GeneWatch UK comments on the Data Protection and Digital Information Bill: serious implications for public trust in the use of genetic data

November 2023

GeneWatch UK is a not-for-profit organisation which aims to ensure that genetic science and technologies are used in the public interest.

GeneWatch UK played an active role in the debate regarding the retention of innocent people's DNA databases on the police National DNA Database, leading to the adoption of the Protection of Freedoms Act 2012, and now leads the Forensic Genetics Policy Initiative, which provides information regarding best practice for forensic DNA databases to countries around the world.[1] GeneWatch UK has engaged in debates regarding health and research genetic databases and the need for regulation of human genetic tests for 25 years.

This briefing relates to the implications of the Data Protection and Digital Information Bill for genetic data.[2]

The Bill as proposed poses a major threat to genetic privacy, as detailed below. In particular, it:

- **(i) Redefines the scope of data protection law so it no longer covers some genetic data, despite the potential for such data to be used to identify individuals and their relatives as genetic databases grow in size;**
- **(ii) Redefines consent to the research uses of data, so that virtually any data processing could be undertaken under the guise of 'scientific research' without seeking fully informed consent;**
- (iii) **Potentially allows routine sharing and processing of genetic data (collected, for example, for health, research or commercial purposes) for criminal investigation and security purposes, abandoning the current balancing test, under which the police must first convince a judge that such access is necessary and proportionate to solve a specific case.** There is a lack of clarity regarding whether this is really the Government's intention, as no explicit reference is made in the Bill to the further processing of data that falls into the category of "special data' (including genetic data). Data that could be shared automatically with police includes genetic information from the blood spots collected from every baby at birth in the NHS, which are currently being stored indefinitely, as well as from existing and planned genetic databases held by UK Biobank, the National Institute for Health and Care Research (NIHR) Bioresource, Genomics England, Our Future Health, 23andMe and Ancestry.

In addition, the Bill creates considerable confusion and complexity by: requiring data controllers and processers to interpret three inter-related pieces of legislation[3]; redefining crucial terms such as the meaning of personal data, defined purposes and consent; undermining data subjects rights; giving the Secretary of State significant powers to make further changes to the rules without full parliamentary scrutiny; and allowing the UK Government to use future legislation to override data protection laws. This is likely to lead to **significant loss of public trust** as people will no longer know whether the basis on which they give consent to data processing will be maintained into the future.

1. Background

In health and research projects, genetic data is stored in the form of genotypes (information about multiple genetic variants that an individual carries), exomes (information from the

protein-coding part of the genome) or whole genome sequences (the full sequence of a person's DNA). Such genetic data acts as a biometric (a 'genetic fingerprint') which can identify an individual. It is particularly sensitive because it can also identify relatives and non-paternity, as well as containing some sensitive health information (such as whether an individual is a carrier of a genetic disorder). Genetic data also potentially allows statistical inferences to be made regarding a person's 'genetic ancestry' and likelihood of developing a variety of diseases or physical and behavioural traits. Police DNA databases contain more restricted genetic information, in the form of forensic DNA profiles, based on the number of short sequences (short tandem repeats) repeated at certain places in the genome. Forensic DNA profiles can be used to identify relatives and non-paternity but are not thought to contain information about an individual's health or other characteristics.

Loss of genetic privacy can have major implications. Since genomic data is expected to be shared internationally, individuals (including political dissidents, for example) could be tracked down wherever they are, and their relatives could also be identified and targeted. Women and children can be put in danger if non-paternity is exposed, families could be broken up, vulnerable people (such as people on witness protection schemes or fleeing domestic violence) could have their identities exposed and be tracked by their abusers, as could undercover police officers or security service personnel, and powerful people could be blackmailed if children born outside marriage can be identified.[4,5] In addition, categories derived from statistical analysis of genetic data (such as 'genetic ancestry', predicted health risks, or claimed genetic propensities to certain behaviours) can lead to stigma and discrimination.

The following analysis describes the most important clauses in the Bill.

1. Clause 1: Information relating to an identifiable living individual

This clause changes the current definition of personal data, so that some genetic data will no longer be treated as personal data, even when it comes from a living individual. This is because the proposed new clause only covers circumstances where the living individual will be, or is likely to be, identifiable by another person "*by reasonable means <u>at the time of the processing</u>*".

In current data protection legislation (the EU's General Data Protection Regulation, GDPR, as applied to the UK, and the Data Protection Act 2018: known as the UK GDPR), genetic data is explicitly defined as 'personal data', which clearly falls within the scope. Further, genetic data falls within the category of 'special categories of personal data' which require extra safeguards. The ICO explains the current situation thus:

"*..in practice, genetic analysis which includes enough genetic markers to be unique to an individual is personal data and special category genetic data, even if you have removed other names or identifiers. And any genetic test results which are linked to a specific biological sample are usually personal data, even if the results themselves are not unique to the individual, because the sample is by its nature specific to an individual and provides the link back to their specific genetic identity.*

