Buying Your Genetic Self Online – pitfalls and potential reforms in DNA testing

Andelka M. Phillips

www.andelkamphillips.com

This is the pre-print accepted version. This article appears in the May/June 2019 issue of IEEE Security and Privacy. Digital Object Identifier 10.1109/MSEC.2019.2904128 Date of publication: 14 May 2019

Introduction

Today's world is one of constant monitoring and tracking – sometimes driven by us, sometimes driven by others. Developments in the field of health and identity are no exception. New technologies such as wearable devices and other technologies in consumer centred healthcare allow us to track our fitness and health data, and connect us with others.

Similarly, the rise in direct-to-consumer genetic testing services ("DTC", sometimes known as personal genomics or commercial genomics), can be viewed both as an example of emerging technology and also as disruptive innovation. These services have created a commercial market for genetic tests, allowing people to buy their own DNA tests online without a medical intermediary.

However, as with wearable health devices, DTC potentially affords opportunities for other entities to access and compile that data and subject us to profiling. Consumers therefore need to understand what's involved when we buy our 'genetic self' online.

This article provides a brief introduction to the world of DTC and its potential traps for the unwary. It discusses some short and longer term regulatory measures that may help to iron out the most serious risks to consumer privacy. In particular, it concludes that the industry needs more oversight

and consumers need more control of their genetic data and personal data in the DTC context.

The growth of 'direct to consumer' genetic testing

The market for DTC has been experiencing significant growth in the last couple of years with some prominent DTC companies having databases with several million consumers' samples.

Ancestry testing is particularly popular, but the industry varies widely with a broad spectrum of services available. The best known ancestry and health tests are provided by prominent companies, such as 23andMe, AncestryDNA, Orig3n, MyHeritage, and Family Tree DNA. However, there are also companies offering lesser known tests that are often more dubious, including assessing child talent; peace of mind paternity; and infidelity (often dubbed surreptitious testing). Several of these tests raise privacy and ethical concerns.

The proliferation and variety of services on offer are increasingly attracting attention from researchers. My own research (due to be published as a book later in 2019) included a review of the online contracts of 71 DTC companies providing tests for health purposes. It found that a number of terms commonly included in these contracts are problematic from a consumer protection standpoint. Some companies, such as Soccer Genomics, have also resulted in concern from research scientists, with Stephen Montgomery at Stanford University launching a parody 'Yes or No Genomics' website in response. Another parody website, DNA Friend, is a useful resource to highlight the sensitive nature of these services. However, these parodies do to some extent assume a level of knowledge about genetics and we really need more efforts to assist the public in understanding the risks here.

While there is increasing public awareness of ancestry and health tests, what is less well understood is that these tests are generally not standardised and that any entity collecting genetic data could potentially use that data for secondary research or share it with third parties, such as

law enforcement. This article explores the problems that can arise as a result. It also discusses the existing and potential mechanisms that might help to resolve those problems.

A lack of standardisation

In relation to DTC tests for health purposes, many tests for common complex diseases are not harmonised and the validity of their findings is open to dispute.

In particular, DTC companies often do not provide whole genome scans and instead focus on portions of an individual's genome. Also, they can focus on different genetic variants and also frame their populations differently. As a result, it is possible to get contradictory disease risk estimates from different companies.

The more common ancestry tests have also not been standardised, and it is similarly possible to obtain contradictory ethnicity estimates from different companies. There have even been instances of DTC companies providing DNA test reports on canine samples without distinguishing them from human samples. For example, in their article "Heredity or hoax?" on the CBC News website (13 June 2018), Jorge Barrera and Tiffany Fox discussed an example where a man had sent a dog DNA sample to a company (under a human name) and received an estimate of 20% First Nations ancestry.

This means that consumers need be cautious about these services. At the very least, the public needs to be provided with more information about the limitations of testing. The utility of the service being sold may be limited.

Secondary use of genetic data

The potential for genetic data to be used in ongoing research is high. A number of the most prominent DTC companies have begun to partner with the pharmaceutical industry and we have also begun to see investment by

the insurance industry in DTC. One challenge here is that it is not possible to truly anonymise genetic data. (See for example the work of Yaniv Erlich, Science 339, 321–324 (2013)). If something goes wrong, we cannot change our stored genetic data in the same way we could change our bank password. So it is particularly important that where DTC companies engage in such research they implement strong security practices and infrastructure.

It is important for consumers to understand the potential for secondary use here. The source of profit for DTC companies will often be partnerships and mergers with other entities and there is a significant level of uncertainty here in relation to the variety of ways in which genetic data could be used in the future.

