GeneWatch UK response to the Ministry of Justice's Call for Evidence on the Review of the Balance of Competences between the United Kingdom and the European Union: Information Rights

July 2014

GeneWatch UK is a not-for-profit group which aims to ensure that genetic science and technologies are used in the public interest. Our work covers environmental issues (in relation to the open release of genetically modified organisms, GMOs) and human rights issues, in relation to the retention, use and sharing of genetic data in the health, research and criminal justice contexts.

The data protection issues addressed in this evidence are particularly relevant to UK Government plans to sequence whole genomes, storing the data permanently as attachments to NHS electronic medical records, and sharing this information with private companies such as Google, which may store it in the Cloud i.e. on servers overseas. Health Secretary Jeremy Hunt has stated that he wishes the whole genome of every baby in NHS England to be sequenced in the future[1], and the 100,000 Genomes Project is seen as a pilot project for sequencing the whole population.[2] GeneWatch has raised extensive concerns about these plans in relation to their implications for privacy, human rights and the future of the NHS.[3]

The planned data-sharing is "pseudo-anonymised" (i.e. it retains the link back to the individual) so that risk assessments can be fed back to individuals. "Personalised risk assessments" or "risk stratification" might be misused by commercial interests, e.g. for direct marketing of supplements, drugs or medical tests (leading to over-treatment of healthy people) and could also lead to stigma and discrimination e.g. by employers and insurers. Risk assessments are currently unregulated and misleading assessments (made by computer algorithm) are already being sold (in some cases combined with products such as supplements). Genetic information also acts as a 'biometric' (tagging the individual's records to their physical self) and can be used to identify relatives (including non-paternity), so there is also potential for mass surveillance by governments, police or commercial interests or tracking down of individuals by anyone who can access the system (e.g. abusers, tabloid journalists). Because genetic information acts as a unique (or near-unique) identifier, anonymisation will not be achievable. Without fully informed consent about who is going to share their data for what purposes, there is a danger of a massive loss of public trust in medical research.

Access to information is relevant more broadly to GeneWatch's work. We make extensive use of the Freedom of Information Act (FoIA) and the Environmental Information Regulations (EIRs) and the EU Public Access to Documents Regulation. We regard these as important regulations to improve the transparency and accountability of government.

This submission draws on our extensive experience of working in these areas from a public interest perspective.

Q1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

Data protection is essential to maintain public trust in a wide range of services, including medical confidentiality in the NHS and security of financial information held by government (e.g. HMRC) and companies (e.g. banks). People need to know that their data is held securely and access and uses are restricted to what is necessary to provide the service. Otherwise public trust and confidence can be severely undermined.

Privacy is a right enshrined in the Council of Europe's Human Rights Convention (Article 8) and other international instruments. For example, the World Medical Association's Helsinki Declaration includes requirements to protect the "*dignity, integrity, right to self-determination, privacy and confidentiality of personal information of research subjects*".

In a health context, the advantages of protecting privacy include encouraging individuals to seek treatment without fear that relationships or employment prospects with be harmed if others become aware of their condition. More broadly, protection of privacy acts as a deterrent to authoritarianism, for example by restricting governments' ability to track political dissidents and persecute or stigmatise individuals or their families for their political beliefs, religion, ethnicity or genetic make-up, or based on any physical or mental impairment. It is difficult to quantify these benefits.

For business, the main benefit is maintaining public trust in services, which can be harmed by loss of personal data or by its misuse for services not requested or required by the individual (such as direct marketing). Individuals may be harmed in a variety of ways, including by commercial exploitation, financial loss, and mental distress if their personal data is misused. Trust in public services, including the NHS, tax collection, and government more broadly, is also essential to a functioning democratic society.

The EU's competence in this area is important because data (and interpretations of data) is increasingly flowing across borders and being used for multiple purposes. For example, an individual providing information to their doctor for medical purposes may find it feeding into a risk assessment being made by an insurer for entirely different purposes, or being used for personalised marketing. It is important that people can rely on assurances of medical confidentiality, even if their data is sent elsewhere in the EU (for example, as part of a European-wide research project) or stored on servers in the USA or China. Otherwise confidence may be lost in medical research (leading to reduced access to data) or in medical services (perhaps leading to people failing to seek medical care when they need it).

In 2008, the New Labour Government proposed over-ruling data protection laws through a data-sharing provision hidden in Clause 152 of the Coroners' and Justice Bill. This proposal was rapidly withdrawn after it became highly controversial.[4] One issue raised was the impact on people using the NHS in Scotland whose physicians would no longer be able to guarantee that the use of any patients' data sent to England would meet the conditions specified in consent forms: concerns about this issue led Scotland to withdraw legislative consent from Clause 152. Thus, if NHS England adopts policies which allow widespread data sharing without fully informed consent, based on narrow national rather than EU competency, this may prevent data from elsewhere being sent to England and/or restrict the use of NHS England data elsewhere in the EU. This would be harmful to legitimate medical research, which relies on common ethical standards.

Q2. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?

One source of evidence is the level of public concern about proposals to strip these rights away. For example, the Clause 152 proposals (described above) led to immediate objections which led to its withdrawal within a few weeks.[5] A similar backlash has greeted the recent care.data scheme, with proposals now on hold for at least six months. As soon as people become aware that the main aim of the proposal is not to share data within the NHS but to hand it all to Google, even greater levels of

concern are likely. Internationally, there is considerable evidence that allowing commercial access to medical records and biological tissue raises a wide variety of concerns.[6]

Other relevant research is the consultation in December 2008, conducted by Connecting for Health, about the sharing of medical data for research without consent.[7] The consultation did not mention that this would include sharing of genetic information, however the Human Genetics Commission (HGC)'s response included a large number of concerns raised by the HGC's Consultative Panel of members of the public, including concerns about sharing of data in "sealed envelopes" and the fact that "anonymisation" of data in a way that made individuals unidentifiable was likely to be impossible for rare disorders.[8] In its response to the consultation the Wellcome Trust Sanger Centre "*encouraged the NHS Care Records Service to prepare for the integration of significant amounts of genetic and genomic information into patient records*" and argued that: "*If robust systems are in place…….the benefits of research will outweigh the risks associated with the use of identifiable information*" (including information that patients have requested to be kept confidential in 'sealed' and 'locked' envelopes).[9] However, a quarter (25%) of the members of the public stated that they did not believe that it was possible to effectively anonymise data and some people were adamant that "their data" should not be shared for any purposes. There was wide concern amongst participants in the general public about the ability of the NHS to protect personal data. Concerns included risks of data loss by NHS staff, hacking and selling of data to third parties for commercial purposes, especially insurance companies and employers. The consultation revealed widely divergent views between the general public and researchers.

Allowing companies to rip people off, by using their medical records (and those of their relatives) for personalised marketing is not the same as "economic growth". Whilst it is true that many companies want to create a new market for sequencing and storing the DNA of every baby at birth and providing dubious (mis-)interpretations of it, this new market will not be created without enormous public subsidy and at great human cost. There are also significant opportunity costs as more useful areas of research and public health are increasingly neglected.

Q3. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

The new Data Protection Regulation is important for this (see Q4), plus a serious attempt to reform "Safe Harbour" and restrict the personal data stored or accessed by governments or corporations without people's consent, especially in the cloud. One of the most important major new technological developments is the ability to sequence the whole genome of every citizen and store it in the cloud. Contrary to much of the industry PR there is no medical purpose or benefit to this (although sequencing may be medically useful in more restricted circumstances i.e. for some babies with undiagnosed symptoms of a genetic disorder, or for some cancer tumours). Unchecked, it could lead to the total surveillance of the whole population, including by overseas intelligence agencies (e.g. the NSA or China), especially if new rapid DNA technology becomes widely used at borders.

Q4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

Proposals for a new EU Data Protection Regulation take into account new threats and challenges to privacy, such as plans to sequence large numbers of human genomes and store them in the cloud with electronic medical records (see Q10 and 11). Without these protections, there is a risk of a major loss of public trust and potentially a total loss of privacy as governments and corporations

develop the ability to track every individual and their relatives around the world and link all stored information about an individual to a single biometric (so "the computer knows who you are"). This can lead to commercial exploitation, government surveillance and individual loss of autonomy. Some people will be particularly vulnerable (minority ethnic groups, children, disabled people, the mentally ill, political dissidents, women and children fleeing abuse, people on witness protection schemes etc.).

Businesses that take privacy seriously will benefit from good regulation. Further, storing the whole genome of innocent citizens without consent is a clear breach of the European Convention of Human Rights (see the judgement in the case S. and Marper v. the UK, December 2008). Having legislation in place that makes this clear (rather than allowing a database to be built up and then dismantled as a result of litigation later) provides businesses with greater regulatory certainty, as well as protecting human rights.

Q5. What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

GeneWatch UK has made use of the right to access documents, for example by requesting documents relating to policy developments on the draft In Vitro Diagnostics (IVD) Regulation, which will cover how health claims for genetic tests are regulated. This kind of information allows us to input to policy debates from a public interest perspective (in this case, highlighting the consumer's need for reliable information on the clinical value of the tests). Without this information, business interests would be more likely to take precedence over the public interest (for example, by continuing to sell genetic tests with false or misleading claims).

Q6. How would UK citizens' ability to access official information benefit from more or less EU action?

GeneWatch UK would welcome a broader right to official EU information which is not restricted to official documents. In one instance the UK Government (Defra) refused us access to a copy of a letter sent by the GM industry to an EU official on the grounds that this was not covered by the FoIA, whereas letters and emails sent to UK officials and ministers by the industry were released to us. A broader right to official EU information would help improve public transparency and oversight of EU institutions and perhaps improve public confidence in the EU.

Q7. How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?

If the NHS is to function effectively, weak data protection rules in England could prove extremely problematic. Either data sent from Scotland and Wales will be re-used in England (or exported elsewhere) in ways which do not meet the original consent (breaching trust and local legislation), or data will not be sent to England from those countries with higher levels of protection. See the example of Scotland's withdrawal of consent to Clause 152 (response to Q1).

This could apply on a broader scale across the EU, making it harder for scientists in England to collaborate with EU research. If ethical standards are widely regarded as insufficient, data may not meet the requirements to be published in scientific journals or submitted to regulators.

Q8. Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

GeneWatch is not aware of any such evidence.

Q9. What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?

This question presumably refers to the EU Charter of Fundamental Rights. However, it makes little sense to make legislation that is not compliant with the right to privacy (which is also enshrined in the European Convention on Human Rights, which is binding on all EU member states). Good data protection will facilitate data flows and the EU's market in data by ensuring that the right to privacy is protected and the trust of data subjects is maintained. Without such trust there is no market (as explained above).

Q10. What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?

It has been proposed that people's entire genomes and electronic medical records could be stored in the cloud and shared with companies such as Google. As the Edward Snowden revelations showed, this data could then be accessed by intelligence agencies such as GCHQ and the US National Security Agency (NSA). It is likely that China and other countries have or are developing similar capabilities. This would allow governments to track every individual and their relatives, for example by testing DNA at borders (using new rapid on-the-spot DNA technology) and searching against databases. This would in effect mean the end of privacy: it can only be prevented by strengthening and enforcing existing safeguards, for example requiring fully informed consent and implementing the 'right to be forgotten'.

Q11. Is there any other evidence in the field of EU Information Rights that is relevant to this review?

Costs of sequencing DNA are reducing over time and a person's genotype (based on specific parts of their DNA) acts as a biometric (a 'genetic fingerprint') by linking their physical presence to any database in which their genotype or genome is stored. Searching for partial matches can also identify relatives and non-paternity.

Opposition to the draft EU Data Protection Regulation is being driven largely by Google and medical research funders (especially the Wellcome Trust) who hope to be involved in a proposed public-private partnership to sequence all NHS users and store their genomes as attachments to electronic medical records. Google would calculate personalised health risk assessments by data-mining this data and feed them back to individuals via their online medical records. Whilst DNA is not expected to be collected without consent in the NHS, it may be sequenced without consent as a 'secondary use' (e.g. by using the millions of stored babies' blood spots) or else sequenced for a medical or research purpose but then stored for secondary uses and shared with companies such as Google without the knowledge of the individual (or their parents, in the case of a baby or child): this type of 'broad consent' is being piloted by the 100,000 Genomes Project. Whilst the 100k Genomes Project states it will store the data on its own servers and require commercial researchers to visit its physical location, the long-term plan for a whole population database is to store the data in the cloud. In this way, Google hopes to get around the requirement to obtain individual informed consent before processing people's genomes and medical data, with the aim only of obtaining consent to feedback

of risk assessments later on (after they have already been calculated and the privacy risks of storing and sharing the data, and its enormous costs, have already been taken). This is a deliberate attempt to undermine the example given in paragraph 86, in which explicit consent is required before processing health data. It also undermines to right to object to direct marketing (para 76) because Google will only make a profit from this plan if it can monetise the data by using it to sell products such as medicines, supplements, functional foods or further medical tests (or perhaps also by selling to third parties such as insurers). Thus marketing is being dressed up as 'research'. Finally, it would allow a DNA database to be built by stealth in the NHS, in contravention of Article 8 of the European Convention on Human Rights.

The new EU Data Protection Regulation rightly includes a requirement for explicit prior informed consent before processing data for medical research and this is the real reason why the UK Government is objecting to EU competence in this area. However, it should be noted that if EU competencies were reduced:

(i) There would still be a major risk in terms of loss of public trust in proceeding with this plan;

(ii) Legal challenges would probably be inevitable because Article 8 of the European Convention on Human Rights and other safeguards would still apply (although a challenge in the ECtHR might take a decade to play out);

(iii) Major problems would arise in transfer of NHS data in and out of England (to/from Scotland, Wales, Northern Ireland), due to lack of equivalent data protection standards in England compared to the rest of the UK;

(iv) Problems would also be created in relation to transfer of data within the EU (for example, for medical research);

(v) People's right to privacy would be irretrievably damaged since shared data may not be retrievable and DNA can be used to track an individual and their relatives.

For further information contact:

Dr Helen Wallace
Director
GeneWatch UK
60 Lightwood Rd
Buxton
SK17 7BB
Email: helen.wallace@genewatch.org
Tel: 01298-24300
Website: www.genewatch.org

References

[1] Children could have DNA tested at birth. The Telegraph. 8th December 2013. http://www.telegraph.co.uk/health/healthnews/10501788/Children-could-have-DNA-tested-at-birth.html

[2] Our Genomic Future: What would happen if we all had our genome sequenced? Nesta, London Event 2nd July 2014. http://www.nesta.org.uk/event/our-genomic-future

[3] A DNA database in the NHS: Your freedom up for sale? GeneWatch UK. May 2013. http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAinNHS_GWbriefing_fin.pdf

[4] Straw bows to pressure over data sharing. The Observer. 8th March 2009. http://www.theguardian.com/technology/2009/mar/08/data-sharing-civil-liberties

[5] Government abandons data-sharing scheme. The Telegraph. 7th March 2009. http://www.telegraph.co.uk/news/uknews/law-and-order/4954058/Government-abandons-data-sharing-scheme.html

[6] Caulfield T, Burningham S, Joly Y, Master Z, Shabani M, Borry P, Becker A, Burgess M, Calder K, Critchley C, Edwards K, Fullerton SM, Gottweis H, Hyde-Lay R, Illes J, Isasi R, Kato K, Kaye J, Knoppers B, Lynch J, McGuire A, Meslin E, Nicol D, O'Doherty K, Ogbogu U, Otlowski M, Pullman D, Ries N, Scott C, Sears M, Wallace HM, Zawati MH (2014) A review of the key issues associated with the commercialization of biobanks. Journal of Law and the Biosciences, 94–110. http://jlb.oxfordjournals.org/content/1/1/94.full.pdf

[7] Connecting for Health (2008) Consultation on the wider use of patient information.

[8] HGC (2008) NHS Connecting for Health – Consultation on Public, Patients, and other interested parties views on Additional Uses of Patient Data: Response by the Human Genetics Commission. 15 December 2008.

[9] NHS Connecting for Health (2009) Summary of responses to the consultation on additional uses of patient data. 27th November 2009. http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Consultations/Responsestoconsultations/DH_109310