However, there are cases where genetic information is not identifiable personal data. For example, where you have anonymised or aggregated partial genetic sequences or genetic test results (eg for statistical or research purposes), and they can no longer be linked back to a specific genetic identity, sample or profile; a patient record; or to any other identifier".[6]

Under the Bill, this changes significantly. Genetic data that is attached to an individual's name or other identifiers clearly relates to "*an identifiable living individual*" and continues to

fall within the scope of the regulation. However, genetic data that is not attached to an individual's name or other identifiers requires a process of re-identification before the individual is regarded as identifiable. This process can utilise other information stored with the genetic information, or be based on the genetic information alone. The disclosure of limited other information, such as health diagnosis codes, alongside a persons' genome, may be sufficient to identify them, by comparing DNA sequences from a research project with electronic medical records.[7] Based on genetic information alone, in the absence of any identifying information, an individual can be identified if their relative is in a genetic database, even if they themselves are not, because people share parts of their DNA with their families.[8] In the USA, there is already sufficient information in public genetic genealogy databases to deduce the identity of many individuals by triangulating other information such as surname, age and state.[9] Alternatively, an individual's surname can sometimes be deduced from information about DNA on the Y-chromosome that is passed down the male line (although such deductions will not always be correct).[10] Although the likelihood of re-identification grows as genetic databases grow in size, it is nevertheless the case that not all individuals can currently be identified in this way.

In evidence to the Commons Bill Committee, the following exchange took place between Jonathan Sellors MBE, Legal Counsel and Company Secretary, UK Biobank, and Chi Onwurah, MP,[11]
"***Jonathan Sellors:****…Releasing quite a big bit of my genetic sequence does not make me re-identifiable.*
Chi Onwurah *Currently.*
Jonathan Sellors: *Currently—I accept that*".

Thus, it is clear that, under the Bill's proposals, genetic data could be released and treated as falling outside the remit of data protection laws if it is regarded as not currently identifiable "*by reasonable means at the time of the processing*", even though there is a widespread expectation that all such data will become identifiable as genetic databases grow in size in future. **This exempts genetic data that currently falls within the remit of the UK GDPR from any data protection regulation.** In addition, **it creates considerable confusion**, as it exempts data which will become identifiable and hence require protection at a future date: creating the likelihood that such protections will come too late.

Biometrics (including, but not limited to, genetic data) can't be changed, and excluding any biometrics from the scope of data protection law on the basis that they cannot currently identify an individual is extremely short-sighted and dangerous. In the case of genetic data, this serious problem is further exacerbated by the fact that it relates not only to the data subject but also to their relatives.

In addition to these serious privacy concerns, it should be noted that genetic research can include highly controversial research, for example related to 'genetic ancestry' or race, and non-health-related traits (such as intelligence, criminality or sexual preferences). The proposed re-definition of personal data in the Bill could therefore allow controversial research to take place using people's genetic information without their knowledge or consent.

This clause could lead to a significant loss of public trust in the use of genetic data by researchers, commercial companies and the NHS, since it removes all the current safeguards from an important subset of genetic data (i.e., genetic data collected from living persons which is not immediately identifiable, but which will likely be identifiable in future).

Because genetic data is explicitly included in the definition of personal data (and sensitive data) in the GDPR, **this clause also risks the loss of the EU GDPR adequacy decision**

as it relates to the UK, with significant adverse impacts on scientific research and businesses.

2. Clauses 2 and 3: Meaning of research and statistical purposes, and the use of broad consent

In Clause 2, scientific research is defined extremely broadly as "*any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity*". In addition, historical research is defined as including "*processing for the purposes of genealogical research*". Although using personal data for "statistical purposes" requires the controller not to use the personal data or resulting information to support measures or decisions regarding an individual, there is no such restriction on processing for "scientific research".

The GDPR states that, "'*consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*." Clause 3 implies that consent can be "treated as" consent in the context of research even if it does not fall within this definition. This means that so-called consent to scientific research no longer has to be specific and informed, provided it is "*consistent with generally recognised ethical standards relevant to the area of research*".

Safeguards for processing for research and scientific purposes (referred to as 'RAS purposes) are described in Clause 24. These allow living individuals to be identified in cases in which the RAS purposes cannot be fulfilled without doing so.

Together, these clauses significantly weaken an individual's control over their data. In the context of genetic data, these changes undermine the requirement for fully informed consent to data-sharing with commercial companies; genealogical research (including research categorising people based on their race or 'genetic ancestry'); and controversial research in non-health related areas (such as the genetics of intelligence, criminality or homosexuality).

Because the definition of 'scientific research' is so broad and decisions can be taken about individuals based on processing for 'scientific research' purposes, virtually any data processing could be monetised without seeking fully informed consent.

In the context of medical research, including genetic research, **these provisions are not consistent with the Helsinki Declaration**, which requires research subjects to give fully informed consent.[12]

As noted above, genetic research can include highly controversial research, for example related to 'genetic ancestry' or race, and non-health-related traits (such as intelligence, criminality or sexual preferences). The proposed re-definition of consent in the Bill could therefore allow such controversial research to take place using people's genetic information without their knowledge or consent.

