KEEPING YOURSELF TO YOURSELF: GENETIC PRIVACY IN THE UNITED KINGDOM

SARAH HARROP AND CORINNE ATTON
WilmerHale, London

Introduction

Knowledge of our genetic make-up has grown exponentially over the last hundred years, paving the way for remarkable advances in science and medicine. Fifty years after the discovery of the structure of deoxyribonucleic acid (DNA), large-scale co-operation and significant advances in many fields of technology have enabled the identification of an increasing number of DNA-encoded (genetic) characteristics and disorders. We have now witnessed the sequencing of an entire human genome and new genes are being identified on a near daily basis. This, however, is only the beginning. Genetic information has the potential to impact on virtually every aspect of our lives. It is both empowering and at the same time a Pandora's box: we have seen its application in our criminal justice system and we are increasingly witnessing its effect on the availability of healthcare, employment and services such as insurance. These and further, as yet unknown, applications for genetic information will continue to present significant legal challenges.

This is the first of two articles that will consider the current legislative framework in both the United States and the United Kingdom and will ask whether it meets the challenges posed by the surge in the identification and availability of, genetic information. Are individuals sufficiently protected? Is the right balance being struck between the protection of the individual and the obtaining of benefit for society, particularly in the context of medical research? This first article will explore the nature of DNA and will consider the UK legislative framework.

The Nature of DNA

Genetic information is unique. It can be obtained from a very small amount of material, possibly without the consent of the owner, it is remarkably stable over very long periods of time and can be used for a wide and increasing variety of purposes. By way of example, it has the capacity to confirm family relationships, assist with reproductive choices, identify the presence of, or susceptibility to, various diseases, and enable a prediction of the effectiveness of various drugs and treatments. It is therefore, ideally suited to an increasing array of testing purposes, each of which may at present be undertaken on samples of blood, hair, bone, and other body tissues.

Genetic information, by its very nature, will always contain information specific to the individual from whom it was extracted. Indeed, it is this key connection with the individual that makes it such a rich subject for medical research, whether it is stored directly in medical records, or indirectly in, for example, DNA profiles (for example, forensic databases), family histories, population databanks (for example, genealogical databases), tissue samples, disease registries, adverse drug reaction databases, bio-banks (for example, to identify the factors contributing to common diseases) and, finally, bioinformatics databases. Moreover, increasingly complex and sophisticated technology means that this direct or indirect genetic information can now be exchanged electronically in seconds, for example between doctors and hospitals via the internet. This raises a number of important legal questions. Who retains control over the electronic storage of this information? What happens with information that is stored electronically and that then legitimately needs to leave a secure system? To what extent can (or should) the individual donors of genetic information control how it is used and disclosed?

UK Legislation

Genetic information is protected as 'personal data' in the United Kingdom by the Data Protection Act 1998 (which implements the European Community (EC) Data Protection Directive),[1] to the extent that it is possible to associate the genetic information, directly or indirectly, with a living individual. Given the unique nature of genetic information, this association will always be possible unless such information can be made anonymous (and whether it can be truly made anonymous is, as a matter of science, a moot point). Genetic information further falls to be protected as 'sensitive personal data', because it consists of, amongst other things, information as to an individual's health. Since genetic information, depending on the amount extracted, will

1) Directive 95/46 EC.

nearly always reveal information as to an individual's health and potentially other factors such as ethnicity, even if the DNA was not extracted for this purpose, it will, as a result, nearly always fall to be protected as 'sensitive personal data' and will therefore attract a higher degree of protection as will be explained below.

Rights and Principles

The UK Act sets out a compliance regime that must be observed by everyone who collects and processes genetic information in the United Kingdom. At the heart of the the UK regime are eight 'data protection principles'. These impose loosely worded obligations on everyone collecting and using genetic information (see table). These principles cover the fair and lawful processing of the information, the quality of the information, the rights of the individual in relation to the information, the security of the information, and, finally, the export of the information outside the European Union (EU).

Summary of Data Protection Principles

1.	Personal data shall be processed fairly and lawfully (and subject to certain pre- conditions).
2.	Personal data shall be obtained only for specified and lawful purposes, and shall not be processed in any manner incompatible with those purposes.
3.	Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.
4.	Personal data shall be accurate and, where necessary, kept up to date.
5.	Personal data processed for any purposes shall not be kept longer than is necessary for those purposes.
6.	Personal data shall be processed in accordance with the rights of data subjects.
7.	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8.	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The first principle provides the foundation on which the rest are built. It requires that genetic information must be treated in a fair and lawful manner and sets out certain pre-conditions on the collection and use of such information. In order for the collection and use of the information to be lawful, amongst other things, a formal notification must be made to the UK Information Commissioner. The Information Commissioner's Office ('the ICO') maintains a public register of organisations that process personal data. Indeed, a failure to notify the ICO can result in criminal charges. The first principle also sets out the minimum steps an organisation must take in order for the collection and use of the data to be fair. This is often referred to by the ICO as the fair processing code.

The next step is to comply with the pre-conditions before any processing of the information can occur. The most important of these in the context of medical research is that of obtaining the donor's consent. Consent in the context of non-sensitive personal data can be obtained in various ways and can be implied from the circumstances surrounding collection. Consent in the context of sensitive personal data such as genetic information must be explicit. In order for consent to be explicit, there needs to be a positive consensual action on the part of the donor of genetic information. (The distinction is important in the context of the limitations and exceptions below, where the requirement for 'explicit' consent is relaxed in some circumstances.)

