COMPUTER LAW & SECURITY REVIEW 44 (2022) 105655

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

Using public data to measure diversity in computer science research communities: A critical data governance perspective

Rachelle Bosua[a,b,*], *Marc Cheong*[b], *Karin Clark*[c], *Damian Clifford*[d], *Simon Coghlan*[b], *Chris Culnane*[b], *Kobi Leins*[e], *Megan Richardson*[f]

[a] *Information Sciences, Faculty of Science, Open University of The Netherlands, Valkenburgerweg 177, 6419 AT Heerlen, The Netherlands*

[b] *Computing and Information Systems (CIS), The University of Melbourne, Royal Parade, Parkville 3010, VIC, Australia*

[c] *Melbourne Law School, The University of Melbourne, Royal Parade, Parkville 3010, VIC, Australia*

[d] *ANU College of Law, Australia National University, 5 Fellows Rd, Acton ACT 2600, Australia*

[e] *Department of War Studies, King's College, London, Strand London WC2R 2LS United Kingdom*

[f] *ARC Centre of Excellence for Automated Decision-Making and Society Professor Melbourne Law School, The University of Melbourne, Royal Parade, Parkville, 3010, VIC, Australia*

ARTICLE INFO

Keywords:
Privacy
Data protection
Public data
Diversity
Critical data governance

ABSTRACT

Encouraging and supporting diversity and inclusion in computer science research communities is a critical issue for many reasons, including the ethical and robust design, delivery and publication of research that addresses real-world situations ranging from the use of digital tools in health to predictive policing to workplace hiring practices, just to name a few. One way to measure diversity is to apply analytical research methods to data sourced from the public domain for use in research. However, attempts to measure diversity using public data may themselves raise legal and ethical questions about the provenance of the data, research methods adopted, and treatment of diversity in the publication of results. This article interrogates the challenges of measuring diversity using public data, examining an illustrative case study framed around an academic research project at an Australian university using a public data set to identify gender representation in computer science communities. Employing a critical data governance perspective, we point to a range of ethical and legal concerns and recommend greater regulatory guardrails to better balance public interests in research and the privacy, data protection and other ethical interests of research subjects.

* Corresponding author.
E-mail address: rachelle.bosua@ou.nl (R. Bosua).

https://doi.org/10.1016/j.clsr.2022.105655

1. Introduction

Over the last decade, the 'big data revolution' has created many new opportunities.[1] Accompanying the growth in publishing and sharing of data, analytical methods drawing on complex algorithms, artificial intelligence (AI) and machine learning (ML) have evolved exponentially – yielding novel insights and extending interventions in areas formerly too expensive or cumbersome to explore. As a result, the enthusiasm for access to large open data sets has grown globally, encouraging the use of these sources to find possible solutions to some of the most complex problems the world faces today. Access to public data (often referred to as 'public use data') – i.e., data that can be freely drawn on without the need to obtain formal approval – thus holds great promise for researchers as a tremendously rich and low-cost resource.

The increase in research on large public data sets makes it even more important to ensure intersectional diversity of the research communities engaged in such research, because of the speed, scale and potential real-world impact of such research. Establishing and maintaining diversity and supporting inclusion in research communities is a critical issue for many reasons, including the ethical and robust design, delivery and publication of research that addresses real-world situations ranging from the creation of digital tools in health to the use of computer science in predictive policing to workplace hiring practices, just to name a few.[2] As Crawford observes, '[l]ike all technologies before it, artificial intelligence will reflect the values of its creators'.[3] Such observations are consistent with the findings of management studies, confirming that diversity in teams and communities is not only ethically desirable but positively linked to improvement in performance and innovation.[4] Likewise, cultural diversity is becoming recognized as a critical issue for computer science research (CSR) communities, with implications not only for ethics but for the robust design and risk management of research projects.[5] Nevertheless, despite what is sometimes referred to as 'ethification' of computer sciences, in reality change is happening slowly and guidance is not consistent across these communities.[6]

That the use of public data for research may pose ethical and methodological challenges is not new.[7] However, the speed, scale and scope of the use of AI and ML systems risk harming individuals or communities whose data is being used, often without consent or even knowledge.[8] One real risk is identities that were previously considered to be 'deidentified' can now be revealed through CSR methods. In addition, sensitive inferences (true or false) can be drawn in ways that were previously unanticipated. And research projects them-

[1] See Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34 Computer Law & Security Review 754; Yanqing Duan, John S Edwards and Yogesh Kumar Dwivedi, 'Artificial Intelligence for Decision Making in the Era of Big Data – Evolution, Challenges and Research Agenda' (2019) 48 International Journal of Information Management 63; Katharina Sielemann, Alenka Hafner and Boas Pucker, 'The Reuse of Public Datasets in the Life Sciences: Potential Risks and Rewards' (2020) PeerJ 8:e9954 <https://doi.org/10.7717/peerj.9954> accessed 7 May 2021.

