Canadian Journal of Law and Technology

Volume 15 | Number 1 Article 8

1-1-2017

Third-Party Services as Potential Sources for Law Enforcement Procurement of Genomic Data

Katherine Kwong

Third-Party Services as Potential Sources for Law Enforcement Procurement of Genomic Data

Katherine Kwong*

INTRODUCTION

Genomic data have become increasingly popular with people who are eager to learn more about themselves, their families, and their health.[1] Many individuals have sought to obtain this type of information by using third-party services that collect and analyze genomic data, which have become popular in part due to their relatively low price point and simple processes.[2] The companies that provide these services have become the keepers of enormous amounts of genomic data, creating a rich source of private individuals' information.[3]

The immense growth in this type of data collection has not escaped the notice of law enforcement. Genomic data have the potential to be very useful to law enforcement who seek to identify suspects, reconstruct crimes, or obtain additional evidence.[4] But not every piece of potential genomic evidence will turn up a match in official law enforcement databases.[5] When unable to obtain genomic data through other methods, law enforcement may turn to third-party businesses, seeking their customers' genomic data.[6]

Many companies include clauses in their terms of service informing customers that they will comply with law enforcement requests when legally

---

* J.D. student, Harvard Law School; Master of Public Health, Public Health Genetics, University of Washington.

1 See Cathelijne H. van der Wouden et al., "Consumer Perceptions of Interactions with Primary Care Providers After Direct-to-Consumer Personal Genomic Testing" (2016) 164:8 Ann. Intern. Med. 513; Wylie Burke and Susan Brown Trinidad, "The Deceptive Appeal of Direct-to-Consumer Genetics" (2016) 164:8 Ann Intern Med 564.

2 23andMe, perhaps the most well-known company offering services directly to consumers, promotes the simplicity of its $199 service by saying, "It's just saliva. Provide your saliva sample from home. Mail it back to our lab in the same kit it came in — the postage is pre-paid. We bring your genetics to you." 23andMe, online: < www.23andme.com > .

3 23andMe and Ancestry.com each have more than one million samples. Stephanie Lee, "As Companies Collect More Health Data, Cops Will Ask to See It", *BuzzFeed* (5 November 2015), online: *www.buzzfeed.com* > .

4 See Karen J. Maschke, "DNA and Law Enforcement", in Mary Crowley, ed., *From Birth to Death and Bench to Clinic: The Hastings Center Bioethics Briefing Book for Journalists, Policymakers, and Campaigns* (Garrison, NY: The Hastings Center, 2008) 45.

5 *Ibid.*

6 Paul Elias, "Law Enforcement Investigators Seek Out Private DNA Databases", *Boston Globe* (26 March 2016), online: < www.bostonglobe.com > .

appropriate.[7] These clauses mean companies providing third-party genomic data services may be put in the position of providing data to law enforcement against their customers' wishes. While these companies obviously do not wish to be put in a position of defying valid warrants, court orders, or subpoenas that legally compel them to provide information, the companies must also manage customer expectations. That means companies must consider how to design their processes and procedures to both comply with legal requests and maintain crucial customer relationships.

These difficult decisions are not merely a matter of speculative concern. Companies such as Ancestry.com[8] and 23andMe[9] have already received requests from law enforcement to provide genomic information these companies have stored on their servers. This paper examines two cases studies: Ancestry.com's experience with law enforcement use of its genetic databases, and 23andMe's responses to requests for users' genomic data. Analyzing the responses to law enforcement requests by the two of the largest providers of third-party genomic services provides insight into the struggles third-party genomic services are likely to face and possible future directions for companies facing this type of law enforcement request.

I. ANCESTRY.COM AND PUBLICLY AVAILABLE GENETIC DATABASES

Ancestry.com, a for-profit genealogy service, operates AncestryDNA, a service with the mission of "help[ing] everyone discover, preserve, and share their family history through the use of genetic testing and analysis."[10] Through AncestryDNA and related services, Ancestry.com hopes to add value to its customers' experiences by allowing them to connect with others who are genetically related to them.[11] AncestryDNA has collected more than one million DNA samples,[12] in addition to other genetic databases Ancestry has developed or obtained. Unfortunately, despite Ancestry's genealogical research intentions, in at least one well-publicized case, genetic information made available by Ancestry was used not just by genealogists seeking to find familial connections, but by law enforcement searching for suspects in a crime.