The second principle is also of fundamental importance. It requires that the donor of genetic information be informed of each and every purpose for which the DNA is being collected at the time of collection (ambiguity of expression frequently occurs at the point where the 'purpose' is communicated to the donor). (Again, limitations and exceptions to this requirement are discussed below.)

The third principle requires that the genetic information collected be adequate, relevant and not excessive in relation to the purposes for which it was collected. This curtails opportunistic collection. (For example, a recent call by the UK Government for DNA testing for all babies born in the United Kingdom is, in our opinion, likely to fall foul of this principle, absent further legislation.)

Retention periods are of particular concern in the context of genetic information databases. The fifth principle requires that personal data shall not be kept longer than is necessary for the purpose for which it was collected. This is problematic as significant investment is nearly always made in the creation of bio-banks and other storage banks, with a view to these becoming valuable assets. Indeed, as a further issue, database rights in the United Kingdom are potentially perpetual, provided the database is regularly updated. (Again, there are limitations and exceptions to this requirement, discussed below.)

Another principle worthy of comment in the context of genetic information and databases is the seventh principle. This requires that appropriate security measures be put in place. This provision is again, unfortunately, drafted in relatively loose language. It is, therefore, open to the controllers of such databases to decide what security is appropriate in the circumstances, given the nature and sensitivity of the information concerned.

Finally, the eighth principle requires that genetic information is not transferred outside the EU unless there is in force an adequate level of protection in the receiving jurisdiction. This has proved to be particularly problematic for international companies for whom such transfers are essential. There are, however, various means of achieving compliance with this principle. These include obtaining the express consent of the donors, putting in place contractual safeguards based on the EU standard clauses (known as 'model contracts')[2] or, as regards transfers to the United States, signing up to the US Safe Harbor.

Limitations and Exceptions for Medical Research

As regards the use of genetic information in the specific context of medical research, there are limitations and exceptions from certain of the above principles.

- The requirement for consent to be 'explicit' is relaxed in the context of the creation and maintaining of genetic databases for research purposes (including historical and statistical analysis purposes), where the database is substantially in the public interest, is not used to take decisions about any person without consent, and is not likely to cause substantial damage or distress to the donors (or, indeed, any other person).[3]

- The further processing of information contained in genetic databases for research purposes only (including historical and statistical analysis) shall not be regarded as incompatible with the purpose for which the information was originally obtained. Thus, aspects of the second principle are relaxed.

- Genetic databases which are used for research may be kept indefinitely, notwithstanding the fifth data protection principle. Databases of this type are also exempt from subject access requests under the sixth principle (provided that they are not made available in a form which identifies the donor).

- The requirement for consent to be 'explicit' is also relaxed where the processing of genetic information is necessary for medical purposes. Medical purposes are defined as 'preventative medicine, medical diagnosis, *medical research*, the provision of care and treatment and the management of healthcare services'. It is important to note, however, that this alternative is only available where a health professional (or a person who owes an equivalent duty of confidentiality) conducts the processing.

Compliance Methodology

Considering the above exceptions together, there is a fairly broad basis on which genetic information may be used for medical research. By way of example, however, although bio-banks may be able to rely on the specific exemption for databases, they still need to comply with the remaining principles. In order to conduct research in a manner that ensures fair processing of the genetic information and minimises the risk that such processing could be deemed to be inconsistent with the applicable data protection law, it is recommended that all such research be carried out in conformity with an appropriately tailored methodology or blueprint setting out the principles that will apply to the research project. Depending on the nature of the research, a formal impact assessment may also be required in order to determine whether less intrusive research methodology is feasible. The methodology should then set out parameters as to who conducts and has access to the research, where the research will take place, where the results will be stored and for what duration, the security precautions surrounding the results and then the procedures for any onward transfer of the database or any of its contents, particularly where transfers are desired outside the EU.

Conclusion

Ambiguity of purpose surrounding the initial collection of genetic information can be compounded through the sale and transfer of databases between businesses. Add to this the transfer of such databases outside the EU, the subjective nature of security arrangements, the derogations to the requirement to obtain explicit donor consent (mentioned above) and the perceived lack of enforcement, it appears that the scope for processing outside the original purpose is substantial. From the point of view of the individual donor, this is not good news. Equally, from the point of view of the

2) Decision C (2001) 1539 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; Decision C (2001) 4540 of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC; Decision C (2004) 5271 of 27 December 2004 on amending decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

3) The Data Protection (Processing of Sensitive Personal Data) Order 2000.

companies investing in genetic information, the data protection regime relating to medical research is already complicated and imposes a significant compliance burden. In addition to the UK Act and the statutory instruments mentioned in this article, there is the European Convention on Human Rights (which includes the right to respect for private and family life). There are also many codes of practice and guidelines issued by bodies such as the Department of Health, and the Medical Research Council. The result is that neither individual nor society is particularly well served by the current legislative framework in the United Kingdom.

The next article will consider the US legislative framework and whether the UK and US protection regimes meet the challenges discussed in the opening paragraphs above.