

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

SIMONE MAGAARD<sup>1</sup>

DANIEL MARKUS<sup>2</sup>

ANN-SOFIE KLARELD<sup>3</sup>

# Genomic privacy? Direct-to-consumer genetic testing companies and the processing of sensitive personal data

---

1 Simone Magaard received her master's degree in archival science from Lund University in 2021 and has been working as an archivist since. Currently she works for the Region Skåne archives.

Email: [simone\\_magaard@hotmail.com](mailto:simone_magaard@hotmail.com)

2 Daniel Markus received his master's degree in archival science from Lund University in 2021. Today he is working as an archivist for the Swedish municipal administrative authority VA SYD.

Email: [daniel\\_markus@hotmail.com](mailto:daniel_markus@hotmail.com)

3 Ann-Sofie Klareld is a senior lecturer at the Department of Arts and Cultural Sciences, Lund University. She has a PhD in Archives and Information Science from Mid Sweden University. Klareld teaches at the Master's Programme in Archival Studies, Library and Information Studies, Museum Studies (ALM). Her current research interests include archives in society, the professional role of archivists, and contemporary family history.

Email: [ann-sofie.klareld@kultur.lu.se](mailto:ann-sofie.klareld@kultur.lu.se)

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

**Abstract:** This paper explores the processing of sensitive personal data for genealogical purposes by studying how the privacy policies of three direct-to-consumer genetic testing companies comply with the General Data Protection Regulation (GDPR). The methodological approach is content analysis. The privacy policies are analysed in relation to the three core principles of 1) adherence to GDPR; 2) transparent processing of personal data; and 3) consent. The paper also discusses privacy in relation to third parties whose sensitive personal data is processed indirectly due to the nature of DNA as shared between family members. The main result is that the privacy policies rarely mention GDPR; when mentioned it is done in a brief way; the privacy policies studied convey insufficient transparency as regards data processing; and the current legal framework does not suffice to protect the privacy of genetic relatives of users whose personal data is being processed indirectly.

**Keywords:** personal data, privacy, genetic data, GDPR, genealogy

## Introduction

Direct-to-consumer genetic testing (DTCGT) are DNA-testing products that consumers can purchase over the counter or online. DTCGT is a rapidly growing industry developed alongside advances in genetic and genomic science, arguably transforming family history by enabling genetic genealogy (Stallard & De Groot, 2020). Genetic data warrants a high standard of privacy protection since 1) it may be used to identify predispositions, disease risk, and predict future medical conditions; 2) it may reveal information about the individual's family members, including future children; 3) it may contain unexpected information or information of which the full impact may not be understood at the time of collection; and 4) it may have cultural significance for groups or individuals (Future of Privacy Forum, 2018). The General Data Protection Regulation (GDPR) prohibits processing genetic and biometric data with several exceptions, including when “the data subject has given explicit consent to the processing of those personal data for one or more specified purposes”, and when “processing relates to personal data which are manifestly made public by the data subject” (GDPR, 2016, Article 9).

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

DTCGT companies do try to avoid, to a reasonable extent, health informative markers and privacy policies exist to ensure that consumers can make informed decisions. However, researchers have raised concern regarding transparency related to confidentiality, privacy, and secondary use of data (Howard, Knoppers & Borry, 2020), compliance with international guidelines (Laestadius, Rich & Auer, 2017), and information provided to third parties (Wallace et al, 2015). A recent Swedish report indicated problems concerning one DTCGT company's' privacy policy and their terms and conditions by concluding "a number of the terms that Swedish consumers agree to should be considered unreasonable" (Swedish Consumers' Association, 2020, our translation).

On the basis of international research pointing to problems with privacy policies in general and the Swedish Consumers' Association pointing to specific problems regarding one DTCGT company operating in Sweden, this paper explores the privacy policies of three DTCGT companies offering their products and services to Swedish customers. The privacy policies are read in relation to GDPR, and their implications are discussed in relation to personal integrity. Note that the paper does not claim to assess the industry as a whole, nor point out any company as 'worse' than any other. It does, however, take a critical standpoint as the guiding principle, discussing privacy protection in general and sensitive personal data in particular.<sup>4</sup>

## Aim and purpose

The paper contributes to the field of research that concerns the tensions between sensitive personal data, law, and new technical possibilities. Our purpose is to explore and problematize what three selected DTCGT companies say in their privacy policies about their processing of genetic personal data, and discuss the limitations of the legal

---

<sup>4</sup> The concepts used in the paper are defined according to GDPR, Chapter 1, article 4.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

framework in relation to the nature of DNA as shared between different individuals. The research questions are:

1. How do the three companies' privacy policies comply with the General Data Protection Regulation?
2. What are the limitations of the current legal framework when considering the nature of genetic data as shared between individuals?

## Background

GDPR came into force in 2018 with the aim to protect citizen's integrity. Provisions existed previously in extant European Data Protection Law under an EU Directive (95/46/EC). GDPR asserts that "the protection of natural persons in relation to the processing of personal data is a fundamental right" (GDPR, 2016). It includes definitions of what personal data is, and how this data may be processed. The main principle is that natural persons are to have control over their own personal data, and that sensitive data merit specific protection. GDPR applies both when the entity processing the personal data is established within the EU and when an entity outside the EU offers goods and services to people within the Union, even if the data are being stored or used outside of the EU. Consequently, GDPR has had a significant influence on privacy and data protection law worldwide (Phillips, 2019, Zaeem & Barber, 2020). GDPR applies in principle to every kind of operation and activity and regardless of who carries out the processing. Thus, while none of the companies in focus of the present paper are EU entities, they are still obliged to follow GDPR.