---

7 See e.g. Ancestry, "AncestryDNA Privacy Statement" (12 June 2015), online: <dna.ancestry.com/en/legal/us/privacyStatement>; 23andMe, "23andMe Privacy Statement" (7 December 2015), online: <www.23andme.com/about/privacy/#Full>.

8 Ancestry, "Ancestry 2015 Transparency Report", online: <www.ancestry.com/cs/transparency>.

9 23andMe, "Transparency Report" (1 August 2016), online: <www.23andme.com/transparency-report>.

10 Ancestry, "Privacy for Your AncestryDNA Test", online: <www.ancestry.com/cs/legal/PrivacyForAncestryDNATesting>

11 *Ibid.*

12 Lee, *supra* note 3.

Michael Usry's father donated his DNA years ago to the Sorenson Molecular Genealogy Foundation, a non-profit project sponsored by the Church of Jesus Christ of Latter-day Saints.[13] The project's genetic database was subsequently purchased by Ancestry, which allowed the data to be made publicly available.[14] Law enforcement officials who were investigating a 1996 murder had tried and failed to find a DNA match in national criminal databases, but found what seemed to be a promising match with the genetic profile of Usry's father when they searched the data publicly available online in the Sorenson Molecular Genealogy database.[15] Although the name of the person associated with the genetic profile was listed as "protected" in the Sorenson Molecular Genealogy database and was not publicly available, the police used a search warrant to obtain from Ancestry "all information including full names, date of births, date and other information pertaining to the original donor to the Sorenson Molecular Genealogy project."[16]

The strength of the genetic match appeared to indicate that a relative of Michael Usry's father had left the DNA evidence at the scene of the crime.[17] Police further narrowed their suspect pool down from all of the donor's relatives to Michael Usry based on Facebook friends in the same state as the crime, his sisters having attended college in the state, and the types of films he made professionally, which included killings in their plots.[18] Based on this relatively weak information, law enforcement officials were able to obtain a warrant requiring Michael Usry to provide a DNA sample for comparison purposes.[19] Ultimately, Michael Usry was not a match for the DNA evidence found at the scene of the crime, and was eventually cleared of being a suspect in the crime.[20]

When asked about Michael Usry's case, a spokesperson for Ancestry said, "On occasion when required by law to do so, and in this instance we were, we have cooperated with law enforcement and the courts to provide only the specific information requested but we don't comment on the specifics of cases."[21] The

---

13 Jim Mustian, "New Orleans Filmmaker Cleared in Cold-case Murder; False Positive Highlights Limitations of Familial DNA Searching", *New Orleans Advocate* (8 March 2015), online: < www.theneworleansadvocate.com > .

14 Brendan Koerner, "Your Relative's DNA Could Turn You Into a Suspect", *Wired* (13 October 2015), online: < www.wired.com > .

15 Mustian, *supra* note 13.

16 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", *Electronic Frontier Foundation* (1 May 2015), online: < www.eff.org > .

17 Koerner, *supra* note 14.

18 Mustian, *supra* note 13.

19 *Ibid.*

20 Debra Cassens Weiss, "Cops Seek DNA Information from Ancestry.com and 23andMe", *ABA Journal* (20 October 2015), online: < www.abajournal.com > .

21 Kashmir Hill, "Cops Are Asking Ancestry.com and 23andMe for Their Customers' Data", *Fusion* (16 October 2015), online: < www.fusion.net > .

Sorenson Molecular Genealogy database has since been removed from public viewing, with a statement saying, "[u]nfortunately, it has come to our attention the site has been used for purposes other than that which it was intended, forcing us to cease operations of the site."[22] Ancestry has stated that it does not intend to make the database publicly available again in the future.[23]

Removing this type of data from being available publicly is a good first step towards ensuring that customers' data is not used for unintended purposes. If the Sorenson Molecular Genealogy database had not been publicly available, then law enforcement officials would not have been able to run the genetic profile they were seeking to match against the more than 100,000 genetic profiles[24] contained within the database. Without that initial apparent match with a publicly available profile, the subsequent search warrants for the donor's name and information and Michael Usry's DNA sample would almost certainly have not been so easily obtained, and Ancestry would not have become the subject of extensive news coverage about its inadvertent role as a law enforcement tool.

