YALE UNIV.

Reboot ethical review for the age of big data

Forty years on from a foundational report on how to protect people participating in research, cracks are showing, warns **Nathaniel Raymond**.

One of the primary documents aiming to protect human research participants was published in the US Federal Register 40 years ago this week. The Belmont Report was commissioned by Congress in the wake of the notorious Tuskegee syphilis study, in which researchers withheld treatment from African American men for years and observed how the disease caused blindness, heart disease, dementia and, in some cases, death.

The Belmont Report lays out core principles now generally required for human research to be considered ethical. Although technically governing only US federally supported research, its influence reverberates across academia and industry globally. Before academics with US government funding can begin research involving humans, their institutional review boards (IRBs) must determine that the studies comply with regulation largely derived from a document that was written more than a decade before the World Wide Web and nearly a quarter of a century before Facebook.

It is past time for a Belmont 2.0. We should not be asking those tasked with protecting human participants to single-handedly identify and contend with the implications of the digital revolution. Technological progress, including machine learning, data analytics and artificial intelligence, has altered the potential risks of research in ways that the authors of the first Belmont report could not have predicted. For example, Muslim cab drivers can be identified from patterns indicating that they stop to pray; the Ugandan government can try to identify gay men from their social-media habits; and researchers can monitor and influence individuals' behaviour online without enrolling them in a study.

Consider the 2014 Facebook 'emotional contagion study', which manipulated users' exposure to emotional content to evaluate effects on mood. That project, a collaboration with academic researchers, led the US Department of Health and Human Services to launch a long rule-making process that tweaked some regulations governing IRBs.

A broader fix is needed. Right now, data science overlooks risks to human participants by default. In 2016, data scientists Jacob Metcalf and Kate Crawford first articulated an inherent flaw in the protection of human research participants: guidelines wrongly assume that data that are already public cannot pose new threats and so exempt the use of such data from review (J. Metcalf and K. Crawford *Big Data & Society* January–June; 2016). Recently, a council convened by the US National Science Foundation to lay groundwork for big-data ethics concurred. It concluded that technology had created "mismatches" between conventional ethical paradigms for protecting individuals and new sorts of "informational harm".

Data science can aggregate publicly available data to create and classify new groups of individuals. That can pose threats to privacy, security and dignity. For example, purchasing patterns can allow retailers such as Target to identify women who might be pregnant, and researchers have been able to re-identify individuals almost 90% of the time from supposedly anonymized credit-card data.

Two new types of group data are inappropriately exempted in some cases by current guidelines. The first is demographically identifiable information — data that allow inferences to classify, identify or track people (named or unnamed) or groups of people according to ethnicity, economic class, religion, gender, occupation, health status or other combinations of factors. The second is what I call action-based information, such as mobile-device data that reveal time and place-specific behaviour.

CONTINUED ACCEPTANCE OF THE LACK OF GUIDELINES IS AN ABROGATION OF THE RESEARCH COMMUNITY'S ETHICAL DUTIES.

IRBs need help to assess these risks. How do Belmont principles apply to methods that use publicly available data to identify people who died from opioid overdoses? What new machine-learning methods for leveraging mobile-phone data to trace contacts might expose vulnerable populations, such as people with HIV, to social stigma and exclusion from services if the data become public?

The scientific community needs agreed-on frameworks to cope with these sorts of group data. Tweaks to existing rules are not sufficient. Nor is another round of working groups and 'call to action' articles. The European Union's General Data Protection Regulation provides some defence (in some countries) against misuse of online data, but protection for research is sorely lacking.

Continued acceptance of the lack of guidelines is an abrogation of the research community's ethical duties. We should call on Congress, in parallel with international bodies such as the World Health Organization, to authorize a national commission to write another Belmont Report to deal holistically with applications of data science that will only become more complicated as technology progresses. IRBs can help by capturing what big-data research has and has not been considered exempt, and publishing cases of how specific ethical challenges might best be addressed. This will not eliminate risks or rein in all bad practice. But it would be a pivotal step towards encouraging international harmonization of disparate approaches to difficult questions that face researchers around the world.

Belmont 2.0 can ensure the clear benefits of big-data research are adequately balanced against poorly understood risks and harms. It should not require abuses on the scale of the Tuskegee syphilis study to prompt us to create guidelines fit for the digital world. ■

Nathaniel Raymond *researches how information technologies affect human rights and security at Yale University's Jackson Institute of Global Affairs in New Haven, Connecticut.*
e-mail: nathaniel.raymond@yale.edu