Technological development, having "transformed both the economy and social life", is stated as the main reason why GDPR was created (GDPR, 2016). DNA analysis combined with digital data processing is an example of such transformative technology. As King puts it, "DTCGT represents a new frontier in the collection of personal information" (King, 2019, p. 2).

Commercial DNA-testing has been used since the 1980s to assist with criminal investigations (Aronson, 2007) and determine familial relations (Cole, 2001). Today, tests are advertised for a variety of purposes, including genealogy. Like traditional records, the results need to be interpreted and evaluated regarding accuracy and significance

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

(Donovan, Pasquetto & Pierre, 2018). Taking a DNA-test does not automatically reveal all one wishes to know about familial relations, and it can take a lot of time and effort to, for example, find the genetic grandfather one is looking for (Classon, 2019). Nevertheless, the advent of DNA testing has undeniably opened up a new information resource for genealogists to explore. According to Stevens, “DNA sequencing machines are computerised instruments that produce DNA as bits and bytes. In this sense, a human genome sequence is already a new media object – it is born online, to be stored in databases and transmitted across the Internet” (Stevens, 2015, p. 394).

The DTCGT companies’ value lie in providing a platform through which users can exchange information and utilise the logic of crowdsourcing when they organise and make accessible large volumes of data. Opting in to make yourself searchable and available for matching with others is a prerequisite for using the test result to its fullest extent. The privacy policies that users need to approve before using the services that DTCGT-companies provide should convey clear appreciation and understanding of all relevant facts, implications, and consequences. However, a recent case indicates that these requirements are not always met. In 2020, the Swedish Consumers Association (SCA), reported MyHeritage to the Swedish Authority for Privacy Protection. A review of MyHeritage’s contract terms, concluded that the terms and conditions were unreasonable, violated the 3 § of the Swedish Contract Terms Act (SFS, 1994:1512), and did not follow GDPR (Swedish Consumers’ Association, 2020). SCA said it was almost impossible for consumers to understand the terms and conditions, including the privacy policy; that the texts were too long and contained difficult words and concepts normally only used by lawyers and researchers within the field of medicine; that the terms and conditions as well as the privacy policy contained misleading wording and disclaimers; that the English and the Swedish versions did not correspond; and that the company was careless with personal data. MyHeritage also demanded that users waive the right to a trial in Sweden, insisting that consumers would not have the right to report the company anywhere but Israel, where the head office was located. According to MyHeritage’s contract terms, it would therefore be impossible to bring a lawsuit against the company in Swedish court. In an email to SVT

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

Nyheter [Swedish Television News] MyHeritage responded briefly to some of the criticisms levelled at them, announcing that they had never shared personal data with third parties and that they were working to produce clearer agreements (Sveriges Television, 2020).

The example above points to a reason why DTCGT companies do not follow GDPR, namely that their business stem from and operate within other legislations that are not compatible with GDPR. Nevertheless, any person or entity operating within the EU should, according to GDPR, adapt their processing of personal data to the principles and rules established in the regulation.

## Related research

Zaeem & Barber (2020) attempted to quantify how GDPR had improved privacy policies around the globe. Their findings indicated that though some progress had been made, more was necessary. Noncompliance often occurred “in the form of failing to explicitly indicate compliance, which in turn speaks to an organization’s lack of transparency and disclosure regarding their processing and protection of personal information” (Zaeem & Barber, 2020, p. 1). Similar problems have been shown in studies that focus on other legal frameworks than GDPR. In a study focusing on the differing legal frameworks of England, Wales, Germany, and South Korea, Lee found that though the laws were different the problems of how genetic data could be used was very similar, suggesting that clearer guidelines are needed to balance the use of DNA technology with the laws (Lee, 2016). In a study focusing on federal statutes and regulations in the USA, Wright Clayton et al. criticised the existing juridical framework, arguing that “it has been difficult to develop broadly applicable legal principles for genetic privacy” and concluded that “few, if any, legal doctrines or enactments provide accurate protection or meaningful control to individuals over disclosures that may affect them” (Wright Clayton et al., 2019, p. 1). Phillips reviewed contracts of 71 DTCGT companies that provide tests for health purposes, concluding that it was questionable if the contracts were adequate to comply with UK law (Phillips, 2017 & 2019). Laestadius, Rich, & Auer (2017) assessed compliance with international transparency

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

guidelines concluding that these were not consistently met in relation to transparency, privacy, and secondary use of data. Stevens examined the interdependence between biotechnology and new media in the development of DTCGT companies, maintaining that the Web “allows genetic testing services to operate within an ambiguous regulatory framework” (Stevens, 2015, p. 395).

Noncompliance and legal ambiguity are however not the only problems - research on online contracts and wrap agreements show that users might not read them due to their length and to their rate of recurrence in the online environment (Obar & Oeldorf-Hirsch, 2020), and that even when reading privacy policies, there is “a significant level of misunderstanding on the part of consumers” on their meaning and effect (Phillips, 2015a, p. 72). In relation to DTCGT, Phillips argued that privacy policies need to be “(...) more comprehensive and address the issues of data sharing, sale, storage, and security in much greater depth and explicitly draw consumers’ attention to companies’ privacy practice” (Phillips, 2015b, p. 63), and suggested that contracts could be improved by making them more interactive, drawing attention to key clauses, and offering more options to opt out of services (Phillips, 2015a, p. 73). Surveying privacy policies of 90 DTCGT companies operating in the USA, Hazel & Slobogin observed “tremendous variability across the DTCGT industry in the quantity and quality of information provided to consumers concerning the collection, use, and sharing of their genetic data” (Hazel & Slobogin, 2018, p. 66), and though the majority made vague references to potentially applicable laws in their policy documents, they provided little or no information regarding their scope or potential applicability to DTCGT. Benoliel & Becher conducted linguistic readability tests to the five hundred most popular websites in the United States that use sign-in-wrap agreements, arguing that “Whereas consumers are expected and presumed to read their contracts, suppliers do not generally have a duty to draft readable contracts” (Benoliel & Becher, 2019, p. 2256). Yet, despite the shortcomings of privacy policies, an interview study conducted by King (2019) indicated that users are prone to lack risk awareness, trust DTCGT companies with their sensitive data, and assume that anonymity will protect them from potential privacy harm.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