[2] See, for instance, Annaliese K Beery and Irving Zucker, 'Sex Bias in Neuroscience and Biomedical Research' (2011) 35 Neuroscience and Biobehavioral Reviews 565; C J Kahane, 'Injury Vulnerability and Effectiveness of Occupant Protection Technologies for Older Occupants and Women' (US National Highway Traffic Safety Administration, May 2013) <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811766> accessed 7 May 2021; Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (2018) 81 PMLR 77; Maria De-Arteaga, Alexey Romanov, Hanna Wallach, Jennifer Chayes, Christian Borgs, Alexandra Chouldechova et al., 'Bias in Bios: A Case Study of Semantic Representation Bias in a High-stakes Setting' (Proceedings of the Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery, 2019) 120-128 <https://arxiv.org/abs/1901.09451> accessed 7 May 2021; Caroline Criado-Perez, *Invisible Women: Data Bias in a World Designed for Men* (Abrams Press 2019).

[3] Kate Crawford, 'Artificial Intelligence's White Guy Problem' *New York Times* (New York, 26 June 2016) <www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html> accessed 7 May 2021. Cf Susan Leavy, 'Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning' (*2018 IEEE/ACM 1st International Workshop on Gender Equality in Software Engineering (GE)*, Gothenburg, Sweden, 2018) 14-16 <https://ieeexplore.ieee.org/document/8452744> accessed 7 May 2021.

[4] Sandel Hoogendoorn, Hessel Oosterbeek and Mirjam van Praag, 'The Impact of Gender Diversity on the Performance of Business Teams: Evidence From a Field Experiment' (2013) 59 Management Science 1514; Anna-Lena Claeys-Kulik, Thomas Ekman Jørgensen and Henriette Stöber, 'Diversity, Equity and Inclusion in European Higher Education Institutions: Results from the INVITED project' (European University Association, 19 November 2019) <https://eua.eu/resources/publications/890:diversity,-equity-and-inclusion-in-european-higher-education-institutions-results-from-the-invited-project.html> accessed 7 May 2021.

[5] Louise Ann Lyon and Jill Denner, 'Broadening Participation: Community Colleges: A Resource For Increasing Equity and Inclusion in Computer Science Education' (2017) 60 Communications of the ACM 24; Casey Haines, Evangeline Rose, Karan Odom and Kevin Omland, 'The Role of Diversity in Science: A Case Study of Women Advancing Female Birdsong Research' (2020) 168 Animal Behaviour 19; Alicia Nicki Washington, 'When Twice as Good Isn't Enough: The Case for Cultural Competence in Computing' (SIGCSE '20: Proceedings of the 51st ACM Technical Symposium on Computer Science Education, February 2020) 213-219 <https://doi.org/10.1145/3328778.3366792> accessed 7 May 2021.

[6] https://arxiv.org/abs/2109.06598 Niels van Dijk, Simon Casiraghi, and Serge Gutwirth, 'The 'Ethification' of ICT Governance. Artificial Intelligence and Data Protection in the European Union' (2021) 43 *Computer Law & Security Review* 105597. See also Anna Rogers, Tim Baldwin, Kobi leins, 'Just What Do You Think You Are Doing, Dave?' A Checklist for Responsible Data Use in NLP (2021) Findings of EMNLP < https://arxiv.org/abs/2109.06598>, accessed 14 October 2021.

[7] Sue Newell and Marco Marabelli, 'Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of "Datafication"' (2015) 24 Journal of Strategic Information Systems 3; Effy Vayena, Marcel Salathé, Lawrence C Madoff and John S Brownstein, 'Ethical Challenges of Big Data in Public Health' (2015) 11 PLoS Computational Biology e1003904 <https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1003904> accessed 7 May 2021.