Ancestry has also taken proactive steps to address customers' (and potential customers') concerns about the privacy of their genetic data. One element of this is increased communication about when and how genetic data may be disclosed by Ancestry. Both AncestryDNA's official Privacy Statement[25] and AncestryDNA's FAQ page[26] state that DNA results will be disclosed, "as may be required by law, regulatory authorities, or legal process," as well as under other described circumstances.

Ancestry has also taken steps towards increased transparency regarding its disclosures to law enforcement. The company had previously refused to state how many requests it received from law enforcement for its users' data,[27] but released a Transparency Report at the end of 2015. The Transparency Report covered all types of law enforcement requests for customer data, including non-genomic data related to issues such as credit card fraud and identity theft.[28] According to the Transparency Report,

> Ancestry did not receive any requests relating to the health or genetic information of any Ancestry member in 2015. In our history, we have received just one request relating to DNA information — a 2014 search warrant ordering us to provide the identity of a person based on a DNA sample that had previously been made public for which the police

---

22 Sorenson Molecular Genealogy Foundation, online: < www.smgf.org > .

23 *Ibid.*

24 Lynch, *supra* note 16.

25 Ancestry, "Privacy Statement", < dna.ancestry.com/legal/privacyStatement > .

26 *Supra* note 10.

27 Cassens Weiss, *supra* note 21.

28 *Supra* note 8.

> had a match. We disclosed information in response to that valid warrant.[29]

The Transparency Report explicitly states, "We received no requests for information related to the health or genetic information of any Ancestry member [in 2015], and we did not disclose any such information to law enforcement."[30]

The lack of genomic data disclosure to law enforcement appears to be the result of a lack of requests by law enforcement, rather than any company stance on attempting to protect its customers' data. The report's language makes clear that future law enforcement requests are likely to be complied with, saying, "Ancestry requires valid legal process in order to produce information about our members. We comply with legitimate requests in accordance with our Privacy Statements."[31] Of the 14 law enforcement requests made to Ancestry in 2015 (all of which were for non-genomic data), the company provided the information requested in all but one case.[32]

In the face of the very real possibility that Ancestry might disclose genomic information to others, customer control over their own data is important. Ancestry has sought to allow customers to control who has the ability to view their genetic results, and to permanently delete their DNA test results at any time, to ensure that no one has access.[33] Allowing permanent removal of data may be particularly important to customers who want to feel as though they retain control over their data and how the data might be used.

II. 23andMe AND PERSONAL GENOMICS

23andMe offers direct-to-consumer genetic testing that provides personalized information about individuals' genomes.[34] The company has sequenced more than one million customers' genetic information from customer supplied biological samples.[35] The data collected by 23andMe include information about customers' ancestry, carrier status for genetic conditions, and information about other inherited traits,[36] all of which could be used by law enforcement to help identify individuals, or for other law enforcement purposes.

Like Ancestry, 23andMe seeks to communicate to its customers that their data may be disclosed to law enforcement. The 23andMe Privacy Statement includes a warning that, "23andMe will preserve and disclose any and all

---

[29] *Ibid*. This statement is presumably an oblique reference to the Michael Usry case, as well reassurance that Ancestry did not receive any similar requests in 2015.

[30] *Ibid*.

[31] *Ibid*.

[32] *Ibid*.

[33] *Supra* note 10.

[34] 23andMe, "What You Get", online: < www.23andme.com/service/ > .

[35] 23andMe, "About", online: < www.23andme.com/ > .

[36] *Supra* note 34.

information to law enforcement agencies," when it believes it is required to do so.[37] In addition to this warning (which might not be seen by customers who do not read the full Privacy Statement prior to signing up for 23andMe's services), the company's Privacy Center, which is designed to be more accessible to consumers, includes as section on "Law enforcement requests."[38] This type of disclosure is important to ensure that customers are fully informed about their potential exposure to law enforcement requests. 23andMe's step of including the information on a page specifically designed to communicate clearly with customers (and not just burying it within a lengthy privacy policy) is a good practice to help ensure that the information actually reaches customers in a way they can understand.

