A ranking of direct-to-consumer

DNA testing:

spotting privacy and ethical implications

CONTENT

Executive summary
The use of direct-to-consumer (DTC) DNA services is growing worldwide. Such services are becoming increasingly diversified and technologically advanced, allowing users to obtain information about their relatives, ancestry, and health just by mailing a saliva sample. However, in a context characterized by a weak regulatory framework and lack of public knowledge about the implications of DNA data management, this raises many questions about the use of such sensitive data by these organizations, as well as the methods used for ensuring data subjects' rights. This report introduces the legal and ethical implications of DTC services focusing on privacy issues. It also offers a ranking of DNA banks based on critical variables so consumers can better understand existing options, whether to use these services and make an informed decision.

1. INTRODUCTION

Private companies offering direct-to-consumer (DTC) DNA services have increased their business market significantly in recent years. The basic functioning of these services consists of users mailing saliva samples to DTC service providers to have their genotypes analyzed and receive back their raw genetic data, often with additional information about their past or health. Well-known and bigger organizations in the field, such as 23andme or Ancestry, have technology **able to compare millions of DNA characteristics** and offer DNA matching services for a low cost (~€100-€200). Moreover, some of their genetic analysis can support the identification of relatives up to the fourth order. It was estimated that by 2021 more than **100 million people** would have provided their DNA to four leading commercial ancestry and health databases (Regalado, 2019).

However, the vast reach and potential benefits of these services must be weighed against their risks. Even though the construction of a DNA profile and its analysis is already standard procedure (it can, for instance, largely be automated), the **accurate interpretation** of the results of the matches is very challenging and requires significant expertise (Annas, 2006). Additionally, the provision of genetic information to direct-to-consumer genetic testing services is fraught with legal, ethical and social concerns.

1.1 Main legal concerns

Information on the individual submitting their data to a DNA biobank is varied. Consumers are typically encouraged to provide sensitive information about themselves or their families to maximize the utility of the genetic test being offered. For example, "self-reported" information might include personal and family medical history, ethnicity, physical traits, or details about the consumer's lifestyle and habits. This compounds the privacy implications of personal health information as it includes not just the genetic data of the primary customer, but it exposes their relatives' information as well (Edge and Coop, 2020). According to GDPR Article 9, these special categories of personal data, such as genetic data, require further security measures for processing since, as stated by the ECHR (2022: 13), concerning DNA profiles, "*the possibility of drawing inferences from them*

as to an individual's ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life, calling for heightened protection".

Addressing these risks, all DNA banks should have **internal data security policies at the operational level**, including training for team members. Such training should be integrated into the organization's Standard Operating Procedure (SOP). Organizations should also have a comprehensive operations guide to support proper data curation and usage. However, in many cases, DNA bank entities do not perform the whole data management system in-house, including sequencing and analysis (Takai-Igarashi et al., 2017). Instead, many organizations outsource part of the sequencing or analysis process to be conducted within the premises of a third organization. This governance can affect the DNA bank's level of control over data security and quality.

In Europe, DNA banks' data management must follow the requirements and principles established by the GDPR (Art. 5). This includes data minimization, accuracy, purpose and storage limitation, and data security. **Information on the privacy protections** afforded at the testing laboratories should be provided to data subjects prior to sharing the biological samples and performing any tests, allowing them to make an informed decision on submitting their sample. Emphasis should be placed on expressing **affirmative consent** for the data uses stated, with each different use carrying a separate consent indication. The literature has shown that making consent specific and explicit enhances users' assessment of the personal and moral implications of biobanking (Eisenhauer et al., 2019).

Moreover, DNA banks' data controllers must also provide adequate and user-friendly **communication channels** that the data subject can easily use for accessing their data. Once an access request is received, the controller must check whether any of the person' personal data is being processed at all, and activate mechanisms to enable access, rectification or cancellation of data. Many bank organizations, however, still **do not have explicit access policies** within their consent and information protocols, enabled, in part, by the fact that "conflicts" between the European and national regulations still exist unaddressed. This includes cases where entities managing genetic data are not allowed to share results with data subjects (patients) without the intervention of a specialist, or instances where data cannot be released to the parents of children providing their samples (Narayanasamy et al. 2020).

