GeneWatch UK: The Data Protection Bill: Implications for DNA and genetic data

February 2018

[Note: this briefing has been revised to take account of amendments in the Lords]

GeneWatch UK is a not-for-profit organisation, which aims to ensure that genetic technologies are used in the public interest. This briefing therefore highlights the implications of the Data Protection Bill for the collection, storage and use of DNA and genetic information.

GeneWatch UK welcomes the Government's decision to introduce the Bill and to seek to implement the provisions of the EU's new General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED). However, we have a number of concerns about the provisions in the Bill. These relate to the unacceptable inclusion of delegated powers and a large number of overly broad exemptions.

1. **Background**

Genetic information can act as a "biometric", may also provide health information about the individual and family members, and in addition reveals a person's family relationships (Box A).

Due to its sensitivity, genetic information is classed as one of a number of "special categories" of personal data for the purposes of the GDPR and LED. It is widely recognised that it is impossible to anonymise significant amounts of genetic information.

Box A: What is genetic information?
A person's DNA is contained in every cell in their body and may be extracted from a biological sample (e.g. their blood or saliva) and analysed to obtain genetic information. This can include information about a single genetic mutation (which may occur in many individuals), or multiple genetic differences (which may give a high probability of uniquely identifying an individual), up to an including the whole genome (a long string of chemical letters that is likely unique to a given individual). A forensic DNA profile is a string of numbers based on parts of a person's DNA which has a high discriminatory power. Genetic information can be stored digitally on a computer database and searched and used like a "genetic fingerprint" to identify an individual. However, unlike a fingerprint, genetic information can also identify a person's relatives, including non-paternity. Some (but not all) genetic information may provide reveal information about a person's current or future health and other physical characteristics (such as appearance). This may include information that they themselves may be unaware of (such as the risk of developing a late-onset disease, or of passing a genetic disorder to their children).

Genetic data is currently routinely collected and used by the police, security services, immigration services, commercial companies (for paternity, ancestry and health testing, and for research), universities and research institutions, and the NHS. Currently, genetic testing within the NHS is mainly limited to specific tests in limited patient populations, but there are proposals to expand this significantly in the future, including through public-private partnerships. Some commercial companies already offer "direct to consumer" genetic testing (e.g. the Google-funded company 23andMe, and Ancestry.com). All the major digital companies, including Google, have expressed an interest in storing and analysing genetic data, and Google has repeatedly discussed potential access to genetic information from the NHS with the UK Government.[1]

Genetic information has many uses, but is also open to abuse (Box B). To prevent these abuses, and maintain public trust in legitimate uses of DNA and genetic information, it is vital that adequate safeguards are in place.

Box B: Genetic information: uses and abuses
Genetic information has important uses in identifying suspects in criminal investigations, resolving paternity disputes, diagnosing genetic disorders, and (in some circumstances) identifying some health risks. However, it is also open to abuse, as stored genetic information can be misused for a range of purposes, including: government surveillance (for example, identifying who attended a political meeting and tracking down their relatives); exposing individual identities and those of their families in ways which may put a person at risk of abuse (for example, by exposing non-paternity in families, or the location of a vulnerable individual); other criminal activity (e.g. identity theft); and commercial tracking and exploitation (for example, targeting persons claimed to be at high genetic risk of disease with marketing for drugs or supplements); genetic discrimination based on interpretations regarding a person's ancestry or further health.

Previous examples of Government failure to maintain trust through adequate safeguards include significant controversy around the retention of innocent people's DNA profiles on the police National DNA Database (ultimately resolved by the Protection of Freedoms Act 2012)[2]; and the furore surrounding Clause 152 of the Coroners and Justice Bill in 2009 (which was rapidly dropped)[3].

2. Comments on the Bill

Many of our concerns have already been highlighted by others, including Liberty[4], Privacy International[5], and MedConfidential[6]. The focus of this briefing is to highlight why adequate safeguards are particularly important in the context of genetic information.

A number of our concerns strengthen the view that Article 8 of the European Charter of Fundamental Rights ought to be expressly included in the Bill; and that more care should be taken to define the terms "substantial public interest" and "public interest", which may allow the processing of genetic data (including cross-border transfers) under exemptions from many of the safeguards in the Bill. Both these issues are discussed further in the note from Deputy Counsel to the Joint Committee on Human Rights.[7]

2.1 Delegated powers

There is significant concern regarding the powers given to the Secretary of State in Clause 10(6 and 7) and Clause 16. These clauses allow the Government wide powers to alter the application of the GDPR and to amend Schedule 1 (conditions for processing special categories of personal data, which includes genetic data) and Schedules 2 to 4 (exemptions to the data protection principles and rights beyond those provided for by the GDPR).

Similarly, Clause 35(6) provides delegated powers to amend safeguards for processing of sensitive personal data for law enforcement; Clause 86(3) provides delegated powers to amend safeguards for processing of sensitive personal data by intelligence services; and Clause 113 provides delegated powers to make further exemptions from data rights regarding intelligence services processing.