To further promote customer control and choice, 23andMe also allows its customers to decide whether their original genetic samples will be stored, how their data are shared with other 23andMe members, and whether they wish to participate in optional tools which might connect them to relatives (similar to some of AncestryDNA's tools).[39] Customers are also able to delete their data at any time, which would at least theoretically prevent the deleted data from being utilized by law enforcement.[40] While none of these steps will completely protect existing customers from law enforcement requests for their data while they continue to use the service, all of these measures should be seen as good practices to follow as a baseline for protecting customer privacy.

One positive practice that should be emulated by other companies is 23andMe's expressed preference for notifying customers affected by a law enforcement request. 23andMe's privacy officer told a reporter by email that, "[i]n the event we are required by law to make a disclosure, we will notify the affected customer through the contact information provided to us, unless doing so would violate the law or a court order."[41] This assurance is echoed for customers on the Privacy page.[42] While the effect of this policy may admittedly be limited if law enforcement forbid such disclosure when making their requests, it should nonetheless be considered a best practice to disclose law enforcement requests to affected customers whenever possible.

This type of communication is part of 23andMe's broader policies related to transparency. The company appears to have been the first company in the consumer health data industry to issue a transparency report, releasing its first transparency report in October 2015.[43] As part of the report, available on

---

37 *Supra* note 7.

38 23andMe, "Privacy & Data Protection", online: <www.23andme.com/about/privacy>.

39 *Ibid.*

40 Hill, *supra* note 21.

41 *Ibid.*

42 *Supra* note 38.

43 Hill, *supra* note 21.

23andMe's website, the company disclosed that, in the United States, it had received four requests for user data that affected five user accounts.[44] The company says that it has thus far been able to avoid disclosing any of its customers' information to law enforcement and that it is committed to continuing to fight law enforcement requests for data.[45] 23andMe has stated that it will update the report quarterly; as of the August 1, 2016 update, these numbers have remained unchanged.[46] The 23andMe Transparency Report also states that the company has not received any requests for customer data from law enforcement agencies in Canada, the United Kingdom, the Netherlands, Sweden, Finland, Denmark, or Ireland.[47]

The highly positive reception[48] received by 23andMe's Transparency Report further supports arguments that voluntary transparency and disclosure by companies about law enforcement requests for customer data can be a net positive for companies' images and their relationships with their customers. 23andMe's privacy officer has used the Transparency Report as a way of promoting the company's image with customers and the general public as being concerned with its customers' privacy. The privacy officer told a reporter that, "[t]he Transparency Report represents our dedication to being forthcoming with our customers and doing everything we can to protecting customer information."[49] 23andMe's announcement of its Transparency Report may have been part of what pushed Ancestry to change its stance on releasing information about the number of requests it has received.

If such reports become increasingly common and desirable to customers, then they may move from a "best practice" to an "expected practice" for companies that wish to maintain a positive image related to privacy and transparency. Market pressures may make transparency reports even more important for companies from a marketing perspective. Earlier adoption may be seen as a proactive step to protect customer data and privacy, rather than a reactive step once an incident has occurred.

Increased transparency about data usage and requests from law enforcement has been particularly been praised by watchdog groups such as the Electronic Frontier Foundation, which argues that divulging such requests can help improve customer perceptions of companies such as Ancestry and encourage accountability.[50] Other groups such as the Center for Genetics and Society have expressed concerns that a transparency report, "isn't actually that transparent at the end of the day," because it may not reveal bulk collection or methods other

---

44 *Supra* note 9.

45 Hill, *supra* note 21.

46 *Supra* note 9.

47 *Ibid.*

48 *Ibid.*

49 Hill, *supra* note 21.

50 Lee, *supra* note 3.

than formal requests by law enforcement made directly to the company.[51] Nonetheless, transparency reports have been seen by many researchers and groups as a positive first step in disclosing companies' relationships with law enforcement.