Data subjects should be informed of the specific persons or institutions that would be provided access to their data and the reasons for granting it (Hallinan, 2021: 169). This includes access by anyone from staff members within the organization, to family members, to law enforcement. Several law **enforcement legal frameworks and jurisdictions in Europe and beyond** allow competent authorities to access private DNA banks in the public interest, and people who upload their DNA to public sites to learn more about their health or family history may not realize how law enforcement could use the information. Although in many countries, these authorities are subjected to establishing "*appropriate technical and organizational measures to ensure a level of security appropriate to*

the risk" (as for Art. 32 GDPR), such data reuse entails ethical implications, since it may involve a breach of initial consent.

1.2 Main ethical and societal concerns

Many of the above legal implications mirror **ground ethical dilemmas**, which can be classified in four dimensions:

- Probability tests vs health-related effects
- Direct access to data vs lack of genetic counseling
- Inequality in matching accuracy vs data protection implications
- Impact on relatives vs the ethics of data sharing

Firstly, issues concerning the **accuracy and clinical validity of DTC genetic tests** need to be considered (Grosse et al., 2010). It should be noted that these tests provide probability information regarding the future **development of certain diseases** such as cancer, diabetes or Alzheimer's. Therefore, consequences of imprecise or incorrect genetic assessment can include discrimination, stigma or impacts on an individual's health due to them adjusting behaviours or routines based on test outcomes. Moreover, the literature reveals that this process has significant effects on users' psychological **well-being** (Broady et al., 2018).

Given the risks of this business model, Almeling & Gadarian (2014) show that **most people, 65%** of surveyed individuals in their study, consider that clinicians should be implicated in clarifying and interpreting genetic test results. Despite this, marketing strategies and services provided by these companies often do not adequately address the genetic council, leaving users without proper guidance about their results (Farahani, 2022).

Thirdly, any genetic testing **should be accompanied by disclosure of the test's specificity and accuracy,** as it also has societal implications for the individual's **wider family unit and beyond**. For instance, accuracy in matching data against specific **ethnic groups** has privacy implications. The more an ethnic group is represented in genetic databases, the more likely that additional members of that group can be identified. If, for example, a person lives in the United States and has European ancestry, there is a high likelihood that a third cousin or closer relative can also be **identified in the database**, while it would be much harder to identify relatives of someone from an underrepresented ethnicity or race. In addition, surname inference can lead to the identification of personal genomes affecting the privacy of persons' data present in the database. While ethnic diversity indicates that a person is more likely to be matched with a relative, further implications to their privacy must be explained to benefit the data subject and to allow them to provide informed consent on submitting their genetic data.

Suppose we rely on the **bedrock of informed consent** as our standard. In that case, we could limit or eliminate the possibility of accidentally uncovering direct genetic relatives (e.g., a child put up for adoption as discussed in the case study in 2.2) in DTC genetic testing. Still, the possibility of **indirect discovery** would not be avoided. As a result of these complications, allowing individuals to learn their genetic connections to others necessarily threatens the right of individuals to

remain anonymous. Stakeholders must handle the unveiling (or not) of genetic relatives they are aware of and prioritize existing social relationships.

Lastly, an additional and related ethical dilemma to be weighed concerns the implication of DTC genetic testing results for **users' family members**. DTC DNA results concerning both risks of developing a disease or relatives' discovery based on the genetic testing may significantly impact the data subject's relatives if they are revealed. This fact questions the ethical nature of users sharing or communicating personal and health data, and the associated interpretation to those affected by it (Peterson, 2005).

1.3 White paper report goals and method

This white paper aims to illustrate the above issues by introducing **three case studies** concerning the use of DNA data for **forensic, adoption, and research purposes** and guiding readers through **existing DNA bank options** by producing a ranking of the most important services worldwide. We will rank them according to three main dimensions, data management, data sharing policies, and your rights vs their terms. The ranking is based on a review of their Terms and Conditions and Privacy Policies to extract indirect evidence concerning each variable (11 in total). Documentary and literature reviews are also used to provide an understanding of DTC DNA services risks and benefits.