The use of DNA databases also creates several new ethical, legal, and integrity related challenges due to the possibility to reveal sensitive personal information about genetic relatives. Law enforcement agencies have been able to identify criminals by accessing databases managed by DTCGT companies. Often it is not a case of direct matches, but of using genetic data from relatives to hone in on a suspect. Thus, though an agreement between two parties – the DTCGT company and the user – might seem unproblematic it potentially affects other persons as well, regardless of them knowing about it. This is because, as Ram puts it, “genetic information is not like other forms of private or personal information because it is shared— immutably and involuntarily— in ways that are identifying of both the source and that person’s close genetic relatives” (Ram, 2015, p. 873). Extending this perspective to a societal level, King has argued that DTCGT “could be the final nail in the coffin of anonymity, as even those people who don’t have a traceable digital presence find themselves drawn into a genetic human map through their relatives” (King, 2019, p. 27). It has been argued that DNA technology needs to be complemented and limited with a better and clearer legal framework and that cooperation is required between companies, law enforcement, bioethicists and others involved to create a responsible use of people’s DNA (Kennett, 2019).

## Theory

This section provides a brief overview of privacy as a theoretical concept and its relation to genetic data which is the type of data we focus on specifically in this paper.

Privacy is a normative concept, inscribed in article 12 of the Universal declaration of human rights (United Nations, 1948). The right to privacy refers to “the ethical and legal principles that recognize the importance of limited access to an individual or information about an individual” (Wright Clayton et al., 2019, p. 5). According to GDPR, limiting access is a challenge due to “rapid technological developments and globalisation” which have brought new obstacles for the protection of personal data, not least due to the increased scale of data collection and sharing (GDPR, 2016, p. 2). Disclosure or misuse of personal data can negatively affect individuals’ relationships, reputation, employability,



## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

insurability, financial status, and more (Nissim & Wood, 2018).

Privacy was originally associated with secrecy or concealment, a “right to be let alone” (Warren & Brandeis, 1890, p. 193). The current understanding of privacy focuses more on privacy as a matter of control in relation to data privacy, “a personal right to control the use of one’s data” (Schwartz, 2000, p. 816). This “privacy control-paradigm”, Schwartz argues, is a “liberal autonomy principle” that places the individual at the centre of decision-making through “individual stewardship of personal data”, and “encourages a property approach to personal information that transforms data into a commodity” (ibid., p. 820). Personal data can even be described as the “currency of the Internet” (Zaeem & Barber, 2020, p. 17). GDPR fits into this paradigm as it is an attempt to balance the interest of businesses with the interest of the individual. Though GDPR revolves around information privacy, the concept of privacy is not used in the regulation. The individual is at the centre of the regulation, and is referred to as “data subject”, a term that occurs 406 times, or “natural person”, a term that occurs 131 times. Exchanges and flows of personal data are in GDPR connected to the proper functioning of the internal market - creating trust is described as essential to “allow the digital economy to develop” (GDPR, 2016).

There are different types of personal data and some are considered sensitive, such as genetic data, “personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question” (GDPR, 2016). Theoretically, a difference can be made between genetic material and the information rendered from analysing it, but these entities can also be seen as indistinguishable: De Witte and ten Have discussed the ownership of genetic material and information, maintaining that “On the level of scientific research there is hardly a distinction between genetic material and genetic information (genetic material is genetic information)” (De Witte & the Have, 1997, p. 58), and therefore: “With regard to genetic material and genetic information a reason to acknowledge ownership is not so much the possibility of selling genetic material and information, but the right to prevent others from having access to one’s genetic material and information” (Witte & ten Have, 1997, p. 57f). Wright

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

Clayton et al. also highlighted that the genome is “a uniquely individual assemblage of widely shared common elements” that “imbues it with a dual private and public significance that confounds any discussion of policy addressing genetic privacy” (Wright Clayton et al., 2019, p. 2). This complicates GDPRs’ notion of personal data as tied to and owned by one individual.

In the context of DTCGT the genome can be seen as an information resource or even a “book of life” (Kay, 2000) that people can explore to learn more about themselves and their familial relations. In their study about how DNA was used among attendees at DNA collection sessions in northern England, Scully, King & Brown (2013), conceptualised genetic code as “a form of archival memory” connected to narratives of identity, which in turn relate to macro narratives such as nationality, collective memory, and domesticity. According to Stevens, “DNA histories connect individual history (genealogy) to grand stories of human migration and exploration” and provide “powerful ways of forming group identities at a time when older narratives of identity (centred on nation, ethnicity, culture, and language) are being eroded” (Stevens, 2015, p. 391). DTCGT companies offer to give test takers insight into their genetic heritage on an aggregate level, and also on a more personal level tied to familial relations with other test-takers. However, once two test takers are connected, for example by revealing that they are half-siblings, the relationships to other family members, such as genetic parents, are also revealed - regardless of their consent or knowledge.