3. Clauses 5 and 6 (and Schedules 1 and 2): Crime detection as a 'recognised legitimate interest' and a purpose 'compatible with original purpose'

Data processing is only lawful if it is performed for a lawful purpose. If this purpose is the 'legitimate interests' of the controller or a third party, the fully informed consent of the individual is not generally required. Currently, processing for 'legitimate interests' requires a balancing test as to whether the individual's interests over-ride that of the data controller.

Clause 5 removes this requirement by defining certain 'recognised legitimate interests' which will no longer require this test (provided in Schedule 1). These include,
"(a) detecting, investigating or preventing crime, or
(b) apprehending or prosecuting offenders".
National security and public security are also included as 'recognised legitimate interests' in Schedule 1.

Current legislation also restricts the lawful use of data to the purpose for which it was originally required, except "*when such a restriction respects the essence of the fundamental rights and freedoms and is necessary and proportionate measure in a democratic society*". Clause 6 of the Bill removes this requirement for proportionality by listing purposes in Schedule 2 which are automatically considered as compatible with the original purpose for which the data was collected. These again include,
"(a) detecting, investigating or preventing crime, or
(b) apprehending or prosecuting offenders",
as well as national security and public security interests.

Both Schedules 1 and 2 allow the data to be disclosed "*to another person in response to a request from another person*" and require the disclosure to be necessary for a list of purposes that include the prevention and detection of crime or public security. However, there is no longer any reference to proportionality. In Clause 6, the police and intelligence services are given powers to use such data (collected other than from the data subject and/or processed by other controllers).

Genetic data falls within the special categories of personal data, which is subject to additional restrictions on processing (Article 9 of UK GDPR). If the lawful basis of processing is the newly defined 'recognised legitimate interests' in Clause 5 and Schedule 1, these additional restrictions still apply and would appear to prevent processing for law enforcement, unless it is necessary for reasons of "substantial public interest", as well as proportionate to the aim pursued. Thus Clause 5 (and Schedule 1) do not appear to weaken safeguards for genetic data. However, Clause 6 (and Schedule 2) are a different matter. If the lawful basis of processing of genetic data is explicit consent for a specified purpose (such as health, research or commercial purposes), the effect of Clause 6 (and Schedule 2) appears to be to treat processing for law enforcement or security purposes as compatible with the original purpose, regardless of whether it involves special data or not. If such databases were created with consent under GDPR (e.g. for health, research or commercial purposes), Clause 6 states that the data can only be used in this way if "*the controller cannot reasonably be expected to obtain the data subject's consent*". However, there is no indication in the Bill of what is may be regarded as "*reasonable*". Thus, Schedule 2 appears to allow existing genetic databases (created with explicit consent for a different purpose) to be accessed for crime and national security purposes without consent.

Some doubt about whether this is the Government's intention is raised by the insertion by Clause 6 Subsection (3) of this phrase at the end of Article 5 UK GDPR: "*For the avoidance of doubt, processing is not lawful by virtue only of being processing in a manner compatible with the purposes for which the personal data is collected*". In relation to this change, the Explanatory Notes state: "*Subsection(3) clarifies that meeting a condition under Article 8A for further processing does not permit controllers to continue relying on the same lawful basis under Article 6(1) that they relied on for their original purpose if that basis is no longer valid for the new purpose. In many cases, controllers will be able to establish a lawful basis under Article 6(1) for the new purpose through satisfying the conditions under the new Article 8A*." In the case of processing that does not involve 'special data' it is clear that such a lawful basis might be provided by the idea of 'recognised legitimate interests' introduced by Clause 5 of the Bill. However, in the case of 'special data' the situation is unclear, because there is nothing in the Bill about the legal basis for processing under UK GDPR

Article 9 ('special categories of data'), which could potentially be on the basis of consent to the original purposes. Unlike in Clause 12 (Automated Decision Making), an explicit exemption has not been applied to special data, which suggests that the intention is that further processing of special data for criminal investigations purposes is allowed by the changes in the Bill.

These provisions appear to remove the current balancing test which requires an assessment of whether accessing genetic databases during criminal investigations is necessary and proportionate and sufficient to override the interests and rights of the data subject. Instead, blanket use of genetic databases (set up for health, research or commercial purposes) appears to be granted for the purpose of detecting crime and/or protecting public security. There is a lack of clarity regarding whether this is really the Government's intention, as no explicit reference is made in the Bill to the further processing of data that falls into the category of "special data' (including genetic data).