2. SHEDDING LIGHT THROUGH THE FOG: three case reports

Three uses of genetic data that pose the **biggest challenge to privacy and security are addressed in this section**. First, an analysis of the use of genetic data for **forensic purposes** which questions the legality and ethical promise of extracting genetic data as a means to secure a conviction and solve a criminal case. For instance, there is a long history of conviction cases being made based on wrong interpretations of DNA results (Gabel and Wilkinson, 2008; Walsh et al., 2016). Secondly, the use of genetic data to **identify relatives** or find links within a family tree, the primary offering for several data banks, which can be both a helpful tool to reunite families and a risky venture when one turns over their data to a data bank that may not be entirely secure in its privacy efforts. Lastly, and perhaps the murkiest, the use of genetic data for **research purposes**. Important medical benefits may be obtained by profit-motivated uses of genetic data, and involve improper research purposes and protocols that benefit medical innovation while placing data subjects at risk for stigmatization and privacy violations.

2.1 Misuse of DNA in forensic services: the Parabon case

In some cases, DNA data collected for specifically consented purposes (i.e., a DNA genealogical analysis) may be required by **law enforcement**. Therefore, DNA banks may have to adapt the conditions for data processing to fulfill reasons of public interest related to a **criminal investigation**. First, however, the controller may need to establish the purpose of reuse and whether it is "authorized by law", either under national regulation or a statutory code. In this sense, it may be necessary to prioritize the use of the DNA data to search for criminal suspects, or even the search for relatives based on a Courts' request (Tillmar et al., 2021).

An example of misuse of the above approach can be found in the **1986 Nancy Daugherty assassination case** (Turtinen, 2020). The Chisholm Police Department, in cooperation with Parabon NanoLabs, a private company based in the state of Virginia, examined two databases storing data from people whose genetic information was disclosed without a warrant or informed consent to identify the suspect. Court documents reveal that **Parabon** was provided with **a sample of the suspect's DNA from the crime scene,** and the lab used genetic phenotyping as well as genetic genealogy analysis, which involves identifying potential relatives and building family trees through commercially available genetic databases. The investigation linked the sample to Michael Allan Carbo Jr., 53, who was charged with the rape and killing of 38-year-old Nancy Daugherty.

Parabon tests found matches in its databases, which the company used to develop an **extensive family tree** of the DNA sample and "hypothesizing" Carbo as the source. The Chisholm police and the Minnesota Bureau of Criminal

Apprehension then began pursuing him as a suspect, obtaining DNA samples from Carbo's garbage and, later on, from him directly.

This process may violate Minnesota law and the state and federal constitutions. The Minnesota Bureau of Criminal Apprehension has pointed out there are no previous cases solved through Parabon services, but that using Parabon for criminal investigation purposes **raises constitutional and privacy concerns** without precedence in the Minnesota judicial system. Although prosecutors have claimed that the company merely provided a "lead" for investigators to follow, the Carbo defense has argued that Parabon employees were **illegally engaged in law enforcement work**. Although a judge later dismissed constitutional challenges to the investigation, the process represents an expansive understanding of the potential use of private DNA databases for law enforcement purposes and questions the principle of informed consent concerning affected DNA bank users.

2.2 The adoption of Carrie Reynolds: privacy and ethical implications

The chance of finding a relative via a search of an existing DNA database is minimal (Baffer, 2019). Thus, the claims of commercial DNA databases that there is a fair chance that users will be able to identify a relative are often exaggerated. Instead, it is **more feasible to test for a match in known relationships**, for instance, when an adopted person already has a concrete clue of who their family is, or where they live. Then, if one or more people from a particular village are willing to submit their DNA, it could be proven with a 99.99% probability that the adopted person originally is from that village. In these cases, the matching person/group is already known. The same procedure can also be applied to trace anonymous sperm donors.

Adoptees often use DTC testing to "create an identity" based on biological, familial data. However, even in cases where testing does provide the correct answers to users, other concerns need to be considered. Among other ethical implications, it is crucial to evaluate the balance between the adoptee's right to know their parentage and the **parent's right to protect their own privacy** (Darroch and Smith, 2021).

The **case of Carrie Reynolds** helps illustrate this point. Reynolds was born in 1975 in Ponte Vedra Beach, Florida and adopted. In 2018, she decided to get a genetic testing kit from AncestryDNA, provided a saliva sample, and sent it for processing. Results revealed information about her Irish, Scottish, and Swedish roots.