## Material and method

Our material consists of privacy policies from three selected DTCGT companies. To use the services that the companies provide, users must agree to two types of policy documents where one is the privacy policy, and the other is the terms and conditions. The choice to focus primarily on the first type is that this is where the companies describe what data they collect, how they process personal data, and how they adhere to GDPR. The companies were selected on the basis of a list compiled by the Swedish Society for Genetic Genealogy (SSGG) of the top companies active in Sweden. This association’s purpose was to support genealogists and

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

accelerate the use of DNA for genealogical purposes in Sweden and we thus regarded SSGG as a solid basis for knowledge about DTCGT companies operating in the country. Further, the companies chosen are not only known in genealogical circles but are household names that continuously expand their business not only in Sweden but also in other countries in the European Union and other parts of the globe. MyHeritage, an Israeli company founded in 2003, was in 2021 according to SSGG the company with the largest number of tested persons from Europe and among the more popular in Scandinavia. FamilyTreeDNA, founded in Texas in 2000 and in 2021 bought by the Australian company MyDNA, was according to SSGG was the company with the largest number of tested Swedes in 2021. Ancestry, founded in USA 1996, was in 2021 the largest company among the three. Their database had a preponderance of American history and genetic information which had proven especially useful for Swedes searching for emigrant ancestors (SSGG, 2020).

The versions of the privacy policies studied were from July 6, 2021 (MyHeritage), July 5, 2019 (FamilyTreeDNA), and August 3, 2021 (Ancestry). The amount of text ranged from about 5000 to 7000 words. The result was obtained through qualitative content analysis (Krippendorf, 2013), facilitating systematic reading and thematizing. The material was read repeatedly to acquire a good grasp of the whole. The units of analysis (Neuendorf 2017) selected were occasions where the privacy policies mentioned GDPR or explained how sensitive personal data was processed. Processing entails to collect, register, organise, preserve, change, read, transfer, spread, delete, or destroy data (IMY, 2021b). The occasions found were extracted, then sorted deductively according to the three principles of (i) adherence to GDPR, (ii) transparent processing of personal data, and (iii) consent. The material was also used to understand the problems of ensuring the privacy of genetic relatives of individuals using the services of DTCGT companies. To help interpret the privacy policies in relation to GDPR we used writings from the Swedish Authority for Privacy Protection ([Integritetsskyddsmyndigheten] IMY), designated by the Swedish government as the supervisory authority under GDPR (IMY, 2021a).

## Result and analysis

The GDPR principles informing the examination of the privacy policies are presented under the respective sub section below. The core of GDPR is that personal data should only be processed when there are good reasons for it – it must be justified why an organisation holds a collection of personal data, and controllers should weigh their own interests against those of the data subjects.

### ADHERENCE

It is not enough to state *that* GDPR is followed, it must be clear *how*. Controllers need to “demonstrate the compliance of processing activities with this Regulation” (GDPR, 2016, p. 14). This section is therefore guided by the question of how the companies show that they adhere to the principles of GDPR. The result shows that only one of the companies mention GDPR in their privacy policy.

Ancestry did not mention GDPR but said, “Under EU and UK law, we are required to specify the purposes for which we process your Personal Information and the legal bases which we rely on to do this”. The legal bases were accounted for in a separate document, where “Legitimate interests” was stated as the legal base to personalise, understand, maintain, develop, and improve Ancestrys’ services and to conduct scientific, statistical, and historical research on aggregated genetic information. What was meant by legitimate interests was not explained further than saying “Where we rely on legitimate interests to process your Personal Information, you have the right to object to such processing (meaning that you can ask us to stop). You can use your privacy settings to control certain ways in which we process your data”. Other legal bases found in the document seemed more straightforward, such as explicit consent (to undertake scientific research on biological samples), consent-device based permissions (to collect geolocation information from users’ devices), and compliance with legal obligations (to detect and defend against fraudulent, abusive, or unlawful activity).

FamilyTreeDNA did not mention GDPR either, instead they referred to Privacy Shield Framework, an agreement that they said allowed American companies to process personal data from Europe. However, in its judgement of 16 July 2020 (Case C-311/18), the Court of Justice of the European Union had ruled that the EU-US Privacy Shield

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

was no longer a valid mechanism to transfer personal data from the European Union to the United States. The annulment of Privacy Shield meant that personal data controllers in the EU were no longer allowed to transfer personal data to recipients in the US based on Privacy Shield. The European Commission and the US Government had started negotiations on a successor arrangement to the EU-US Privacy Shield to comply with the judgement of the Court. A possible explanation as to why this agreement was still in the privacy policy was that the latest update when the document was accessed was made in 2019. However, GDPR was already adopted by then. Thus, FamilyTreeDNA referred to an obsolete regulation.

MyHeritage said they had “taken steps to ensure compliance with all applicable privacy laws, including the general data protection regulation (GDPR)”. However, the Terms and conditions (2020) still asserted that: “This Agreement and any dispute regarding the Service shall be exclusively governed by the laws of the State of Israel, without regard to conflict of law provisions, and you agree that any legal proceeding about the execution, performance and/or enforcement of this Agreement shall be brought exclusively to the courts located in Tel Aviv, Israel.” In the privacy policy, under the heading “Legal grounds for the processing of personal information” MyHeritage aimed to explain their justification for processing personal data, which included when “the processing is in our legitimate commercial interests subject to your interests and fundamental rights”. What was meant by legitimate commercial interests or what basic rights consumers was not explicitly stated.

## TRANSPARENCY

This section focuses on linguistic clarity. GDPR says “any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used” (GDPR, 2016, p. 9).