Currently, the police can argue in court that accessing a genetic database set up for health or research purposes is in the public interest in specific circumstances (for example, when investigating a specific crime).[13,14] However, they must demonstrate that their request is necessary and proportionate. Organisations managing databases for genetic research or for the NHS often tell participants that they will resist access by the police. For example, UK Biobank's public information leaflet states, "*Insurance companies and employers will not be given any individual's information, samples or test results, and nor will we allow access to the police, security services, relatives or lawyers, unless forced to do so by the courts*".[15] Genomics England is a Government-owned company which manages genomic and health data collected from the NHS Genomics Medicine Service, via the National Genomics Health Library (NGRL), and is also running a pilot project looking at sequencing the genome of every baby in the NHS.[16] The NGRL states that requests for forensic uses will "*typically be refused outright*" and in addition, "*Requests in the form of Court Orders will be referred to Genomics England's Legal Counsel as promptly as possible, so that all representations may be made to the court, for example to limit the information requested*".[17]

Commercial companies offering genetic testing on the internet also resist police access. For example, genetic testing company 23andMe states, "*23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access*".[18] The company Ancestry states "*Ancestry does not voluntarily cooperate with law enforcement*" and "*Respect for the privacy and security of our users' account data drives our approach to complying with legal requests for information*".[19]

Blood spots are currently collected from every newborn baby in the NHS using a heel prick, to test for some important medical conditions.[20] The Code of Practice covering these blood spots currently states, "*Appropriate legal permission (written court order or by instruction of a Coroner) is required for the release of residual newborn blood spots from specific dead or missing people for forensic purposes. This access should be carefully controlled. Directors of Newborn Screening Laboratories may wish to liaise with the legal and governance department within their own Trusts/Health Boards when such requests are received. Samples from individuals who are alive and not missing should rarely be released for this purpose since alternatives are available – this would also require legal permission (written court order or by instruction of a Coroner). Directors of Newborn Screening Laboratories may wish to check such applications with their Trust/Health Board's legal and governance department.*"[21]

The changes in the Bill potentially over-ride these efforts to maintain public trust by allowing the routine use of such databases for criminal investigations, without any

reference to the need for proportionality or a balancing test with an individual's rights.

This is of particular concern in the context of proposals to expand the collection of genetic information for health and/or research purposes. This includes the roll out of the Genomic Medicine Service (GMS) within the NHS[22]; the controversial proposal to sequence the DNA of every baby in the NHS (beginning with a pilot study in late 2023)[23,24]; the National Institute for Health and Care Research (NIHR) Bioresource's new initiative to collect DNA from children, called the DNA, Children + Young People's Health Resource (D-CYPHR)[25]; and the 'Our Future Health' research project. The latter plans to recruit 5 million adults via the NHS to share their genetic data with commercial companies, and to return Polygenic Risk Scores to consenting individuals, despite concerns that such scores have poor predictive value and lack evidence that they will improve health outcomes.[26,27,28,29] The D-CYPHR has already piloted recruitment of children's DNA via a small number of schools and has now launched nationwide.[30] A previous attempt to allow blanket sharing of genetic data with commercial companies and the police (Clause 152 of the Coroners and Justice Bill in 2009) was dropped following a massive public backlash against the proposals.[31] The newborn blood spot screening Code of Practice (dated 2018) also states the policy of storing blood spots for a limited time (5 years) is under review, so that currently these blood spots are stored indefinitely. [32] Research projects undertaken with the blood spots include a feasibility study conducted in 2019 to assess the utility of Next Generation DNA sequencing in newborn screening.[33] The potential sequencing of babies' blood spots without explicit consent, combined with the proposal to allow automatic sharing of this data with police and security services in this Bill, could lead to significant loss of trust in the newborn screening programme. **Clause 6 revives concerns that the Government wishes to create a backdoor DNA database within the NHS, available for routine use for surveillance purposes.**

Clause 6 is likely to breach international human rights safeguards (the right to privacy) as protected under Article 8 of the European Convention on Human Rights and Article 17 of the International Covenant on Civil and Political Rights. The use of DNA for law enforcement and security purposes requires the adoption of extensive legal safeguards and tight restrictions on whose DNA may be collected and used without consent.[34] Internationally, both Kuwait and Kenya have annulled laws which would have allowed blanket collection, retention and processing of DNA and genetic information from all citizens: these laws were found to be unnecessarily intrusive and in breach of article 17 of the International Covenant on Civil and Political Rights.[35,36,37] In England and Wales, innocent people's DNA profiles were removed from the National DNA Database, and stored DNA samples were destroyed, under The Protection of Freedoms Act 2012, following a judgement by the European Court of Human Rights (in the case of S. and Marper v. the UK) which found that, "*the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society*".[38,39,40,41] Prior to the implementation of the Protection of Freedoms Act, the controversy surrounding the retention of innocent people's DNA contributed to a significant loss of public trust in the police use of DNA.

In addition to negative impacts within the UK, Clause 6 sets a poor precedent for other countries, since blanket access to genetic databases by authoritarian regimes is likely to lead to human rights abuses, such as the tracking of political opponents and identification of their relatives. The potential identification of non-paternity also has serious implications for families, including the safety of women and children.

Clause 6 also risks the loss of the EU GDPR adequacy decision as it relates to the UK, with significant adverse impacts on scientific research and businesses. Sharing of genetic data with other countries is also likely to be adversely affected, since foreign governments

could no longer guarantee that their citizen's genetic data is adequately protected (see Section 4).