The Delegated Powers and Regulatory Reform Committee has referred to these clauses as "*widely-drafted and highly significant Henry VIII provisions*", and stated "*We are troubled that the Government should think it appropriate, on the basis of such a thin justification, to seek*

to take wide-ranging powers allowing current or future Ministers to implement important policy changes without the need for further primary legislation".[8]

In GeneWatch's view these clauses make the protections in the Bill meaningless as they remove any requirement for detailed parliamentary scrutiny, should the Government choose to weaken or even totally remove the safeguards in the Bill. In order to maintain public trust that genetic information and other data are adequately protected by law, these clauses need to be deleted.

2.2 Automated decision-making

Clause 14 provides for automated decision-making authorised by law in some circumstances. Similarly, law enforcement agencies are exempted from the prohibition on making purely automated, significant decisions by clauses 49 and 50, and intelligence agencies by clauses 96 and 97. However, these clauses do not provide for any safeguards to prevent discrimination, or to ensure that the decisions are based on a valid analysis of the available data.

Genetic information may inform decisions regarding: the identity of an individual or the relatedness of families (e.g. for immigration or maintenance payment purposes); the pursuit of an investigation of an individual, or their family member (using 'familial searching' for partial DNA profile matches), for a criminal offence; or the diagnosis or prediction of disease. It is likely that such decisions may become more automated in future, through the use of computer algorithms. In the health area, in particular commercial black-box algorithms may provide highly misleading information about a person's health.[9] There are also many examples of misidentification of criminal suspects using genetic databases.[10,11,12,13,14,15] In some cases, commercial computer software has been used to try to identify an individual's DNA profile from a mixture: however such results are always open to interpretation.[16,17] It is important that any algorithms can be independently validated and that their limitations are known to the police and to the courts.

Further safeguards are therefore essential to: (i) ensure the analysis of genetic data is valid and undertaken in an appropriate context (with expert involvement as necessary); and (ii) prevent genetic discrimination.

Some relevant safeguards already exist: for example, Crown Prosecution Service guidelines require corroborating evidence if a DNA match is used in a prosecution; and the Equality Act 2010 restricts what employers can ask about in pre-employment medical checks, which limits the potential for genetic discrimination. However, the status of other protections post-Brexit remains unclear. For example, the Charter of Fundamental Rights of the European Union prohibits discrimination based on genetic features (Article 21), but no such prohibition exists in domestic law. The Forensic Regulator lacks statutory powers to enforce standards, including for DNA collection and analysis.[18] The In Vitro Diagnostics Regulation (IVDR) requires clinical evidence to support claims regarding the diagnostic and predictive value of medical tests, including genetic tests[19]: but the IVDR is not operational for the purposes of the EU (Withdrawal) Bill, and therefore will not be automatically incorporated into UK law.

GeneWatch UK believes it is premature to add broad exemptions to the Bill to allow for automated decision-making, as safeguards to ensure valid data analysis and prevent discrimination are currently inadequate.

2.3 National Security, Defence and Immigration

Numerous broad exemptions to the rights of individuals in relation to processing for national security, defence and immigration purposes have been highlighted by Liberty, Privacy International and the Information Commissioner's Office.[20,21]

Rapid DNA analysis, which allows on the spot automated DNA testing for policing purposes, is beginning to be introduced. This speeds up the process by avoiding the need for a sample to be sent to experts in a laboratory, but it also raises concerns that on-the-spot testing might in future be used on the streets or at borders, posing major risks to human rights (for example, by allowing the tracking of individuals who are not suspects under investigation for criminal offences, and identification of their relatives, including non-paternity). Such uses could fall within the exemptions as proposed, posing an unacceptable risk to the rights of individuals. On-the-spot fingerprinting is indeed already being piloted, raising human rights concerns.[22] However, DNA testing would be even more intrusive, and adds the worrying possibility of potentially identifying non-paternity in the street.

Further, there is already concern about Home Office access to confidential patient information to aid immigration enforcement.[23] Were this to include genetic data (which is expected to be collected more widely in the NHS in future), there would be additional concerns about the impact on families, as genetic data can reveal relationships and private health information about other members of a person's family.

Data protection or privacy laws which cover police information, including genetic information, are an important part of international best practice worldwide, and governments increasingly require standards to be met before sharing genetic information across borders for policing purposes.[24] Similar safeguards are increasingly likely to be required for cooperation in intelligence and border control: not least because the expected increasing volumes of data will increase the number of mistakes. Thus, failure to provide adequate safeguards could not only damage public trust but also prevent legitimate cross-border co-operation.

GeneWatch UK therefore believes that any exemptions for national security, defence and immigration purposes should be strictly limited to prevent abuses.