She also **discovered two half-siblings** she had not previously known about. When Reynolds contacted one of them, Mark, through the Ancestry's system, she found he was also an adoptee. They worked together to **identify their biological parents** and discovered a third half-sibling in the Ancestry system, who provided information about her birth father. However, when Reynolds finally met her biological father after the process of DTC DNA analysis and he, in turn, provided information about her birth mother, she did not receive any answer from her. Even

though Reynolds was disappointed, she decided to focus on the fact that her adoptive parents were her actual parents and pointed out, "*My family is my family, no matter what the DNA says*" (Mertz Esswein, _2019). While it is not possible to know the reasons for Reynolds's mother not getting in contact with her, this case embodies another side of the ethical and privacy issue behind DTC and its potential consequences.

2.3 Research activities and DTC genetic testing: the case of MGC

In 2019, a data breach at the neurology department of Massachusetts General Hospital (MGC) **risked the genetic data of nearly 10,000 people**. This breach was not the hospital's first, after an earlier employee mishandling of data had already exposed the names, lab results and Social Security numbers of 648 patients. Research organizations, **often collaborating with DTC DNA banks in pursuing joint research on genetics**, have a responsibility to maintain the privacy of individually identifiable health information and should implement proper standards for the security of patients' information and policies and procedures to manage data breaches. A privacy-promoting framework is subject to issues of the fairness of using personal genetic information, the potential impact that it will have on the data subjects, and internal privacy measures to ensure that each person that handles the information understands the degree of responsibility they have to their data subjects.

These can be observed in two main ways:

a. *Legal and Regulatory Framework on research activities involving genetic data*

Several regulatory frameworks exist to protect data subjects from unlawful disclosures and misuses of their genetic data and afford them legal protection over their data. The AU Convention on Cyber Security and Personal Data Protection explicitly mentions genetic data as a form of health data, which are a type of sensitive personal data (Article 1). The Convention stipulates, among others, that processing personal data involving genetic information and health research is one of the actions that require prior authorization by the national protection authority (Article 10.4). The UNESCO Universal Declaration on the Human Genome and Human Rights Article 5(c) and UNESCO International Declaration on Human Genetic Data Article 10 addresses the **right to decide whether to be informed about research results**. From the UNESCO International Declaration on Human Genetic Data Article 10, it follows that in case of medical genetic testing, "*the information provided at the time of consent should indicate that the person concerned has the right to decide whether or not to be informed of the results*." However, this approach is not entirely reflected in the public documents for informed consent published by MGH.

b. *Ethical concerns surrounding research activities in genetic data*

Some research activities can be framed in a way that **stigmatizes genetic traits and conditions** and ultimately, since the subjects cannot control the messaging,

they can be made to feel stigmatized. Additionally, it makes individuals with rare genetic markers more likely to be de-identified which makes them **more vulnerable** than they ordinarily would have been. In the case of the MGH data breach, data subjects were exposed not only to unlawful disclosures but also to endure the emotional and psychological effects of having their personal health data exposed without their permission.

2.4 Identified legal and ethical implications

Commercial DNA databases are interested in having **as many DNA profiles as possible**. Of course, clients always have to share their DNA profiles before they can employ the services of the DNA database. Most DNA databases apply a neat opt-in approach by default. This means that their profiles are only stored with the client's explicit consent. Of course, whether they actually remove the profile when a customer opts out depends on each Bank's legal basis for processing and consent. Most commercial DNA databases indicate in their privacy policies and contracts that they indeed remove the data lawfully. However, usages and retention periods are multiple, each data processing goal has its own policy, and not all users carefully read or can understand them.

In this scenario, the **case studies illustrate several ethical dilemmas** and legal issues related to the broader effects of an opt-in. If someone opts-in for their DNA profile, they, de facto, opt-in for all their close relatives – probably without them being aware of it. Finding a user's relative, when that relative is unaware of the behavioral or criminal record or DNA storage taking place in a large commercial Bank can lead to problematic legal and/or psychological conflicts. For example, the case where a person's participation in a DNA testing database led to their family member's arrest. Moreover, the potential of the legal requirement to collaborate with law enforcement and other data processing potentially leading to function creep[1] should be considered. These issues reveal the potential implications of using DTC private tests for health diagnoses or ancestry discovery purposes, the need for taking precautions in data sharing, including an in-depth analysis of banks' data processing purposes and conditions, and getting certified genetic counseling (Matloff, 2018).

[1] Following the OIPC, ""Function creep" occurs when information is used for a purpose that is not the original specified purpose."