The number of words in the privacy policies ranged from 5000 to 7000. Counting other referenced documents (terms and conditions, cookie policy, extended details on privacy preference) added 8500 - 15 500 words. Users thus needed to read a significant amount of text to grasp how

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

their data was being processed. All three companies stated that they might change their privacy policy at any time, requiring users to keep updated. A general problem was that the privacy policies did not offer a clear distinction between personal data and sensitive personal data. Another problem was that sweeping phrases – “for example”, “among other things”, “etcetera” – were used when explaining ways in which data was processed. All companies included disclaimers regarding data security, saying that while using reasonable efforts, they could not guarantee that loss, misuse, or alteration of data would not occur. All companies also said they disclosed personal information to third parties, and used personal data to develop new products and services.

Ancestry defined Personal Information as “information that can identify you directly or indirectly”; DNA data as “machine-readable biometric data”; and genetic information as “DNA data and any information derived from it such as ethnicity estimates, communities, traits, and genetic relative matches”. A 7-point bullet list was provided of the primary purposes for which Ancestry used genetic information, which included “studying aggregated genetic information to better understand population and ethnicity-related health, wellness, ageing, or physical conditions”, and to “conduct scientific, statistical, and historical research”. Ancestry emphasised that they only shared genetic information with selected third parties, including Ancestry Companies, other users, and service providers which would “have access to some of your information, including some of your Personal Information, in their systems”. It was highlighted that biological samples were not considered personal information and that users could request to have their biological samples destroyed.

FamilyTreeDNA defined personal information as “information that can help identify you”, and genetic information as “readable DNA Data”, which is converted to from extracted DNA. “Sensitive information” was a term used but not defined. FamilyTreeDNA said they used genetic information for purposes which “may include, in addition to other things not specifically mentioned” to “perform statistical, scientific, and historical research”. Third party service providers, not specified, would “have some of your information in their systems”. Aggregate information was defined as “Information that has been combined with that of

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

other users and analysed or assessed as a whole, such that no specific individual may be reasonably identified". It was unclear what reasonably meant. The possibility of being identified was mentioned in relation to pseudonymous information, of which it was stated: "Information that has been stripped of your Account Information and other identifying data, such that you cannot easily be identified as an individual to the public and is instead only identifiable by a kit number or other alphanumeric sequences." What was meant by easily identified remained unclear. GDPR does not apply to anonymous information. However, it states that "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly" (GDPR, 2016, p. 5).

MyHeritage did not define personal information other than exemplifying with "types of personal information", including "DNA information" of which it was said "DNA-related information is generated and stored when you use our DNA Services". A disclaimer stated "You acknowledge that you provide your personal information at your own risk". MyHeritage explained how they used personal data in a section which contained the most comprehensive information, but it was stated that the privacy policy should be read in conjunction with the Terms and Conditions. The privacy policy said, "We only collect information we believe is necessary for our legitimate business interests, to provide you with the Service". It was unclear what was meant by legitimate business interests. MyHeritage stated that they processed health related information not only of the data subject but also their family: "Before providing you with the DNA Health Reports, we collect certain self-reported family health history information from you, about you and your family members". This information was said to be required in the USA but collected from all users "for data consistency". The privacy policy did not require consent from family members before reporting their health history despite this being personal data that could be highly sensitive.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

### CONSENT

According to GDPR “Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her” (GDPR, 2016, p. 6). This can include ticking a box when visiting an internet website or choosing technical settings for information society services. If the controller intends to process the personal data for a purpose other than that for which they were collected, the controller “should provide the data subject prior to that further processing with information on that other purpose and other necessary information” (GDPR, 2016, p. 12).

All three privacy policies declared that by creating an account, users were confirming that they understood that the company would collect, process, and share the users’ personal data. Additional documents covered informed consent for research, of which it was stated that consent could be revoked at any time, unless the research had already occurred or was underway.

Ancestrys’ Informed consent for research covered “research that may be performed by AncestryDNA, a third-party researcher or in collaboration between AncestryDNA and a third-party researcher” (Ancestry, 2018) under the umbrella of Ancestry Human Diversity Project, which covered a broad spectrum of research related to the study of human genetics, genealogy, anthropology, and health. The research agreed to could be performed by employees of AncestryDNA, as well as “researchers from other organisations and companies who share our Purpose. This might include academic institutions as well as non-profit and for-profit businesses or government agencies”. This statement is problematic since consent should be given only for specific purposes. Potential research participants are to be given information about the key elements of a research study and what their participation will involve. Ancestry’s informed consent seemed to be much broader. The consent covered the use of “all data that you provide to us when you use our Services, including Biological Samples and any data derived from those samples”. Self-reported health and trait data may include information about family members that had not given their consent since it consisted of “lifestyle or other traits of you and your family members”.



## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

FamilyTreeDNAs' privacy policy said DNA samples were stored "so that they can be attainable for future testing", if the data subject had agreed to it. FamilyTreeDNA said one of the primary purposes for which users' genetic information was processed was to "perform statistical, scientific, and historical research", but that the company would not share users' personal information with third parties without additional consent "before we collect and process Sensitive Information as part of your interaction with the Services". However, it was unclear what was meant by Sensitive Information and how this related to what was defined as genetic information or DNA data. FamilyTreeDNA described their consent process for research as "Users wishing to participate in genetic research projects may indicate so and will be included in a candidate pool. If you become a potential candidate for a research project, you will be contacted to grant specific consent for every individual research project opportunity".