Use for law enforcement is also attracting increasing attention. In the last year, there was much media coverage of the genetic genealogy database GEDmatch's involvement in the investigation of the Golden State Killer case, where law enforcement accessed its database in order to find a potential suspect, through the process of familial DNA matching. Since this revelation, it has emerged that more than 100 other DNA profiles from cold cases have been uploaded to GEDmatch. In early 2019 it also emerged that the DTC company Family Tree DNA has been working with the FBI to investigate violent crime (see for instance Matthew Haag's article in the New York Times on 4 February 2019).

Genetic data is sensitive in nature

Genetic data is generally viewed as sensitive. It can do real harm in the wrong hands. It is also much more than a method of identification in criminal proceedings. Genetic data has certain characteristics, which mean that it can pose long term privacy risks for individuals and their relatives.

Once you have a genetic test, your genetic code is digitised and that digital data can be stored potentially indefinitely and used for purposes beyond the primary purpose for which you gave it. It can also serve as a unique identifier for both you and your genetic relatives (who may be different from your family). The impact of a data leak may be substantial, and it does not decrease over time.

The industry also operates internationally. Typically, a consumer can purchase a test through a website and then they will receive a sample collection kit in the mail. This is normally used for the collection of a saliva sample or a cheek swab, which the individual then sends back to the company for processing. Although services vary, companies will generally provide results through a web interface.

From a regulatory perspective, the international nature of the industry creates complexity. The physical sample may be sent overseas and processed and stored by a company in a different country from where the consumer resides. The sequenced genetic data generated from this physical sample may or may not be stored in that same country. Also, DTC companies may collect other forms of personal data from their consumers through surveys and other research activities. Where this is stored may also vary, and again may be different from where the consumer resides.

These features, among others, affect how we need to think about regulation of businesses that handle genetic data.

The impact of the General Data Protection Regulation on DTC

Europe's data protection law, the General Data Protection Regulation ("GDPR") is supposed to put users back in control of their data. It has direct relevance to the DTC industry: any company that sells or provides services directly to consumers based in the EU needs to ensure that it complies with the GDPR.

Genetic data is included in the prohibition on processing of special categories of data in article 9 of the GDPR. Consequently, in order to comply with the GDPR, companies should be obtaining explicit and informed consent from their consumers for a DNA test. A more traditional "notice and choice" model is insufficient. In my research to date on regulation of DTC it seems likely that many businesses will need to alter their consent mechanisms in order to meet this higher standard.

Part of the problem is that e-commerce based services have relied on their online information (including contracts and privacy policies) to govern relationships with consumers. However, providing clear online information about complex subjects can be a challenge. Also, we have all grown accustomed to ignoring terms and conditions and privacy policies on websites. This is due to a number of factors, but one of the most significant problems is that people often lack the time to read these documents and even where they do take the time, they may struggle to understand their contents. Many businesses have created longer contracts and privacy policies or terms of service documents which are heavily skewed in favour of their interests, rather than those of their consumers. There has also been a lack of oversight of these documents. Consumers are deterred from reading them and may believe that they are not capable of challenging or changing the use of their information in any case.

However, under the GDPR, a high standard of consent is required for data processing and it is not going to be acceptable to bury consent in a lengthy contract or to only make company policies accessible after a consumer has registered for a service. Both under the GDPR and under EU consumer protection legislation there are also requirements for these documents to be in plain and intelligible language. As contracts and privacy policies are often linked together, problematic terms in contracts, which could be challenged on consumer protection grounds may also be found to be

problematic from a data protection perspective as well. EU consumer protection legislation also restricts the inclusion of terms that may be deemed to be unfair and limits their enforceability.

As the GDPR beds in, consumers are also starting to realise that they have genuine mechanisms to challenge what companies are doing with their data. The recurring and self-serving rhetoric expressed by some key players in Big Tech that 'privacy is dead' is changing. We are starting to see a shift with wide-reaching laws such as the GDPR, together with growth in mega data breaches, and calls for further regulation. Privacy is not only still alive – it is kicking. For example, the most recent Annual Report released by the Irish Data Protection Commissioner (which is the first line of regulation for many tech companies in Europe) demonstrates that people do care about their privacy and that complaints lodged under the GDPR are likely to increase.

Many countries outside the EU are also reforming their privacy and data protection laws to cater for new developments. Simply stopping marketing DTC services to EU consumers, to avoid coverage by the GDPR, is therefore unlikely to be a viable solution. DTC companies will increasingly need to meet similar legal requirements for consumers based outside the EU.

Suggestions for reform

The DTC industry has grown in the last two decades with relatively little oversight, during which time the potential of the technology has grown immensely. A number of policy documents have been released by diverse bodies, which could be drawn upon in improving industry governance. For example, the UK's Science and Technology Committee has recently begun an inquiry into Commercial Genomics and is seeking public submissions. It is hoped that this inquiry will lead to improved oversight of the DTC industry in the UK and may provide useful guidance for other countries considering

how to regulate the industry. The UK's disbanded Human Genetics Commission also previously developed a Common Framework of Principles, which could be drawn upon in developing new legislation or industry codes of conduct.

