please feel free to reply to this message or call us at 1-800-ANCESTRY (1-800-262-3787) between the hours of 9am to 11pm EST, seven days a week.
Sincerely,
Tandi
Customer Solutions Associate
Ancestry
For more information regarding our products, please follow the links listed below.
Support | Facebook | YouTube | DNA | Twitter

Figure 3

References

1. James, Randy. "DNA Testing." *Time Magazine*, June 19, 2009. http://content.time.com/time/nation/article/0,8599,1905706,00.html.

2. "How Is Genetic Testing Done?" U.S. National Library of Medicine. Accessed December 12, 2018. https://ghr.nlm.nih.gov/primer/testing/procedure.

3. Regalado, Antonio. "2017 Was the Year Consumer DNA Testing Blew up." MIT Technology Review. February 13, 2018. Accessed December 12, 2018. https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

4. Ryan, Laura, PhD. "Guide to DNA Testing." Innerbody. July 27, 2018. https://www.innerbody.com/dna-testing.

5. "DNA Genetic Testing & Analysis - 23andMe." 23andMe. Accessed December 12, 2018. https://www.23andme.com/.

6. "Ancestry." Ancestry. Accessed December 12, 2018. https://www.ancestry.com/.

7. Fox, Maggie. "What You're Giving Away with Those Home DNA Tests." NBCNews.com. November 29, 2017. Accessed December 12, 2018. https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

8. Malin, Bradley, and Latanya Sweeney. "Determining the identifiability of DNA database entries." In *Proceedings of the AMIA Symposium*, p. 537. American Medical Informatics Association, 2000.

9. Tanner, Adam. "Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study." Forbes. April 25, 2013. Accessed December 12, 2018. https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#822d64292c9b.

10. Sweeney, Latanya, Akua Abu, and Julia Winn. "Identifying participants in the personal genome project by name (a re-identification experiment)." *arXiv preprint arXiv:1304.7605*(2013).

11. Fearer, Matt. "Scientists Expose New Vulnerabilities in the Security of Personal Genetic Information." Whitehead Institute. January 17, 2013. Accessed December 12, 2018. http://wi.mit.edu/news/archive/2013/scientists-expose-new-vulnerabilities-security-personal-genetic-information.

12. Gymrek, Melissa, Amy L. McGuire, David Golan, Eran Halperin, and Yaniv Erlich. "Identifying personal genomes by surname inference." *Science* 339, no. 6117 (2013): 321-324.

13. Lei, Xiaosan, Xiaoyan Zhu, Haotian Chi, and Shunrong Jiang. "Cloud-assisted privacy-preserving genetic paternity test." In *Communications in China (ICCC), 2015 IEEE/CIC International Conference on*, pp. 1-6. IEEE, 2015.

14. Minkoff, Howard, and Jeffrey Ecker. "Genetic testing and breach of patient confidentiality: law, ethics, and pragmatics." *American journal of obstetrics and gynecology* 198, no. 5 (2008): 498-e1.

15. GINA. June 2010. http://www.ginahelp.org/GINAhelp.pdf.

16. Regalado, Antonio. ""Hundreds" of Crimes Will Soon Be Solved Using DNA Databases, Genealogist Predicts." MIT Technology Review. September 13, 2018. Accessed December 12, 2018. https://www.technologyreview.com/s/612001/hundreds-of-crimes-will-soon-be-solved-using-dna-databases-genealogist-predicts/.

17. Zhang, Sarah. "How a Genealogy Website Led to the Alleged Golden State Killer." The Atlantic. April 27, 2018. Accessed December 12, 2018. https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/.

18. "Helix - Follow Your DNA." Helix. Accessed December 12, 2018. https://www.helix.com/.

19. "What Is SSL?" Comodo. September 12, 2017. Accessed December 12, 2018. https://www.instantssl.com/ssl.html.

20. Gomez, Paulina. "Why TLS/SSL Encryption Techniques Are Not Enough and Still Expose You to Hacking Threats - Ciena." Ciena. May 15, 2017. Accessed December 12, 2018. https://www.ciena.com/insights/articles/Why-TLSSSL-encryption-techniques-are-not-enough-and-still-expose-you-to-hacking-threats.html.

21. Prodromou, Agathoklis. "TLS/SSL Explained - Examples of a TLS Vulnerability and Attack, Final Part." Acunetix. March 22, 2017. Accessed December 12, 2018. https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/.

22. Foremski, Tom. "IBM Warns of Instant Breaking of Encryption by Quantum Computers: 'Move Your Data Today'." ZDNet. May 18, 2018. Accessed December 12, 2018. https://www.zdnet.com/article/ibm-warns-of-instant-breaking-of-encryption-by-quantum-computers-move-your-data-today/.

23. Rouse, Margaret. "Firewall." SearchSecurity. Accessed December 12, 2018. https://searchsecurity.techtarget.com/definition/firewall.

24. Kashefi, Iman, Maryam Kassiri, and Ali Shahidinejad. "A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities." *Internationla Journal of Engineering Researh and Applications (IJERA)* 3, no. 2 (2013): 585-591.

25. Navarro, Francis. "Ancestry.com Suffers Big Data Leak - 300,000 User Credentials Exposed." Kim Komando. December 28, 2017. Accessed December 12, 2018. https://www.komando.com/happening-now/435921/ancestry-com-suffers-big-data-leak-300000-user-credentials-exposed.

26. Blackham, Tony. "RootsWeb Security Update." Ancestry Blog. December 23, 2017. Accessed December 12, 2018. https://blogs.ancestry.com/ancestry/2017/12/23/rootsweb-security-update/.

27. Brown, Kristen V. "Hack of DNA Website Exposes Data From 92 Million Accounts." Bloomberg. June 5, 2018. Accessed December 12, 2018. https://www.bloomberg.com/news/articles/2018-06-05/hack-of-dna-website-exposes-data-from-92-million-user-accounts.

28. "MyHeritage Statement About a Cybersecurity Incident." MyHeritage Blog. June 4, 2018. Accessed December 12, 2018. https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/.

29. Malin, Bradley A. "An evaluation of the current state of genomic data privacy protection technology and a roadmap for the future." *Journal of the American Medical Informatics Association* 12, no. 1 (2005): 28-34.

30. Pitts, Peter. "The Privacy Delusions Of Genetic Testing." Forbes. February 15, 2017. Accessed December 12, 2018. https://www.forbes.com/sites/realspin/2017/02/15/the-privacy-delusions-of-genetic-testing/#4abd3e1b1bba.

31. Thompson, Elaine. "5 Ways to Improve Database Security." Business.org. March 21, 2014. Accessed December 12, 2018. https://www.business.org/it/cyber-security/ways-improve-database-security/.

32. Canim, Mustafa, Murat Kantarcioglu, and Bradley Malin. "Secure management of biomedical data with cryptographic hardware." *IEEE Transactions on Information Technology in Biomedicine* 16, no. 1 (2012): 166-175.

33. Lin, Zhen, Michael Hewett, and Russ B. Altman. "Using binning to maintain confidentiality of medical data." In *Proceedings of the AMIA Symposium*, p. 454. American Medical Informatics Association, 2002.