MyHeritage's privacy policy said, "special category data or sensitive personal data is processed on your explicit consent", and that "If you voluntarily agreed to the DNA Informed consent we may use your information (such as DNA Results and other DNA Information) for the purposes of research as specified therein". Their document DNA Informed Consent — MyHeritage DNA Research Project (2021) explained that The MyHeritage DNA Research Project was "a program designed by MyHeritage to better understand human genetics, genealogy, and anthropology". Consent gave MyHeritage the right to use personal data in a broad scope: "research studies designed to further our understanding of genealogy, anthropology, cultures, human evolution and migration, human genetics, population genetics, epidemiology, population health issues, and regional health issues".

GDPR acknowledges that it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, why "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research" (GDPR, 2016, p. 6). Only FamilyTreeDNA said they would ask for additional consent in this way.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

“Data subject” is a concept used frequently in GDPR, mentioned 88 times, but not defined. We understand it as referring to the person who the personal data concerns. GDPR defines personal data as “any information relating to an identified or identifiable natural person” which in the context of DTCGT is the person who has taken a DNA test, but which may also, due to the nature of DNA as partially shared between individuals, extend to genetic relatives. In relation to DTCGT, the individual taking a DNA test can be seen both as a data subject, a consumer and as a part of the company’s assets since the business is based on people sharing their data with others. Sharing genetic data is however not limited to being a privacy risk for the person who has taken the test but also for genetic relatives. GDPR does not address this issue but is founded on the idea that my personal is mine alone to do with as I please. One of the privacy policies stated that the company “collect certain self-reported family health history information from you, about you and your family members” which from what we can understand would mean that the person reporting the health history of others thereby would become a data processor “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. This would require consent from concerned family members whose health data was being reported. Wallace et al. has suggested a “generational consent” model and recommended that “companies should make it clearer that clients should inform third parties about their plans to participate, that third parties’ data will be provided to companies, and that that data will be linked to other databases, thus raising privacy and issues on use of data” (Wallace et al, 2015, p. 1). However, which third parties that are concerned is not always clear from the start since there are differences between social family and genetic family, thus consent from a social relative might still breach the privacy of a genetic relative.

An immediate consequence for genetic relatives is that family relations are revealed in an unexpected and unwanted way. Theunissen found that “notions of family were frequently challenged with unexpected DNA test results causing shifts in personal and social identities, especially in their family and biological identities” (Theunissen, 2022, p. 1).

## Discussion and concluding remarks

The first research question was: How do the three companies' privacy policies comply with the General Data Protection Regulation? The result indicated three types of shortcomings in the companies' approach to the regulation:

- The privacy policies seldom mentioned GDPR. When mentioned, it was done briefly and in one case we found references to invalid international agreements. This conflicts with GDPR's requirement that "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation" (GDPR, 2016, Chapter IV Article 24).
- The privacy policies were often vague and even potentially misleading in their wording. The consequence was that users could not fully understand what personal data the companies collected or what would happen to the data. This conflicts with GDPR's requirement that information about data processing should be provided "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" (GDPR, 2016, Chapter III Article 12).
- All companies said they may change or update the terms without notice. This might undermine what the data subject had first agreed to and thus conflicts with GDPR's requirement that personal data should only be collected "for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (GDPR, 2016, Chapter II Article 5).

The second research question was: What are the limitations of the current legal framework when considering the nature of genetic data as shared between individuals? Given the shortcomings we were able to identify, one important point becomes clear:

- The privacy policies studied all make a distinction between genetic material and genetic data, as does GDPR: "Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question" (GDPR, 2016, Article 4). This

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

becomes problematic due to the nature of genetic data as partially shared, which has the consequence that sensitive data such as maternity or paternity can be revealed without consent of all concerned parties. As De Witte & ten Have pointed out it is even problematic to talk of genes as parts of an individual person's body since "is not specific for an individual but refers to a pedigree; similar material is shared with relatives and genes as physical entities are in fact common to all people" (De Witte & the Have, 1997, p. 58).

In sum, we found that there was not always a clear difference between what GDPR says about how personal data should be processed and how the companies said they processed personal data. The problems appeared between the lines – in unclear formulations and inaccessible language, in translated versions of the privacy policies that were not legally binding, in seemingly trivial settings that could have far-reaching consequences, and in conditions that could be changed at any time. Thus, it was a challenge to specify the risks that the privacy policies had in relation to privacy and applicable law. However, we could estimate a few problematic features.

The first relates to the relationship between law and technical development. The services DTCGT companies offer are historically unprecedented. Genealogy and family history are not new phenomena, but the possibility to turn to genetics to the extent done today is based on methods developed in a relatively short time where it is unclear if juridical frameworks have kept up. This is not to say that genealogy based on traditional records or oral narrations is unproblematic. However, contemporary genealogy done by analysing and sharing genetic information increases the privacy risks, both for the individual tested and for their genetic relatives. In one case the company asked users to provide family health history information about not only the user but also about the user's family members, which adds to the privacy risks of people who are not customers.

We also found a lack of a coherent account of what sensitive personal data that the companies processed. Often there were hints as to what type of personal data the privacy policies referred to, but these hints were scattered across the text under different headings. An adjacent problem was that in the two cases where the privacy policies were translated to

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.

Department of ALM, Uppsala University.