Below are some further suggestions for both short term and long term strategies. There is no perfect solution, but a number of steps could lead to significant improvements for consumers and for improving standards across the industry.

In the short term:

- The public needs more independent informational resources to assist them in making informed decisions about whether or not to utilise DTC services. Data protection authorities and privacy regulators as well as consumer regulators could release statements in relation to the industry. The Office of the Canadian Privacy Commissioner has already begun to take steps in this direction. It has released a number of documents in relation to DTC, including recommendations for questions that consumers could ask DTC companies, and questions that they should ask themselves when considering purchasing a test. This example could provide a useful model for other regulators exploring these issues.
- Existing regulators should also consider developing industry codes of conduct and model privacy policies and consumer contracts. One potential foundation for such a code is the Future of Privacy Forum's paper "Privacy Best Practices for Consumer Genetic Testing Services" (June 2018), which was developed in collaboration with some prominent DTC companies. This document makes a number of positive commitments in relation to privacy, but it is voluntary and it remains to be seen how businesses will adhere to this. Unlike the Future of Privacy Forum paper, though, any code should make it clear

that American companies selling genetic tests to consumers based in the EU should still be complying with the GDPR.

- Another model is to make codes of conduct mandatory for the industry to follow. There may be reasonable support for such a move: DTC companies that wish to engage in health research and maintain consumer trust have an interest in showing that they comply with the law and support improvement of industry standards. They will wish to distance themselves from more dubious types of tests.
- Businesses should rethink their drafting of contracts and privacy policies. In relation to contracts, clauses that significantly limit consumers' rights should be avoided. For example, if businesses wish to be compliant with the GDPR and applicable consumer protection legislation then they should not include clauses that allow them to change their terms at any time without notice to the consumer.
- Businesses should also think about their interface design. Given the sensitive nature of genetic data and the complex nature of some health test results, consumers should not be rushed into making a purchase. Putting speed bumps into the process, which encourage reflection and allow consumers to change their minds could help to achieve compliance with the GDPR. It would be beneficial for businesses to allow for a cooling off period as well in between purchase and processing of the sample.
- Businesses should also improve their practices in relation to deletion and destruction of physical samples and data. It should be possible for any company performing a genetic test to provide their consumers with the option of deleting the data and destroying the sample after sending the consumer their test results. Guardiome is an interesting example here, as they offer consumers their whole genome sequence on a device and their approach seems to be more privacy centric.
- Businesses should also keep in mind the GDPR's principles in relation to data processing. In the context of DTC, adhering to the data minimisation principle could be particularly beneficial.

- At the national level, privacy and data protection regulators as well as consumer protection regulators should play a role in improving industry governance. Compliance reviews of privacy policies, contracts, and personal data practices, particularly in relation to security practice would all be beneficial for improving industry governance.

In the longer term:

- We need more specific oversight of the industry in order to improve standards and ensure the protection of privacy and consumer rights more generally. One possibility is the creation of new regulatory bodies with a mandate to regulate all businesses that handle genetic data. This could draw upon existing models of data protection authorities and financial services regulators and in some countries, this could be a new body that was under the oversight of the data protection authority.
- Tests of more dubious validity, such as surreptitious tests and child talent should be banned and regulators should help to alert the public about the most problematic services. In the UK, the Human Tissue Act makes it an offence to analyse DNA without appropriate consent and it is likely that any company offering surreptitious tests to UK consumers is likely to be in breach of this.
- New legislation dealing more specifically with individual's rights in genetic data is needed. The recent Canadian Genetic Non-Discrimination Act could provide a useful model for other countries considering how to strengthen the rights of citizens in their genetic data.
- New industry specific legislation should also be introduced at a nation level and international collaboration to develop more universal standards that could be followed globally could also help consumers given the international nature of these services.

This article has provided an introduction to the world of DTC and the challenges the industry poses for privacy. It is vital to understand that there is also a lot of uncertain risk in this context. We do not know all the ways that our genetic data could be used in the future, but given that we cannot change our genetic data and that it can always potentially be linked back to us, can be used for many different purposes, and can also be used to trace our family members, reform is needed. People do need protection of their rights in this space and businesses should also view this as an opportunity to do things differently.

About the author:
Dr Andelka M. Phillips is a Senior Lecturer at Te Piringa Faculty of Law, the University of Waikato, New Zealand and a Research Associate, Centre for Health, Law and Emerging Technologies (HeLEX), University of Oxford.
Email: andelka.phillips@waikato.ac.nz
www.andelkamphillips.com