Short public response to the Ofcom Call For Evidence on Regulated Online Services Information from medConfidential.org

Edge cases determine success or failure. We have tried to keep this short, but could easily have written pages and pages on nuanced topics we condensed down into half a line. We're happy to meet and address topics you find useful further – this is outside our core remit, but it is important that the model is right to avoid catastrophic damage to the notion of research.

medConfidential offers some experiences from the decades of use and abuse of health data as illustrations and tests for the challenge facing OfCom and DSIT. Some of those lessons are directly relevant, some of them are cautionary tales of unintended consequences.

You are designing multiple processes – an application process (what does an applicant want to do?), a decision process (can/should they do it?), a research process (how do they do it?), and an output process (how do others find out?) – all are mixed together in this consultation. Whatever is decided, an informed public (or user base) requires that there must be a full list of projects disclosing what data was accessed and why – NHS England calls this a data uses register, and projects should be mandated to publish any outputs freely online, even (and especially) null results so the users can read them if they wish.

Access to the database of the full medical history of anyone who has had cancer in England[1] received an application for a "causes of cancer" project; only later did someone spot that it was being run by a tobacco company. Also believing "more is more" on access, Biobank pared back their application process until it was so weak they gave half a million genomes to self-proclaimed eugenicists; two weeks *later* a Government review written by Biobank's former Chief Scientist lauded their governance and suggest it be the model for approvals.

There are many organisations and ecosystems that have examined how to do research access before, and whose experience and pitfalls would be beneficial to OfCom and DSIT. Those include the Data Access Request Service (DARS) team at NHS England, and the Senior Data Governance Panel at the Ministry of Justice. This is hard, there are tradeoffs, and vested interests argue neither is true. We simultaneously argue that the DARS team do a very good job in some respects while not doing enough in various others (often for policy reasons–they implement the stated policy well, usually, but the stated policy may be unwise).

The criteria must be clear, must be objective, and must be transparent, which also means they will be gamed by hostile interested actors. The UK Biobank insists they have blacklisted eugenicists while seeing no problem giving data to a directly related entity – there can be distinctions drawn for self-interested reasons without there being any material differences. What are the criteria that should be prohibited for projects looking at social media posts on contentious topics? Does nationality matter? Does their funding? Does the question they're asking? The NHSE DARS process includes this information for some situations, but it is not perfect. The "five safes" framework may be useful; but everything will get gamed.

[1] At the time it was the Public Health England Cancer Registry, and is now the NHS Cancer Registry, largely because giving cancer patient data to a tobacco company is terrible.

The Interests of Data Subjects

Research is important and necessary, but it is far from clear how this will operate. As the model of access firms up, should it be mandatory for all users' content to be included – should a data subject have the right to choose not to be the subject of research? If there is no opt-in (or a process where making an in/out choice is mandated), the process must be reasonable and acceptable to the majority of users, and not harm particular subgroups. This is likely to be different per platform, per community, and some will legitimately diverge.

What restrictions can be placed on the data such that an independent researcher publishes the "top5 viral posts on war crimes" in a particular conflict, only for the perpetrators of those crimes to use facial recognition to go looking for the people who posted them? What happens when the research subject is the company? Or the platform? Or the people on it?

Companies should not be allowed to blacklist applications merely because they disagree with the applicant, but they should be able to reject applicants for other reasons as vague as "we can't trust them". This is inherently subjective, yet should not be subjective, and is almost impossible to do without data subjects giving some steer on the scope of research they would like data used in (all/some/none). More distinctions without differences.

There are corporate entities who would do "online safety" research to target and undermine their competitors, or to undermine the measures that companies take to protect their users. These differences can be nuanced – an organisation saying "we believe in human rights" and "work in the public interest" or to "further the best interests of others", is good, but an organisation who believes that there are no more rights than are countable on one hand is not quite the same, and whose interests and definitions prevail will be up to … whom?

Will OfCom's rules about mandatory access cover those posts made by users prior to those rules coming out? Ie posted without knowing they'd then become experimental rats in a social media cage (possibly) without any choice. Is that what OfCom wants?

All access processes will be defined by their edge cases – the day before she died, should Molly Russell's social media account have been in the dataset? Should it be in there today, even as some of her private posts have been publicly released by the family, and even if accounts were pseudonymised, she and others can be reidentified from those posts and the pseudonym links to all posts the family did not disclose? Who should see that data? What should they be able to do? What do researchers want to do? Do those constraints apply to those who are still alive and do those constraints apply to others who are not?

medConfidential