In addition, Clause 6 allows the Secretary of State to add to the list of "processing to be treated as compatible with original purpose" (in Schedule 2) without full parliamentary scrutiny. **These powers create significant additional uncertainty for individuals considering taking genetic tests for health or research purposes.**

4. Clause 8: Data subjects rights

Clause 8 limits the rights of data subjects to access information about their data, by allowing data controllers to refuse or charge for so-called "vexatious" requests and also delay the release of information. In addition, it exempts data controllers from providing information in the context of scientific or historical research, if this would involve a "disproportionate effort", taking into account factors such as the number of data subjects involved. In effect, this exempts large research databases from providing information to individual participants.

This clause could make it virtually impossible for data subjects to exercise their rights. This has particularly serious implications for large-scale genetic databases in the context of the other proposed changes discussed above, since **individuals would be unable to identify misuses of their own data, including use for policing/security purposes, commercial exploitation, and/or inclusion of their data in controversial research.**

5. Clause 23 and Schedules 5, 6 and 7: Transfer of personal data to third countries and international organisations

The Bill proposes weakening the standards for international data sharing. Rather than being based on an 'adequacy decision' (a process requiring detailed scrutiny of a country's laws and their enforcement), international data sharing will be approved as a result of a 'data protection test' developed under regulations to be developed by the Secretary of State. These regulations will require the Secretary of State to "consider" certain factors, such as respect for the rule of law. The standard of data protection in the third country or international organisation should not be "*materially lower*" than in the UK.

This weakening of standards for international data transfer compounds the problems identified elsewhere in the Bill, not only because the 'data protection test' is weaker than an 'adequacy decision', but also because the UK's data protection standards themselves are undermined by proposals in the Bill. For example, **if the UK allows routine access to genetic databases for criminal investigations and security purposes, it cannot object to the transfer of genetic data to other countries which also do so. Similarly, if the UK exempts some genetic data from data protection laws, it may also transfer such data overseas.**

In addition, it is unclear how data subjects will be able to exercise their rights in relation to data transferred abroad, particularly as their rights are already weakened in this Bill.

Although the Bill purports to make international sharing easier, it is worth noting that in many cases it may become more difficult as a result of the provisions in the Bill. Internationally, legitimate genetic research projects are extremely sensitive to the need to maintain public trust and it is therefore **unlikely that current data sharing with the UK would continue if shared genetic data could be exempted from data protection regulations and/or routinely accessed for law enforcement or security purposes and shared worldwide with insufficient safeguards.**

For example, the US is concerned about Chinese genomic companies gaining access to data from foreign populations, including in the US, through diagnostic testing and analysis and international partnerships. Michael J. Orlando, Director, National Counterintelligence and Security Center, told the FT, "*In the wrong hands, US genomic data poses serious risks not only to the privacy of Americans, but also to US economic and national security*". [42] Other countries may have similar concerns regarding onward sharing of their citizens' genetic data, perhaps with different countries (or with the US itself).

6. Clauses 111 to 113: Oversight of biometric data

These clauses apply to England and Wales only. Clause 111 abolishes the role of the Commissioner for the Retention and Use of Biometric Material. This role was established under the Protection of Freedoms Act 2012 (PoFA) as part of the measures taken to restore public trust in police use of DNA, following the controversy surrounding the indefinite retention of innocent people's DNA profiles on the National DNA Database in England and Wales, and the judgment of the European Court of Human Rights in the case of S. and Marper v the UK. These changes therefore have the potential to reduce public trust in the oversight of the use of DNA by the police and security services.

Clause 111 amends the Protection of Freedoms Act 2012 (PoFA) and the Police and Criminal Evidence Act 1984 (PACE) to transfer some roles from the Biometrics Commissioner to the Investigatory Powers Commissioner. These are the "casework functions":

(i) oversight of National Security Determinations (including the power to order the destruction of fingerprints and/or DNA profiles if s/he is not satisfied that retention is necessary and proportionate for national security).

(ii) determining (in response to applications by the police) whether the fingerprints and DNA profiles of persons arrested but not charged with a qualifying offence may be retained.

The post of Investigatory Powers Commissioner is currently held by a retired judge who originally rejected the application by S. and Marper for deletion of their records from the National DNA Database, on the grounds that this did not constitute an interference with their rights.[43]

Clause 111 also removes the Biometrics Commissioners' function to review the retention and use, by the police and others, of fingerprints and DNA profiles not subject to a National Security Determination, whether this biometric material has been taken and retained under PACE, the Terrorism Act 2000, the Counter-Terrorism Act 2008, or the Terrorism Prevention and Investigation Measures Act 2011. According to the Explanatory Notes, this is being done on the grounds that these are duplicated powers because ICO has the duty to keep under review the use and retention of personal data by all controllers, including the police.[44] However, this will inevitably mean less attention is paid to this issue. **The Biometrics Commissioner currently publishes an annual report, allowing greater public scrutiny of the use of the police and security service's powers, because of the importance of maintaining public trust.**

Clause 111 gives the body formerly known as the National DNA Database Strategy Board (now the Forensic Information Databases Strategy Board, which also oversees the national fingerprint database) potential oversight of other biometrics databases (in addition to the National DNA Database), and the Secretary of State powers to add or remove databases to those the Board oversees. The Strategy Board's role is to provide governance and oversight over the operation of the relevant databases, rather than independent scrutiny. Its expanded role may be seen as positive, however this is undermined by the power given to the Secretary of State to remove databases from its oversight in future, and by the abolition of the independent role of the Biometrics Commissioner.