3. RANKING DNA BANKS

To **provide an actionable framework** for those who are interested in using these services, we will offer an overview of six major international DNA databases:

- Ancestry, US, 21 million DNA profiles
- 23andMe, US, 12 million profiles
- MyHeritage, Israel, 6 million profiles
- FamilyTreeDNA, US, 2 million profiles
- GEDmatch, US, 2 million profiles
- Living DNA, UK, 0.3 million profiles

While **green boxes** correspond to variables confirmed or made explicit by each DNA Bank, **yellow ones** represent those for which there is a negative correlation or no reference to the element is made in Banks' public documents. **Limitations concerning lack of direct access to data** should therefore be considered and results are taken as general guidance open to interpretation.

Data management

Variables	Ancestry	23andMe	FamilyTreeDNA	Living DNA	MyHeritage[2]	GEDmatch
Adherence to standards - ISO/IEC 27001						
Third parties, outside the controller, are given access to DNA processing						
Full data deletion protocols (including both samples and other personal data) are in place						

[2] In the process of certification for ISO/IEC 27001.

Data sharing policies

Variables	Ancestry	23andMe[3]	FamilyTreeDNA	Living DNA	MyHeritage	GEDmatch
Provision of an exhaustive list of third parties who will receive the data						
Voluntarily cooperates with Law Enforcement						
The DNA bank will notify the data subjects when it receives a request for access to the information from law enforcement						

Your rights vs Their terms

Variables	Ancestry	23andMe[4]	FamilyTreeDNA	Living DNA	MyHeritage	GEDmatch
Complete record of information obtained during the data collection process is offered to users						
Data affirmed as belonging to the data subject						
The possibility to opt-in or opt-out of each intended use						
External and internal uses of the data fully disclosed						
Access raw genomic data by users is possible						

3.1 Ranking and final remarks

All studied DNA banks **follow basic standard policies concerning data protection**, such as ensuring users' rights to access, rectification and cancellation of their personal data. However, as we can see, differences can be found

[3] It should be noted that 23andMe provides a list of categories of recipients of the personal data (Article 13(1)(e) https://research.23andme.com/projects/#collab

[4] 23&Me still indicates that it does not sell Personal Information and indicates that it obtains consent for EU customers for marketing purposes.

concerning their capacity to provide information or enable other relevant policies. Following the above, we rank the six Banks in the following manner:

DNA bank by position (GREEN cases)	Million PROFILES and country
1. MyHeritage (9)	6 million, Israel
2. Ancestry (8)	**21 million, US**
3. FamilyTreeDNA (8)	2 million, US
4. Living DNA (7)	0.3 million, UK
5. 23andMe (6)	12 million, US
6. GEDmatch (3)	2 million, US

Based on our positive answers, we could consider that **Ancestry is the better-positioned DNA bank** since it combines high standards concerning data management, protection and rights provision with a high capacity to provide profiles for matching. However, a **proper case-by-case qualitative analysis** must be conducted when assessing the possibility of using these services. You should inform yourself about notable service providers' events before deciding where to submit a DNA sample. For instance, possible breaches of the purpose limitation principle have been denounced in the case of 23andMe. Therefore, you should combine a careful study of providers' Terms and Conditions with an updated analysis of the intended bank's performance in protecting users' data without losing sight of the importance of genetic counseling.

ACKNOWLEDGEMENTS

Project team: EU Project Team
Project Lead & Research Director: Dr. Gemma Galdon-Clavell, Founder of Eticas Foundation
Writer and Researcher:

- Martín Zamorano, Senior Ethics and Technology Researcher at Eticas
- Matteo Mastracci, Ethics and Technology Researcher at Eticas

REFERENCES

Almeling, R. & Gadarian, S. (2014), 'Public opinion on policy issues in genetics and genomics,' *Genetics in Medicine* , 16, 6, pp. 491–494. https://doi.org/10.1038/gim.2013.175

Annas, G. J. (2006). DNA testing, banking, and genetic privacy. *New England Journal of Medicine*, 355, 545.

Baffer, B. (2019). Closed Adoption: An Illusory Promise to Birth Parents and the Changing Landscape of Sealed Adoption Records. *Cath. UJL & Tech*, *28*, 147.

Broady, K. M.; Ormond, K. E.; Topol, E. J.; Schork, N. J. & Bloss, C. S. (2018), 'Predictors of adverse psychological experiences surrounding genome-wide profiling for disease risk,' Journal of Community Genetics, vol. 9, no. 3, pp. 217– 225.