GeneWatch UK
86 Dedworth Road, Windsor, Berkshire, SL4 5AY, UK
Phone: 0330 0010507
Email: mail@genewatch.org Website: www.genewatch.org
Registered in England and Wales Company Number 3556885

References

[1] A DNA database in the NHS: Your freedom up for sale? GeneWatch UK Briefing. May 2013. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAinNHS_GWbriefing_fin.pdf
[2] The UK Police National DNA Database. http://www.genewatch.org/sub-539478
[3] Coroners and Justice Bill (Clause 152). http://www.genewatch.org/sub-563487
[4] Liberty's briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords. October 2017. https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20Committee%20Stage%20Lords%20Oct%202017%20.pdf
[5] Privacy International's briefing on the Data Protection Bill for Second Reading in the House of Lords. Ocober 2017.

https://privacyinternational.org/sites/default/files/Final%20Privacy%20International%25u2019s%20briefing%20on%20the%20Data%20Protection%20Bill.pdf

[6] medConfidential briefing on the Data Protection Bill (second reading). October 2017. https://medconfidential.org/wp-content/uploads/2017/10/medconfidential-Data-Protection-2nd-reading.docx

[7] Note from Deputy Counsel: The Human Rights Implications of the Data Protection Bill. Joint Committee on Human Rights. DPB (17–19) 001. 6th December 2017. http://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

[8] Data Protection Bill. House of Lords Delegated Powers and Regulatory Reform Committee. 6th Report of Session 2017–19. 24th October 2017. https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/29/29.pdf

[9] Janssens, A.C.J.W., Gwinn, M., Bradley, L.A., Oostra, B.A., van Duijn, C.M., Khoury, M.J., 2008. A critical appraisal of the scientific basis of commercial genomic profiles used to assess health risks and personalize health interventions. Am. J. Hum. Genet. 82, 593–599. https://doi.org/10.1016/j.ajhg.2007.12.020

[10] DNA database in doubt after teenager spends three months behind bars for rape in city he has never even visited because gene samples were mixed up. Daily Mail. 18th May 2012. http://www.dailymail.co.uk/news/article-2114252/Teenager-spends-months-bars-DNA-blunder-fingers-rape-city-visited.html

[11] Las Vegas police reveal DNA error put wrong man in prison. Las Vegas Review Journal. 7th July 2011. http://www.reviewjournal.com/news/crime-courts/las-vegas-police-reveal-dna-error-put-wrong-man-prison

[12] DNA Testing: Foolproof? CBS News. 11th February 2009. http://www.cbsnews.com/news/dna-testing-foolproof/

[13] DNA Match Tying Protest to 2004 Killing Is Doubted. The New York Times. 11th July 2012. http://www.nytimes.com/2012/07/12/nyregion/suspected-dna-link-to-2004-killing-was-the-result-of-a-lab-error.html

[14] Cleared murder accused victim of DNA blunder. Liverpool Daily Post. 10th March 2003. http://www.liverpoolecho.co.uk/news/?objectid=12718961&method=full&siteid=50061

[15] Ancestry firms' DNA database use suspect. The Clarion-Ledger. 27th March 2016. http://www.clarionledger.com/story/news/2016/03/27/ancestory-firms-dna-database-use-suspect/82329306/

[16] DNA test put on trial. Times Union. 16th September 2013. http://www.timesunion.com/local/article/DNA-test-put-on-trial-4815368.php

[17] Reliability Questions Raised Over Algorithm Analysis of Murky DNA Evidence in Criminal Cases. AllGov. 5th November 2016. http://www.allgov.com/news/controversies/reliability-questions-raised-over-algorithm-analysis-of-murky-dna-evidence-in-criminal-cases-161105?news=859721

[18] Forensic science standards 'at significant risk'. BBC. 6th January 2017. http://www.bbc.co.uk/news/uk-38527830

[19] REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0746&from=EN

[20] Data Protection Bill, House of Lords second reading – Information Commissioner's briefing. https://ico.org.uk/media/about-the-ico/documents/2172484/dp-bill-commissioner-briefing-lords-second-reading.pdf

[21] Data Protection Bill, House of Lords second reading – Information Commissioner's briefing. Annex. https://ico.org.uk/media/about-the-ico/documents/2172658/dp-bill-lords-briefing-committee-stage-combined-annex-20171030.pdf

[22] Why it's not okay for police to quietly roll out on-the-spot fingerprint scanning. Liberty. 10th February 2018. https://www.liberty-human-rights.org.uk/news/blog/why-its-not-okay-police-quietly-roll-out-spot-fingerprint-scanning

[23] MRN Legal Challenge against NHS Data-Sharing Deal. Migrants' Rights Network Press Release. 9th November 2017. https://migrantsrights.org.uk/blog/2017/11/09/mrn-legal-challenge-nhs-data-sharing-deal-press-release/

[24] Establishing Best Practice for Forensic DNA Databases. Forensic Genetics Policy Initiative. September 2017. http://dnapolicyinitiative.org/wp-content/uploads/2017/08/BestPractice-Report-plus-cover-final.pdf