These clauses contribute to the overall sense that the Government seeks to weaken independent scrutiny of biometric databases.

7. General weakening of data protection standards

Numerous commentators have noted other aspects of the Bill that raise concerns, which are not discussed in detail here, but which may also have implications for the processing of genetic data. These include: the removal of the requirement for overseas companies to have a UK-based representative (Clause 14); removal of the duty to keep records except in 'high risk' circumstances (Clause 16), the proposed uses of National security exemptions (Clause 26); potential undermining of the independence of the ICO (Clauses 29 and 30); and the powers given to the Secretary of State to implement law enforcement information-sharing agreements (Clause 99).

8. Powers given to the UK Government and the Secretary of State

The Bill gives the Secretary of State extensive powers to: amend Annexes 1 and 2 by regulations (Clauses 5 and 6); make further provisions about automated processing (Clause 12); appoint new bodies to assess the ethics of research (Clause 24); issue designation notices for national security, allowing processing by the intelligence services (Clause 27); issue statements of strategic priorities relating to data protection (Clause 30); require the Commissioner to develop new codes of practice, determine whether such codes need oversight by a panel, and reject such codes (Clauses 31, 32 and 33); determine by regulations whether controllers need to notify the Commissioner of complaints (Clause 41); be consulted by the Commissioner about guidance on complaints (Clause 42); make regulations under the UK GDPR by statutory instrument (Clause 46); set out rules concerning the provision of digital verification services, DVS (Clause 49 and subsequent clauses regarding DVS); make provision, with the Treasury, in connection with access to customer data and business data (Clause 65 and subsequent clauses); make regulations regarding cookies stored on devices (Clause 83); make regulations about direct marketing for the purpose of democratic engagement (Clause 87); make regulations regarding monetary penalties (Clause 89 and 90); remove recognition of EU standards (Clause 95); make regulations regarding overseas trust products for electronic signatures etc. (Clauses 96 and 97); in most circumstances, act as the "appropriate national authority" to make regulations for sharing of information for law enforcement purposes (Clause 100); transfer property, rights and liabilities from the Information Commissioner to the Information Commission (Clause 110); change the databases which the Forensic Information Database Strategy Board is required to oversee (Clause 113); make consequential amendments by regulation (Clause 114); determine when many of the provisions in the Bill will come into force, including all the major changes in Part 1 of the Bill (Clause 119); make regulations to approve transfers of data to third countries or international organisations for general or law enforcement processing (Schedules 5, 6 and 7); in relation to health and adult social care, determine when IT providers are given notices of compliance or public censure, or delegate such functions (Schedule 12); determine the membership of the Information Commission (Schedule 13).

The significant powers given to the Secretary of State create additional uncertainty regarding what safeguards will actually apply to people's data, including genetic data, at any future date.

In addition, **Clause 45 allows the UK Government to make legislation which overrides (through express provision) existing data protection legislation.** This adds yet further to the uncertainty and loss of public trust that the Bill creates.

9. Implications for Wales, Scotland and Northern Ireland

Most of the provisions in the Bill apply the England, Wales, Scotland and Northern Ireland (Clause 118), although in some specific circumstances Scottish or Welsh ministers (rather than the Secretary of State) may be the "appropriate national authority" in relation to implementation of law enforcement information-sharing agreements (Clause 100).

As a result of the Bill, organisations operating in the devolved nations, including the NHS, academic researchers and commercial companies, will in effect no longer be able to guarantee to patients, research participants or customers that their data will be treated according to their wishes or in line with the fully informed consent provided, for example, at the time of taking a genetic test, or volunteering for a research project. This is because, as outlined above, the Bill changes the meaning of terms such as personal data, consent and allowed purposes, in ways that are no longer consistent with their generally accepted meanings or with international human rights standards. As noted above, globally, other countries may simply refuse to share genetic data with the UK, on the grounds that it could be exempted from data protection regulations and/or routinely accessed for law enforcement or security purposes under the proposals in the Bill. However, it is unclear whether or how the devolved governments would be able to protect their citizens data in this way, or control access and exploitation of such data by commercial interests, despite the role of devolution within the NHS. **The Bill thus has potential to cause a significant loss of public trust in the collection and use of genetic data in the devolved nations, by undermining existing safeguards and the basis on which individuals agree to share their DNA and genetic data.** International collaborations involving the devolved nations could also be affected.

In addition, the Scottish Biometrics Commissioner Act 2020 created an equivalent post to the Biometrics Commissioner, with powers to oversee biometric data collected for criminal justice and police purposes in Scotland. Although the Scottish Biometrics Commissioner would continue to exist, the proposed abolition of the Biometrics Commissioner (in Clause 111, discussed above) means that forensic DNA profiles sent from the Scottish DNA Database to the UK National DNA Database in England would no longer benefit from equivalent oversight.