Swedish, the companies stated that the translation was just for convenience, and that only the English version is legally binding. Not all users have the linguistic skills to read English. The companies place much responsibility on the user. This is also relevant in relation to consent. To give consent, the user must understand the privacy policy. Small and seemingly insignificant setting options at the web pages of companies can lead to large consequences for the user. For example, how personal data can be received or shared via the user's profile to others. These settings also hold the potential to have consequences for genetic relatives that have not given their consent to having their data processed. The offer that services can be customised might be problematic since it is difficult for the individual to comprehend the consequences of all settings made. It is hard to predict solely based on the privacy policies how the data will be processed in the future and which consequences that may follow. Our results confirm King's conclusion that "the collective identification presented by DTCGT takes the challenge of managing collective privacy to a new level while also raising critical questions of consent" (King 2019, p. 26). More knowledge is needed about how to handle privacy of genetic relatives in cases where individuals provide genetic data to DTCGT companies. Future research could investigate what specific privacy consequences DNA testing has had for genetic relatives of customers using the services of DTCGT companies, and how the legal framework could be adapted to respond to the development of commercial services based on new advances in genomic and digital technology.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

## References

- Ancestry. *Your privacy*. Effective Date: 3 Aug 2021. Accessed 2021-09-20 from <https://www.ancestry.com/cs/legal/privacystatement>
- Ancestry. *AncestryDNA Informed Consent*. Effective Date: July 24, 2018. Accessed 2022-01-10 from <https://www.ancestry.com/dna/lp/informedconsent-v4-en>
- Aronson, Jay D. (2007) *Genetic Witness: Science, Law, and Controversy in the Making of DNA Profiling*, Rutgers University Press.
- Benoliel, Uri, and Shmuel I. Becher (2019). "The Duty to Read the Unreadable." *Boston College Law Review* 60, no. 8 (November 1, 2019): 2255–96.
- Clayton, Ellen Wright, Barbara J. Evans, James W. Hazel & Mark A. Rothstein (2019). "The Law of Genetic Privacy: Applications, Implications, and Limitations." *Journal of Law and the Biosciences* 6 (1): 1–36.
- Classon, Roland (2019). "Hon topsade sig - och fick en ny farfar" ["She swabbed her cheek - and got a new grandfather"]. *Sydsvenskan*. 19 december 2019. Accessed 2023-11-07 from <https://www.sydsvenskan.se/2019-12-19/hon-topsade-sig--och-fick-en-ny-farfar>
- Cole, Simon A. (2001) *Suspect identities : A history of fingerprinting and criminal identification*. Harvard university press.
- Court of Justice of the European Union (2020). *Judgement in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*.
- De Witte, Joke I. and Henk Ten Have (1997). "Ownership of Genetic Material and Information." *Social Science and Medicine* 45, no. 1: 51–60. doi:10.1016/S0277-9536(96)00309-7.
- Donovan, Joan, Irene Pasquetto & Jennifer Pierre (2018). "Cracking Open The Black Box of Genetic Ancestry Testing Technologies". *Proceedings of the 36th Annual Hawaii International Conference on System Science (HICSS)*.
- FamilyTreeDNA. *Privacy statement*. Last updated 05/07/2019. Accessed 2021-09-20 from <https://www.familytreedna.com/legal/privacy-statement>

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

FamilyTreeDNA. *Group Project Participation Informed Consent*. Effective as of June 5, (2018). Accessed 2022-01-10 from <https://www.familytreedna.com/legal/terms/group-project-participation>

Future of Privacy Forum. “Privacy best practices for consumer genetic testing services”. (2018). [accessed 2022-03-29 from <https://fpf.org/blog/privacy-best-practices-for-consumer-genetic-testing-services/>]

Hazel, James W., and Christopher Slobogin (2018). “Who Knows What, and When: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies.” *Cornell Journal of Law and Public Policy* 28, no. 1 (January 1, 2018): 35–66.

Howard, Heidi C, Bartha Maria Knoppers, and Pascal Borry (2010). “Blurring Lines. The Research Activities of Direct-to-Consumer Genetic Testing Companies Raise Questions about Consumers as Research Subjects.” *EMBO Reports* 11, no. 8 (August 2010): 579–82. doi:10.1038/embor.2010.105.

Integritetsskyddsmyndigheten [Swedish Authority for Privacy Protection] *About us*. (2021a). Accessed 2021-02-20 from <https://www.imy.se/en/about-us/swedish-authority-for-privacy-protections-assignment/>

Integritetsskyddsmyndigheten [Swedish Authority for Privacy Protection]. *Detta är känsliga personuppgifter*. [This is sensitive personal data] (2021b). Accessed 2021-02-20 from <https://www.imy.se/lagar--regler/dataskyddsförordningen/kansliga-personuppgifter/detta-ar-kansliga-personuppgifter/>

Integritetsskyddsmyndigheten [Swedish Authority for Privacy Protection]. *Sanktionsavgifter och varningar*. [Sanction fees and warnings] (2021c). Accessed 2021-03-17 from <https://www.imy.se/om-oss/vart-uppdrag/sa-arbetar-vi-med-tillsyn/vad-kan-tillsynen-leda-till/>

Kay, Lily E. (2000) *Who Wrote the Book of Life?: A History of the Genetic Code*. Writing Science. Stanford University Press.

Kennett, Debbie (2019). “Using Genetic Genealogy Databases in Missing Persons Cases and to Develop Suspect Leads in Violent Crimes.” *Forensic Science International* 301 (August 1, 2019): 107–17. doi:10.1016/j.forsciint.2019.05.016.