Darroch, F., & Smith, I. (2021). Establishing Identity: How Direct-to-Consumer Genetic Testing Challenges the Assumption of Donor Anonymity. *Family Court Review*, *59*(1), 103-120.

ECHR (2022). *Guide to the Case-Law of the European Court of Human Rights. Data protection*. Council of Europe.

Edge, M. D., & Coop, G. (2020). Attacks on genetic privacy via uploads to genealogical databases. *Elife*, *9*, e51810.

Eisenhauer, E. R., Tait, A. R., Rieh, S. Y., & Arslanian-Engoren, C. M. (2019). Participants' understanding of informed consent for biobanking: A systematic review. *Clinical Nursing Research*, *28*(1), 30-51.

Farahani, Fereshteh Shahrabi (2022). "Ethical Concerns of Direct-to-Consumer Genetic Tests" *TalTech Journal of European Studies*, 12, 1, 2022, 145-158.

Gabel JD, Wilkinson MD. (2008). Good science gone bad: how the criminal justice system can redress the impact of flawed forensics. *Hastings Law J*;59:1001–30.

Garner, S. A., & Kim, J. (2018). The privacy risks of direct-to-consumer genetic testing: a case study of 23andMe and Ancestry. *Wash. UL Rev.*, *96*, 1219.

Grosse, S. D.; Kalman, L. & Khoury, M. J. (2010), 'Evaluation of the validity and utility of genetic testing for rare diseases,' *Advances in Experimental Medicine and Biology,* vol. 686, pp. 115–131.

Horton R, Crawford G, Freeman L, Fenwick A, Wright C F, Lucassen A et al. (2019). Direct-to-consumer genetic testing *BMJ*; 367.

Matloff, Ellen (2018). *If I'm Adopted, Should I Have DNA Testing?*, Forbes. Available at https://www.forbes.com/sites/ellenmatloff/2018/07/11/im-adopted-should-i-have-dna-testing/?sh=5a8b0340e029

May, T. (2018). Sociogenetic risks–ancestry DNA testing, third-party identity, and protection of privacy. *New England Journal of Medicine* , 379(5), 410-412.

Mertz Esswein, Patricia (2019). *Discover Your Roots With DNA Testing*. Kiplinger. Available at: https://www.kiplinger.com/article/spending/t065-c000-s002-discover-your-roots-with-dna-testing.html

Narayanasamy S, Markina V, Thorogood A, Blazkova A, Shabani M, Knoppers BM, Prainsack B, Koesters R. (2020). Genomic Sequencing Capacity, Data Retention, and Personal Access to Raw Data in Europe. *Front Genet.* 6;11:303.

Oh B. (2019). Direct-to-consumer genetic testing: advantages and pitfalls. *Genomics Inform.* 17(3):e33.

Peterson, S. K. (2005), 'The role of the family in genetic testing: Theoretical perspectives, current knowledge, and future directions,' *Health Education & Behaviour,* 32, 5, 627–639.

Regalado, Antonio (2019). *Biotechnology. More than 26 million people have taken an at-home ancestry test. The genetic genie is out of the bottle. And it's not going back*. MIT. Available at https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/

Spiers, C. (2022). Keeping It in the Family: Direct-to-Consumer Genetic Testing and the Fourth Amendment. *Houston Law Review*, *59*(5), 1205-1229.

Takai-Igarashi, T., Kinoshita, K., Nagasaki, M., Ogishima, S., Nakamura, N., Nagase, S., ... & Yamamoto, M. (2017). Security controls in an integrated Biobank to protect privacy in data sharing: rationale and study design. *BMC medical informatics and decision making,* 17(1), 1-12.

Tillmar A, Fagerholm SA, Staaf J, Sjölund P, Ansell R. (2021). Getting the conclusive lead with investigative genetic genealogy - A successful case study of a 16 year old double murder in Sweden. *Forensic Sci Int Genet*.;53:102525.

Turtinen, Melissa (2020).*Chisholm man charged in 1986 cold case after DNA breakthrough*. Bring me the news. Available at: https://bringmethenews.com/minnesota-news/chisholm-man-charged-in-1986-cold-case-after-dna-breakthrough

Walsh S, Bright J, Buckleton J. (2016). *DNA Intelligence Databases: Forensic DNA Evidence Interpretation*. Boca Raton: CRC Press.