Conclusions

The Bill as proposed has significant and alarming implications for people's personal genetic data. It:

- **exempts some genetic data from the scope of data protection legislation, although this could be used to identify individuals or their relatives at a future date;**
- **redefines consent to the research uses of data, so that virtually any data processing could be undertaken under the guise of 'scientific research' without seeking fully informed consent;**
- **potentially allows genetic data collected for health or research purposes to be used for criminal investigations, removing the requirement that this is proportionate to the claimed need.** There is a lack of clarity regarding whether this is really the Government's intention, as no explicit reference is made in the Bill to the further processing of data that falls into the category of "special data' (including genetic data).

The Bill also includes numerous other provisions that damage people's rights in relation to their genetic data, by allowing genetic information to be used in a variety of ways without fully informed consent or even the right to be informed about such uses. **The Bill introduces significant additional complexity into data protection legislation and the**

extensive powers given to the UK Government and the Secretary of State create additional uncertainty regarding what safeguards will actually apply to people's data, including genetic data, at any future date.

There are significant privacy risks associated with the proposed weakening of safeguards. This, combined with the 'shifting sands' of unclear definitions, excessive complexity, and arbitrary Government powers to further weaken future safeguards, is likely to create a significant loss of public trust.

The Bill will likely reduce the willingness of individuals to access genetic tests (even in circumstances where these may be relevant to their or their family's health) and to take part in genetic research projects. **The Bill has potential to cause a significant loss of public trust in the collection and use of genetic data in throughout the UK, by undermining existing safeguards and the basis on which individuals agree to share their, or their children's, DNA and genetic data.**

The Bill undermines the ability of the devolved governments to control and safeguard genetic data collected from their citizens, including via devolved services such as the NHS.

The Bill is not compatible with international human rights standards (the European Convention on Human Rights, the International Covenant on Civil and Political Rights and the Helsinki Declaration) and sets a bad precedent internationally.

The Bill will likely lead to the loss of international collaborations in the field of genetic research and commercial applications. This includes (but is not limited to) the loss of the EU GDPR adequacy decision as it relates to the UK, which will have significant negative impacts on businesses and researchers (regardless of whether they process any genetic data). Globally, the Bill could lead other countries to stop sharing citizens' genetic data with UK-based companies, universities and research institutes.

GeneWatch UK
53, Milton Road, Cambridge, CB4 1XA, UK
Phone: +44 (0)330 0010507
Email: mail@genewatch.org Website: www.genewatch.org
Registered in England and Wales Company Number 03556885

Funded by the Joseph Rowntree Reform Trust.

The Joseph Rowntree Reform Trust has supported this work in recognition of the importance of the issue. The facts presented and the views expressed in this report are, however, those of the authors and not necessarily those of the Trust. www.jrrt.org.uk

References

[1] https://dnapolicyinitiative.org/
[2] Data Protection and Digital Information Bill https://bills.parliament.uk/bills/3430
[3] The current bill (if adopted) plus "the 2018 Act", meaning the Data Protection Act 2018, and "the UK GDPR", meaning Regulation (EU) 2016/679.
[4] GeneWatch UK (2011): DNA databases and human rights. GeneWatch UK briefing. 12th January 2011. Available on: https://dnapolicyinitiative.org/resources/dna-databases-and-human-rights/ or to download from: http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/infopack_fin.pdf