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

- King, Jennifer (2019). "Becoming Part of Something Bigger : Direct to Consumer Genetic Testing, Privacy, and Personal Disclosure." *Proceedings of the ACM on Human-Computer Interaction*. 2019;3(CSCW):1-33. doi:10.1145/3359260
- Krippendorff, Klaus (2013). *Content analysis : An introduction to its methodology*. 3rd ed. SAGE.
- Laestadius, Linnea I., Jennifer R. Rich, and Paul L. Auer (2016). "All Your Data (Effectively) Belong to Us: Data Practices among Direct-to-Consumer Genetic Testing Firms." *Genetics in Medicine* 19, no. 5: 513–20. doi:10.1038/gim.2016.136.
- Lee, Jungnyum (2016). "The Presence and Future of the Use of DNA-Information and the Protection of Genetic Informational Privacy: A Comparative Perspective." *International Journal of Law, Crime and Justice* 44 (March 1, 2016): 212–29. doi:10.1016/j.ijlcj.2015.10.001.
- MyHeritage. *Terms and conditions*. Last updated on April 18, 2020. Accessed 2022-01-10 from <https://www.myheritage.se/terms-and-conditions>
- MyHeritage. *MyHeritage Privacy Policy*. Last updated July 6 2021. Accessed 2021-09-20 from <https://www.myheritage.se/FP/Company/popup-privacy-policy.php?dispLang=EN>
- MyHeritage. *DNA Informed Consent — MyHeritage DNA Research Project*. Updated on October 28, 2021. Accessed 2022-01-10 from <https://www.myheritage.mk/dna-informed-consent-agreement>
- Neuendorf, Kimberly A. (2017). *The Content Analysis Guidebook*. 2. ed. SAGE.
- Nissim, Kobbi & Wood, Alexandra (2018). "Is privacy privacy?" *Philosophical Transactions of the Royal Society A*. vol 376, issue 2128. <https://doi.org/10.1098/rsta.2017.0358>
- Obar, Jonathan A., and Anne Oeldorf-Hirsch (2020). "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 23, no. 1 (January 1, 2020): 128–47. doi:10.1080/1369118X.2018.1486870.



## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

Official Journal of the European Union (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 1995

Official Journal of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016

Phillips, Andelka M. (2015). "Think before You Click: Ordering a Genetic Test Online." *SciTech Lawyer* 11, no. 2 (January 1, 2015): 8–12.

Phillips, Andelka M. (2015). "Genomic Privacy and Direct-to-Consumer Genetics: Big Consumer Genetic Data - What's in That Contract?" *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 60–64. doi:10.1109/SPW.2015.19.

Phillips, Andelka M. (2019). *Buying Your Self on the Internet : Wrap Contracts and Personal Genomics*. Future Law. Edinburgh University Press, 2019.

Ram, Natalie (2015). "DNA by the Entirety." *Columbia Law Review* 115, no. 4 (May 1, 2015): 873–940.

Schwartz, Paul M. (2000). "Internet Privacy and the State." *Connecticut Law Review* 32, no. 3 (March 15, 2000): 815–60.

Stallard, Matthew and Jerome De Groot (2020). "'Things Are Coming Out That Are Questionable, We Never Knew About': DNA and the New Family History." *Journal of Family History* 45, no. 3: 274–94. doi:10.1177/0363199020906853.

Scully, Marc, Turi King and Steven D. Brown (2013). "Remediating Viking Origins: Genetic Code as Archival Memory of the Remote Past." *Sociology* 47, no. 5 (October 1, 2013): 921–38.

Stevens, Hallam (2015). "Genetimes and Lifetimes: DNA, New Media, and History." *Memory Studies* 8, no. 4: 390–406. doi:10.1177/1750698015581074.

Svenska Sällskapet för Genetisk Genealogi [Swedish Society for Genetic Genealogy], (2020). *Vilket test ska jag välja? [Which test*

## ARTICLE

Tidskrift för ABM | Vol. 8. No. 1, 2023.  
Department of ALM, Uppsala University.

*should I chose?]* Accessed 2021-09-08 from  
<http://ssgg.se/vilket-test-ska-jag-valja/>.

Sveriges Konsumenter [Swedish Consumers Association]  
(2020a). *Anmälan om oskäligen avtalsvillkor gällande DNA-tester från MyHeritage Ltd [Report on unreasonable terms and conditions relating to DNA tests from MyHeritage]* [2021-09-08].

Sveriges Konsumenter [Swedish Consumers Association]  
(2020b). *Vi anmäler MyHeritage för brott mot GDPR [We report MyHeritage for breach against GDPR]*  
[press release], 13 March 2020.

Sveriges Television [Swedish television] (2013). "Dna-testning anmäls för GDPR-brott" [DNA-testing reported for GDPR violation]. News article, *SVT Nyheter [Swedish Television News]*, April 13, 2020.

Swedish Code of Statutes. *Lag (1994:1512) om avtalsvillkor i konsumentförhållanden [Act (1994: 1512) on contract terms in consumer relations]*

Theunissen, Catherine Agnes (2022). "The Effects of DNA Test Results on Biological and Family Identities". *Genealogy*. 2022;6(17):17. doi:10.3390/genealogy6010017

United Nations (1948). *Universal declaration of human rights*.

Wallace, Susan E., Elli G. Gourn, Viktoriya Nikolova, and Nuala A. Sheehan (2015). "Family Tree and Ancestry Inference: Is There a Need for a 'Generational' Consent?" *BMC Medical Ethics* 16 (December 9, 2015): 1–9. doi:10.1186/s12910-015-0080-2.

Warren, Samuel D., and Louis D. Brandeis (1890). "The Right to Privacy." *Harvard Law Review* 4, no. 5 (December 15, 1890): 193–220. doi:10.2307/1321160.

Zaeem, Razieh Nokhbeh & Baber, Suzanne K. (2020). "The effect of the GDPR on privacy policies: Recent progress and future promise". *ACM Transactions on Management Information Systems*, Vol. 12, No. 1. <https://doi.org/10.1145/3389685>

Copyright: CC BY-NC-ND- 4.0

<https://creativecommons.org/licenses/by-nc-nd/4.0/>