III. LESSONS LEARNED AND FUTURE DIRECTIONS

Based on the experiences of Ancestry and 23andMe, a number of lessons can be identified for third-party services that possess customers' genomic data, with specific, actionable steps. These case studies demonstrate the importance of controlling data access and providing customers with appropriate transparency and disclosure. Additionally, while these case studies show what has happened in the United States, third-party genomic service companies need to prepare for the potential for law enforcement requests in other countries.

Ancestry's experience with the Sorenson Molecular Genealogy database demonstrates that companies should proactively examine the potential access paths into their databases. Ancestry had the best of intentions when it allowed the public to search its database for genetic profile matches. But even when a company intends a data-sharing function to be used for one purpose — for example, to find relatives, or to connect with others who share a genetic trait, or even to encourage people to achieve fitness or health goals through increased accountability — those functions may be used by law enforcement for other purposes if improperly protected, or law enforcement access is provided for by contract or policy. It is one thing to state in a privacy policy that customer data will be disclosed to law enforcement if needed to comply with a court order or other legal request — customers should be able to reasonably expect that companies will not inadvertently disclose data to law enforcement.

To protect customers' privacy, genomic data companies should, at a minimum, ensure that data are not made publicly available; clearly state how and when data will be shared, communicating in a manner that customers are likely to comprehend; allow customers to decide to delete all of their data at any time; and ensure that data are adequately protected from both a technological and security process standpoint. An even better practice would be to default to the most protective data sharing settings, and then educate customers about their options when it comes to sharing their data.

23andMe's experience with their Transparency Report is an example of the potential positive effects that can be achieved with greater transparency. When the number of requests is low, disclosing them is unlikely to cause consumers undue alarm and may improve the company's image as being open and transparent with its customers. 23andMe has used its increased transparency as a successful public relations tool. As more companies begin to issue transparency reports, customers may begin to expect greater openness about law enforcement requests for data. Moving proactively to create transparency systems prior to

---

[51] *Ibid.*

incidents will give customers a "baseline" to compare to and might increase customer trust.

To achieve transparency goals, genomic data companies should create reporting systems that disclose when they receive requests for data law enforcement, including both the number of requests and the number of users affected, as well as whether any data were provided to law enforcement in response to the requests. Such reporting systems should be updated as frequently as possible, to prevent long lag times between when such requests are made and when customers have an opportunity to learn that law enforcement has requested data from the company. Companies should also implement a policy of contacting any affected users whenever possible (so long as it does not violate any court orders).

Finally, companies should prepare to implement appropriate policies and procedures for dealing with law enforcement requests in all of the countries in which they operate. Both companies are pursuing additional international opportunities. AncestryDNA recently expanded its operations and is now available in a total of 35 countries.[52] 23andMe, already available in the United States, Canada, and six European countries,[53] is interested in expanding in China and Southeast Asian countries.[54] Both companies have international privacy policies that contain nearly identical provisions stating that data will be disclosed in compliance with legal or regulatory processes.[55] Given the variations between legal processes and requirements in different countries, these companies should be careful to ensure that they remain in compliance and are prepared to appropriately respond to any law enforcement requests in other countries.

These case studies show that genomic data collection has become an increasingly attractive source of information for law enforcement. Companies that collect genomic data should be aware that sooner or later, law enforcement is likely to come seeking customer information. Learning from past experiences and creating policies in advance will do much to protect companies against negative incidents and bad publicity.

---

[52] Jessica Murray, "AncestryDNA Now Offered in 29 New Countries" (23 February 2016), *Ancestry Blogs* (blog), online: < blogs.ancestry.com > .

[53] Meghana Keshavan, "23andMe's Position on Genomic Diversity, International Expansion" (7 February 2016), online: MedCity News < www.medcitynews.com > .

[54] Caroline Humer and Christina Farr, "After Canada, UK, 23andMe Wants DNA Test Growth Abroad", *Reuters* (15 January 2015), online: < www.reuters.com > .

[55] Ancestry, "AncestryDNA Privacy Statement (Outside the United States)" (18 May 2015), online: < dna.ancestry.com/en/legal/international/privacyStatement > ; 23andMe, "23andMe Europe — Privacy Policy" (7 Dec 2015), online: < www.23andme.com/en-eu/about/privacy/#Full > .