[5] GeneWatch International (2020): Proposals to include DNA in national biometric identification schemes: human rights implications (July 2020). GeneWatch International briefing. 30th July 2020. Available from: http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/dna-and-biometrics-fin.pdf
[6] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/#scd3
[7] Loukides, G., Denny, J. C., & Malin, B. (2010). The disclosure of diagnosis codes can breach research participants' privacy. *Journal of the American Medical Informatics Association : JAMIA*, *17*(3), 322–327. https://doi.org/10.1136/jamia.2009.002725
[8] Erlich, Y., Shor, T., Pe'er, I., & Carmi, S. (2018). Identity inference of genomic data using long-range familial searches. *Science*, *362*(6415), 690–694. https://doi.org/10.1126/science.aau4832
[9] Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science (New York, N.Y.)*, *339*(6117), 321–324. https://doi.org/10.1126/science.1229566
[10] King, T. E., & Jobling, M. A. (2009). Founders, Drift, and Infidelity: The Relationship between Y Chromosome Diversity and Patrilineal Surnames. *Molecular Biology and Evolution*, *26*(5), 1093–1102. https://doi.org/10.1093/molbev/msp022
[11] Data Protection and Digital Information (No. 2) Bill (Second sitting). Debated on Wednesday 10 May 2023.
[12] World Medical Association-WMA. (n.d.). *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects*. Retrieved 27 February 2019, from https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/
[13] Kaye, J. (2006). Police Collection and Access to DNA Samples. *Genomics, Society and Policy*, *2*, 16–27. https://www.lancaster.ac.uk/fss/journals/gsp/vol2no1/kayeabstract.htm
[14] Dranseika, V., Piasecki, J., & Waligora, M. (2016). Forensic uses of research biobanks: Should donors be informed? *Medicine, Health Care, and Philosophy*, *19*, 141–146. https://doi.org/10.1007/s11019-015-9667-0
[15] https://www.ukbiobank.ac.uk/media/ei3bagfb/participant_information_leaflet-baseline.pdf
[16] https://www.genomicsengland.co.uk/
[17] The National Genomic Research Library v5.1. Amendment to The National Genomics Research and Healthcare Knowledgebase v5 https://files.genomicsengland.co.uk/documents/The-National-Genomic-Research-Library-V5.1.pdf
[18] https://www.23andme.com/law-enforcement-guide/
[19] https://www.ancestry.co.uk/c/legal/lawenforcement
[20] https://www.gov.uk/guidance/newborn-blood-spot-screening-programme-overview
[21] *Newborn blood spot screening: Code of practice for residual spots*. (2018, March 28). GOV.UK. https://www.gov.uk/government/publications/newborn-blood-spot-screening-code-of-practice-for-the-retention-and-storage-of-residual-spots
[22] https://www.england.nhs.uk/genomics/nhs-genomic-med-service/
[23] https://www.genomicsengland.co.uk/initiatives/newborns
[24] Biesecker, L. G., Green, E. D., Manolio, T., Solomon, B. D., & Curtis, D. (2021). Should all babies have their genome sequenced at birth? *BMJ*, *375*, n2679. https://doi.org/10.1136/bmj.n2679
[25] https://bioresource.nihr.ac.uk/dcyphr/
[26] https://ourfuturehealth.org.uk/
[27] Sud, A., Horton, R. H., Hingorani, A. D., Tzoulaki, I., Turnbull, C., Houlston, R. S., & Lucassen, A. (2023). Realistic expectations are key to realising the benefits of polygenic scores. *BMJ*, *380*, e073149. https://doi.org/10.1136/bmj-2022-073149
[28] Huntley, C., Torr, B., Sud, A., Rowlands, C. F., Way, R., Snape, K., Hanson, H., Swanton, C., Broggio, J., Lucassen, A., McCartney, M., Houlston, R. S., Hingorani, A. D., Jones, M. E., & Turnbull, C. (2023). Utility of polygenic risk scores in UK cancer screening: A modelling analysis. The Lancet Oncology, 0(0). https://doi.org/10.1016/S1470-2045(23)00156-0
[29] GeneWatch UK Report: Polygenic risk predictions: health revolution or going round in circles? 13th September 2023. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/gw-prs-briefing-fin.pdf
[30] https://bioresource.nihr.ac.uk/dcyphr/
[31] http://www.genewatch.org/sub-563487
[32] *Newborn blood spot screening: Code of practice for residual spots*. (2018, March 28). GOV.UK. https://www.gov.uk/government/publications/newborn-blood-spot-screening-code-of-practice-for-the-retention-and-storage-of-residual-spots

[33] Register of RAC approvals. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/988201/RAC_approved_projects_database_24_May_2021.ods [Listed as an NBS project under the ANNB tab]
[34] 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
[35] United Nations Human Rights Office of the High Commissioner. Concluding observations on the third periodic report of Kuwait. Human Rights Committee. CCPR/C/KWT/CO/3. 11 August 2016. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/KWT/CO/3&Lang=En
[36] Kuwait's high court rules against controversial law on DNA. Zawya. 6th October 2017. https://www.zawya.com/mena/en/legal/story/Kuwaits_high_court_rules_against_controversial_law_on_DNA-SNG_101047768/
[37] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLRPetition 56, 58 & 59 of 2019 (Consolidated) REPUBLIC OF KENYA IN THE HIGH COURT OF KENYA AT NAIROBI CONSTITUTIONAL & JUDICIAL REVIEW DIVISION CONSOLIDATED PETITIONS NO. 56, 58 & 59 OF 2019. https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html
[38] CASE OF S. AND MARPER v. THE UNITED KINGDOM. JUDGMENT STRASBOURG 4 December 2008. https://rm.coe.int/168067d216
[39] Protection of Freedoms Act 2012. https://www.legislation.gov.uk/ukpga/2012/9/contents
[40] Home Office (2013) NATIONAL DNA DATABASE STRATEGY BOARD ANNUAL REPORT 2012-13. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/252885/NDNAD_Annual_Report_2012-13.pdf
[41] Drury, I. (2008, December 5). *One million innocent people could have their profiles wiped from Britain's DNA database after court ruling*. Mail Online. https://www.dailymail.co.uk/news/article-1091880/One-million-innocent-people-profiles-wiped-Britains-DNA-database-court-ruling.html
[42] Smyth, J., & Sevastopulo, D. (2023, April 18). Chinese genetics company targets US despite political tensions. *Financial Times*. https://www.ft.com/content/cc905012-f264-4e87-8171-8e7e243c5d51
[43] https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040722/york-1.htm
[44] Data Protection and Digital Information (No. 2) Bill Explanatory Notes. Bill 265 EN 2022-23. https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf