Human Brain Project HP

Ethics & Society

Nr. 6 · April 2018

Danish Board of Technology (DBT)

Beyond the legal requirements of data driven research

Data on patients and research participants stored in hospitals around the world provide a valuable resource for research. The Human Brain Project (HBP) hopes to use these valuable health databases for its research on providing more accurate diagnoses and personalized medicine for brain diseases. With the incoming General Data Protection Regulation (GDPR), such research raises questions on appropriate data governance and informed consent, but also about trust and societal values.

This brief reports on the outcome of a seminar held in December 2017 at which HBP researchers joined with leading neurologists, personal data managers, bioethicists, legal advisers and patient representatives to discuss the ethical and legal challenges to setting up and participating in data driven research.

A number of health related data projects have failed due to lack of public trust. A well-known example is NHS England's health care programme 'care.data', a gigantic database which tried to collect patient records from all over Britain to improve diagnoses and medical treatments. The programme collapsed shortly after it was launched in 2014; essentially because the public did not trust that the benefits of running this health database would override the risks.

The example of care.data demonstrates that although the intentions are good, data driven research initiatives will not succeed if personal data is not sufficiently protected and if the data stakeholders are not sufficiently informed about the risks and benefits of participating.

Care.data and other failed big data projects illustrate the potential tension between privacy rights and the benefits to society. Prof. Jo Samanta, keynote speaker at the seminar, emphasised that this tension may have huge consequences for data driven research initiatives such as the Human Brain Project (HBP). According to Samanta we need to address this growing tension by not only protecting privacy rights, but also by informing about the benefits to society:

"Data stewardship includes finding ways to inform research participants in a comprehensive and transparent way about how their data is used and how this contributes to the public good." (Samanta)

Recommendations to the HBP:

- Highlight the success stories that the public cares about.
- Make a solid engagement plan.
- Develop patient friendly resources and communication.
- Consider having an ethical spokesperson.
- Write a peer reviewed article on the anonymization approach in HBP.
- Organize a Data Protection Impact Assessment (DPIA) review of the updated data sharing strategy of the Medical Informatics Platform

The GDPR and personal data

The EU's General Data Protection Regulations (GDPR) represents a comprehensive reform of data protection regulations across the European Union. It aims to facilitate appropriate safeguards to ensure that personal data is used adequately while protecting privacy and enhancing public trust.

Consent is a lynchpin in legal and ethical research and is the primary policy device to legitimise research involving personal data, but as stated throughout the seminar, consent could not and should not stand alone.

The premise of informed consent is that the person consenting is an adult subject who understands the purpose of the research, the benefits to the individual and to society, the risks of being involved and the alternatives for not involving.

According to the participants, this ideal situation rarely exists in reality and becomes particular difficult when collecting data from mentally disabled people or children. Prof. Wim Pinxten, who presented during the seminar, emphasised that:

"Informed consent was not designed for non-communicative people." (Wim Pinxten)

Likewise, it was not designed for complex research initiatives that may have impact that reach far into the future or reuse the data for several purposes. In data driven research like the HBP, it may e.g. be impossible to provide the subject involved with precise information about the research in which they are about to participate.

The GDPR addresses this problem by introducing 'broad consent', but as argued by the seminar participants, it does not solve the fact that many people participating in research are unable to consent.

Anonymous harm

Within the HBP the problem of consent is to some extend being addressed by anonymizing and depersonalizing all clinical data at the hospitals. Anonymization is valuable in many situations, but like consent, it also has its drawbacks. According to the seminar speaker Prof. Josep Domingo-Ferrer the paradox of anonymization is that:

"Too little anonymization may be insufficient to prevent re-identification, whereas too much anonymization may hinder big data construction. A midway path is not yet ready." (Domingo-Ferrer)

One other implication of anonymization raised by the participants is that it may not always be clear whether a level of anonymization is sufficient to meet the legal definition of "anonymous" data.

As stressed by Domingo-Ferrer, the data controller may avoid the extra burden of managing personal data by achieving the legally required (very low) risk, irrespective of data utility. Likewise, data controllers may claim that data are anonymous while "competing" agents will try to show that it can be re-identified.

Thus, according to Domingo-Ferrer big data anonymization should be accomplished by two desiderata: 1) Anonymized big data that are published should yield results similar to those obtained on the original big data for a broad range of exploratory analyses. 2) Anonymized data should not allow univocal reconstruction of any subject's profile. Despite the issues with anonymous data, Domingo-Ferrer stressed that anonymization is perhaps one of the few solutions that you can use to cope with the scientific demands, but the quality has to be checked.

As an alternative to anonymization, Dr. Michele Loi recommended a model where all data are treated as personal data with anonymization as a safeguard. Such *"adequately anonymized*

personal data" would according to Loi be desirable since different degrees of anonymization are reasonable in different contexts.

The value of data control

While re-identification of anonymous data is an issue by itself, many ethical concerns related to anonymization remain and particularly the loss of data control was repeatedly mentioned by the seminar participants as a major drawback of anonymization. Anonymization will e.g. eliminate the option of withdrawing from research or tracking how your data is being used. Dr. Alessandro Blasimme, chair at one of the seminar sessions, emphasized the need for control as follows:

"Data control is not to be understood as an absolute value, but as a precondition for other states and values, including autonomy, self-determination, privacy, trust, transparency, and accountability." (Blasimme)

Part of the reason, according to Blasimme, is that data nowadays are everywhere, come from different sources, and no-longer include only traditional clinical data, but also data related to people's ordinary lives. The conventional distinctions between health-related and other kinds of data have become blurred and created a growing mistrust towards the online environment that might spill over to data driven research initiatives.

There was general agreement among the seminar participants that people should have more control of their own data, but it was unclear from the discussion where in the system the control mechanisms should be.

Also, the seminar participants emphasized that it could never be ethical to give people control over more than their own individual participation.

Data sharing based on a web of trust

Neither consent, nor anonymization or data control could, according to the participants, handle the whole array of expectations around what is available with data these days. Rather than focusing on the legal measures and other sorts of documentation for creating trust, Ma'n H. Zawati argued that data sharing must be seen from a multilateral and relational perspective as a web of trust between multiple stakeholders: biobanks (as an example), participants, the public, and researcher communities.

Zawati furthermore emphasized that trust towards biobanks and data sharing platforms should be created and maintained between the stakeholders based on a system of reciprocity:

"According to authors[1], the concept of reciprocity is motivated by the view that individuals will help or benefit others at least in part because they have received, will receive, or stand to receive beneficial assistance from them." (Zawati)

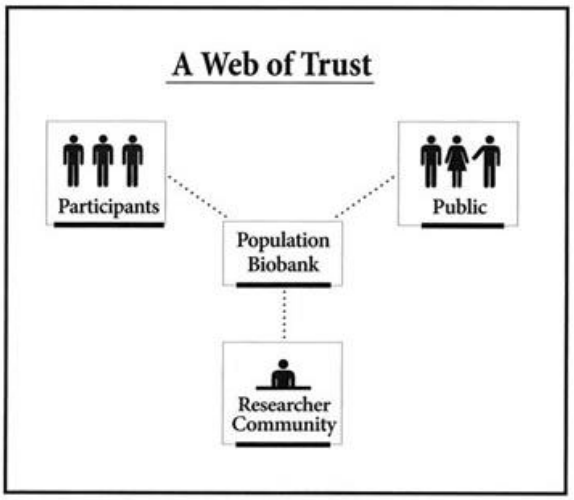

Fig 1: Population biobank Web of Trust (Zawati[2])

[1] Tom Beauchamp and James Childress, Principles of Biomedical Ethics, (New York: Oxford University Press, 2009), 6th edition at 103

[2] Zawati, Ma'n H. "There will be sharing: population biobanks, the duty to inform and the limitations of the individualistic conception of autonomy. "Health law Journal, Annual 2014, p. 97

In this way Zawati sees the relationship between (e.g.) population biobanks and the participants as a relationship based on respect rather than documentation:

"The biobank provides protection of privacy and ongoing communication, but more importantly it provides participants with a feeling of contributing to a greater goal." (Zawati)

According to Zawati, a relationship with the data stakeholders based on reciprocity will motivate more people to participate, create more collaboration, and maximize the statistical power. Hopefully the knowledge will in this way be translated to the clinics, which will result in better health for the population.

Hospitals were mentioned as useful entrances to engage with the data providers and as a starting point for community building. Additionally, engagement with patient organizations and support groups was mentioned to help develop more patient friendly resources such as dementia friendly communication.

Future directions

With the GDPR and an increasing number of data driven research initiatives, we are facing a paradigm shift in the way we collect and process personal data. As noted by Dr. Simisola Akintoye who chaired one of the seminar sessions:

"New and enhanced measures imposed by the GDPR must be adhered to by the HBP as a beacon for good practice and as a model for legal and ethical compliance." (Akintoye)

The GDPR will in this way provide a framework for collecting and protecting personal data, but according to the seminar participants HBP should go beyond the legal requirements for data governance and base its data governance on several personal and societal values that include data privacy but also address data control, reciprocity, reliability, engagement, societal utility and trust.

This brief is based on discussions from a seminar organised by HBP Ethics and Society group, December 2017 in Paris. More information about the seminar can be found at www.hbp.tekno.dk.

Authors:
Karen Riisgaard[1]
List Bitsch
Martin Bejder Nielsen[1]
Jo Samanta[2]
Simisola Akintoye[2]

[1]Danish Board of Technology Foundation
[2] University de Montfort, Faculty of Business and Law

While every caution has been taken to represent the views of the participants quoted in this newsletter accurately, the final representation remains the responsibility of the author(s). The views and opinions expressed in this newsletter may not be taken as those of the HBP or any of its sub-projects.

The newsletter may be freely copied and distributed to the interested parties. Citation may only occur with proper referencing and including a link to www.tekno.dk

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 720270 (HBP SGA1).

Co-funded by