[8] Chris Culnane, Benjamin I P Rubinstein and Vanessa Teague, 'Stop the Open Data Bus, We Want to Get Off' 2019 arXiv https://arxiv.org/abs/1908.05004 accessed 7 May 2021; Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2020) 36 Law in Context 1.

selves may involve processes or subject matter which their subjects or communities would almost certainly not approve. Harm here can include different things – e.g., unfair targeting, stigmatization, lost opportunities for employment and other financial benefits, manipulation of behavior, and invasions of privacy associated with the abusive treatment of deeply personal sensitive attributes of individuals or groups.[9] But how broadly should harm be construed in this context, for instance when it comes to the ethical judgments of research subjects about the research being conducted?[10] Or, for that matter, when it comes to judgments of both research subjects and those left out of the research about the "norms values and assumptions" embedded in the data sets?[11] Even determining what constitutes public data can itself be a challenge, with implications for assessments of harm. Is data that is publicly available to be considered 'public data' irrespective of how it came to be publicly available – for instance, if it is the result of a hack or other unauthorised access?[12] Finally, the open question remains about what frameworks should govern public data sets which have been compiled from material in the public domain.

In view of these issues, this study focuses on the research question: *How can the exposure or appropriation of personal data in the processing of public data be managed?* The following subquestions are asked and addressed: *What are the tradeoffs between individual rights and interests and the common good? How can the thresholds for such tradeoffs be determined? Who gets to decide what those thresholds should be within a given community?*[13]

Specifically, the aim is to identify a range of legal, ethical and methodological concerns that relate to the use of public data in academic research into diversity and to offer some balanced potential solutions as to how these concerns can be managed. The article is structured as follows. Section 2 first starts by describing competing tensions that relate to the processing of public data for research purposes, identifying ethical challenges of academic research conducted on public data. In Section 3 we highlight these concerns through an illustrative case study framed around an academic research project at an Australian university using public data to identify gender representation in academic research publications of CSR communities. Section 4 presents a critical data governance perspective and considers three regulatory models that can be applied to address the challenges associated with the use of public data in academic research. These models range from the high-regulation approach of the EU General Data Protection Regulation (GDPR)[14] and proposed EU Data Governance Act (DGA),[15] to the more low-regulation US and Australian legal approaches, which in the latter case is bolstered to an extent by university ethics standards but with so far patchy or unclear application to public data (which we argue needs to be addressed). In the conclusion and recommendations (Section 5), we draw together the article's arguments and suggest some practical approaches to governance and other strategies to balance public interests in research and the interests of research subjects and other stakeholders.

2. Processing of public data for research – tradeoffs and competing tensions

Over the last few years, there has been significant change in thinking regarding the appropriate ethical foundations for the protection of personal data and the rights of those to whom the data relate (i.e., data subjects). Driven by an increase in digitalization and the rise of digital platforms that collect personal data, the need for accountable, fair, transparent, and lawful processing of personal research data has become a predominant concern, reflected inter alia in the adoption of the EU GDPR. The EU approach to data protection as a fundamental right as recognized in the Charter of Fundamental Rights of the European Union (the EU Charter)[16] and protected in the GDPR in particular, can be considered a landmark in establishing fair and ethical principles for the processing of any personal data, including public research data falling within its scope. It is a core feature of the protections afforded to personal data in the GDPR that they apply even to information in the public domain reflecting the fact that the right to data protection safeguards individuals against the processing of personal data and not the maintaining of confidentiality in a strict sense.[17] Indeed, there is an ongoing academic debate

[9] See Damien Clifford, Megan Richardson and Normann Witzleb, 'Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection Laws' in Mark Findlay, Jolyon Ford, Josephine Seoh and Dilan Thampapillai (eds), *Regulatory Insights on Artificial Intelligence: Research for Policy* (Edward Elgar 2021).

[10] See Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (Pew Internet Survey, 15 November 2019) <www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information> accessed 7 May 2021.

[11] As to which, see Emily Denton, Alex Hanna, Razvan Amironesei, Andrew Smart, Hilary Nicole, 'On the Genealogy of Machine Learning Datasets: A Critical History of ImageNet' (2021) Big Data & Society .

[12] Nathaniel Poor and Roei Davidson, 'The Ethics of Using Hacked Data: Patreon's Data Hack and Academic Data Standards' [2017] Internet Research Ethics for the Social Age 278; Anne E Boustead and Trey Herr, 'Analyzing the Ethical Implications of Research Using Leaked Data' (2020) 53(3) Political Science & Politics 505.

[13] Kobi Leins, Jeyhan Lau and Tim Baldwin, 'Give me Convenience, But Give her Death: Who Should Decide What Uses of NLP are Appropriate, and on What Basis?' 2020 arXiv https://arxiv.org/abs/2005.13213 accessed 7 May 2021.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[15] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.

[16] Charter of Fundamental Rights of the European Union [2000] OJ C364/01. The Charter became legally binding as part of the constitutional law of the EU when the Treaty of Lisbon entered into force on 1 December 2009.

[17] It is well-accepted that the GDPR applies to personal data in the public domain but for a relevant discussion reference can be made to European Data Protection Supervisor, 'A Preliminary Opinion on data protection and scientific research' (6 Jan-

as to the nature of the right to data protection itself in EU law, with some questioning whether the right can be construed permissively as a series of rules or checks and balances.[18] This seems to echo De Hert and Gutwirth's analysis of the contrast between the rights to privacy and data protection when they suggest that data protection promotes transparency whereas privacy facilitates opacity.[19]

Leaving these specific debates to one side, it is clear that the EU approach to concerns related to the increasing reliance on personal data (including research data) was intended to strengthen the protections afforded in hard law. A more detailed look at the GDPR however, demonstrates a tension at the core of the framework. This tension is indicative of the debate relating to the very essence of the right and its non-absolute nature. The GDPR aims to protect (and balance the protection of) personal data and other fundamental rights and interests, and to facilitate the free flow of personal data in the EU through a harmonized level of protection. One example of this facilitation of the free flow of personal data is in the context of the use of personal data for scientific research purposes. Indeed, the Regulation aims to balance the protection of research data falling within the definition of personal data and the legitimate and beneficial use of this information for both public and private research purposes. Although the GDPR does not define 'scientific research purposes', Recital 159 states that it should be interpreted broadly and includes 'for example technological development and demonstration, fundamental research, applied research and privately funded research', with specific reference also given to 'studies conducted in the public interest in the area of public health'.

To situate the competing tensions at the core of the GDPR in the context of research data, Article 7 refers to the conditions for lawful processing. Much has been made of the changes introduced by the GDPR and the potential regulatory burden imposed by the requirement of consent, in particular the introduction of the provision expanding on the conditions for consent in Article 7 of the Regulation. Recital 33 of the GDPR clarifies that for research subjects, broad consent rather than particular consent at data collection will suffice 'when in keeping with recognized ethical standards for scientific research'. However, in the context of publicly available data sets, consent will often not be practically attainable given the high threshold for consent provided for in the Regulation. But consent is only one of the conditions for lawful processing and for instance, here reference can be made to the legitimate interest condition provided for in Article 6(1)(f). In addition, we can also refer to the purpose limitation principle provided for in Article 5(1)(b) which states that the re-purposing of personal data for scientific purposes is compatible with the original purposes for which the personal data was gathered. Although there is a prohibition on the processing of sensitive personal data, such as data concerning health in Article 9(1), Article 9(2)(j) states that processing that is necessary for, inter alia, scientific research purposes is permissible provided it is based on Union or Member State law and is in compliance with Article 89(1). This provision aims to ensure that technical and organizational measures are taken to ensure the protection of the rights and freedoms of data subjects. Article 89(2) further states that Member State or Union law may provide derogations from key data subject rights, namely; access, rectification, restriction and the right to object.[20]

Given the above, although much is made of the role of consent in the GDPR, the legitimacy of personal data processing for research purposes is something that depends on the competing rights and interests at stake, reflecting the tension at the very core of this article. The Regulation requires a context-dependent application of its protections but also, where sensitive personal data are processed, the existence of Member State or Union law is of paramount importance. For better or worse therefore, the GDPR has certainly complicated data use for (and indeed, sharing amongst) researchers and left considerable room for variation in implementation potentially running counter the framework's core aim.[21] There is therefore, an apparent tension inherent to this complex patchwork that is arguably at the root of the recent moves towards legislative reform at the EU level. Thus, the proposed Regulation on European data governance, known as the EU DGA, aims to better facilitate the sharing of data across the Union by establishing; (1) conditions for the re-use of data held by public sector bodies, (2) 'a notification and supervisory framework' for those providing so-called 'data sharing services' (including for anonymized personal data, avoiding the distinction between personal and 'deidentified' data that we see in conventional data protection regimes, the GDPR included), and (3) 'a framework for voluntary registration of entities which collect and process data made available for altruistic purposes'.[22] At the root of this framework is the European Commission's desire to foster the development of the data-driven economy with inspiration taken directly from the FAIR data principles.[23] Although it is made clear that educational institutions do not come within the meaning of public sector bodies,[24] they may be one of the key beneficiaries of data sharing infrastructures and for instance, the providers of data sharing services and the data altruism organizations, which the proposal aims to regulate.

uary 2020) 18 <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf> accessed 7 May 2021.

[18] See Gloria González Fuster and Serge Gutwirth, 'Opening up Personal Data Protection: A Conceptual Controversy' (2013) 29 Computer Law & Security Review 531, Lorenzo Dalla Corte, 'A Right to a Rule: On the Essence and Rationale of the Fundamental Right to Personal Data Protection' in Rosamunde van Brakel and others (eds), *Data Protection and Democracy* (2020) 12. Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer, 2016) 55–61.

[19] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer Science 2009);

[20] It should be noted that this list does not include the GDPR's important right not to be subject to a decision based solely on automated processing including profiling) contained in Article 22.

[21] For a discussion see: Mahsa Shabani, 'The Data Governance Act and the EU's Move towards Facilitating Data Sharing' (2021) 17 *Molecular Systems Biology* 1-3.

[22] See: Article 1(1).

[23] See, the explanatory memorandum to the proposed Regulation. These principles stipulate that data should, in principle, be findable, accessible, interoperable and re-usable.

[24] See Article 3(2).

In this respect the European regulatory approach goes well beyond that of the US and countries such as Australia where legal restrictions on academic research on public data are minimal or at least unclear. The federal Privacy Act 1988 (Cth) is Australia's principal data protection regime, and with its thirteen Australian Privacy Principles (APPs) it's designed loosely to meet EU pre-GDPR data protection standards.[25] However, the Act in s 95A makes an exception for public interest medical research falling within its parameters, subject to the application of "guidelines that relate to the use and disclosure of health information" as approved by the Privacy Commissioner.[26] Further, when it comes to local State and Territory privacy and data protection regimes, which in practice govern most academic research in Australia (with a partial exception for federally-funded research which may also be subject to the federal regime under the terms of funding),[27] broad exceptions for uses of public data are quite often available,[28] in addition to more tailored exceptions for research 'in the public interest'.[29] Further, under proposals to foster access to government data for research and other public purposes under strict requirements designed to safeguard data subjects,[30] it appears that public – i.e. fully released – 'open' data are also treated as exempt from the requirements.[31] Thus, data governance of academic CSR public data is to quite a large extent, non-existent from the perspective of formal law – although university research ethics standards may still be applied.

As to the latter, the National Health and Medical Research Council (NHMRC) *National Statement on Ethical Conduct in Human Research (2007, updated 2018)* (National Statement),[32] the guidelines approved by the Privacy Commissioner under s 95A of the Privacy Act, are the standards applicable to academic research involving research on humans in Australian Universities. Framed in terms of respect for human beings as 'a recognition of their intrinsic value', the National Statement specifies that human research should (1) be guided by 'the values of research merit and integrity, justice and beneficence', (2) have regard for 'the welfare, beliefs, perceptions, customs and cultural heritage, both individual and collective, of those involved in the research, and (3) give due scope, throughout the research process, to the capacity of human beings to make their own decisions, and 'where participants are unable to make their own decisions or have diminished capacity to do so, respect for them involves empowering them where possible and providing for their protection as necessary'.[33] In broad terms, it tasks research ethics committees ('reviewing bodies') established within universities and research organizations with responsibility to ensure compliance with the standards, and balance the diverse interests involved (adopting a proportionality analysis). But it also offers certain guiding principles,[34] and adds that '[t]wo themes must always be considered in human research: the risks and benefits of research, and participants' consent'.[35] As to public data, it notes that:

> Data or information available on the internet can range from information that is fully in the public domain (such as books, newspapers and journal articles), to information that is public, but where individuals who have made it public may consider it to be private, to information that is fully private in character. The guiding principle for researchers is that, although data or information may be publicly available, this does not automatically mean that the individuals with whom this data or information is associated have necessarily granted permission for its use in research. Therefore, use of such information will need to be considered in the context of the need for consent or the waiver of the requirement for consent by a reviewing body and the risks associated with the use of this information.[36]

The context in which this statement is made concerns the issue of consent to secondary uses of existing data sets. But the language of data 'fully in the public domain' might also be taken to mean that ethical review is not necessarily required for such data (as opposed to data that is merely 'public, but where individuals who have made it public may consider it to be private', or 'fully private' data). Thus, research involving

[25] See Privacy Act 1988 (Cth) (Privacy Act) – although note that the Act already contains a number of broad exemptions, including for small business, employee records, journalism, and registered political parties and political acts and practices, and in general its requirements are not especially rigorous by international standards: see Graham Greenleaf, Nigel Waters, Katherine Lane, Bruce Arnold and Roger Clarke, 'Bringing Australia's Privacy Act Up to International Standards' (Submission in Response to the Privacy Act Review – Issues Paper, 18 December 2020) <http://dx.doi.org/10.2139/ssrn.3752152> accessed 7 May 2021.

[26] Thus Privacy Act, s 95A(3) states that the Commissioner may approve for the purposes of the Australian Privacy Principles the guidelines issued by the NHMRC or any other prescribed authority, provided it is satisfied that 'the public interest in the use and disclosure of health information … in accordance with the guidelines substantially outweighs the public interest in maintaining the level of privacy protection afforded by the Australian Privacy Principles'. As to the NHMRC standards, see n 32.

[27] See s 95B requiring this for Commonwealth contracts.

[28] See, for instance, Privacy and Data Protection Act 2014 (Vic), s 12; Health Records Act 2001 (Vic), s 15; Privacy and Personal Information Protection Act 1998 (NSW), s 4(3); Information Privacy Act 2009 (Qld), sch 1, cl 7(a).

[29] See, for instance, Privacy and Data Protection Act 2014 (Vic), sch 1 (Information Privacy Principles 2.1(c) and further 10.2 regarding collection); Health Records Act 2001 (Vic), sch 1 (Health Privacy Principles 2.1(c) and 1.1(e)); Privacy and Personal Information Protection Act 1998 (NSW), s 27B; Information Privacy Act 2009 (Qld), sch 3 (Information Privacy Principles 10(1)(f) and 11(1)(f); sch 4 (National Privacy Principles 2(1)(c) and 9(3)(a)).

[30] Data Availability and Transparency Bill 2020 (Cth). See also Australian Government, 'Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper' (September 2020) <www.datacommissioner.gov.au/sites/default/files/2020-09/DAT%20Bill%202020%20exposure%20draft%20Consultation%20Paper%20Final_0.pdf> accessed 7 May 2021.

[31] ibid [1.2] ('open data cannot be retracted or protected against future uses and misuses').

[32] National Health and Medical Research Council, National Statement on Ethical Conduct in Human Research (2007) (updated 2018) (National Statement) <www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018> accessed 7 May 2021.

[33] ibid [1.10]-[1.13].

[34] ibid Section 1 (introduction).

[35] ibid Section 2 (prefatory statement).

[36] ibid Section 3 (secondary use of data or information).

fully public data might generally be considered an instance of 'negligible risk research' entailing 'no foreseeable risk of harm or discomfort', with 'any foreseeable risk … no more than inconvenience', which under the terms of the National Statement could be treated by institutions as exempt from the need for ethical review, if it involved 'the use of existing collections of data or records that contain only non-identifiable data'.[37]

3. Framing an illustrative case study

The following illustrative case study posits a research project conducted at an Australian university. (The case study is based on a real-life research project but with identifying features redacted.) Its motivation was to start a conversation about gender diversity issues within CSR communities, using CSR as subject-matter and tool. The project used public data from the Microsoft Academic scholarly paper citation repository[38] to analyze the ratio of gender by author names in different areas of expertise under the broad banner of CSR, drawing on author data from over 150,000 scholarly paper records in several areas of expertise (AoEs) – AI, ML, Human-Computer Interaction (HCI) and Natural Language Processing (NLP), among others – in this dataset. From a set of 150,000 records of published papers, all author first names were extracted. The first algorithm reviewed the extracted names against open-source statistical probabilities of gender (male, female, gender neutral or unknown). The fact that the first algorithm is open source means it can be audited and amended by the general public, including groups potentially affected by such an algorithm – as long as they have the technical skills to do so. A second cloud-based algorithm sorted the names to result in the final aggregation of names, male, female and unknown.[39] At this stage, the names unable to be categorized by the first algorithm, would most probably be non-anglophone names. Advocacy bodies and other scholars of related work were consulted on best practices on presenting research on gender. As the data set involved apparently anodyne public data, and the project's research findings did not identify any individuals, the view was taken at the relevant department of the University, that ethics clearance was not required for the research project. (Note that we are not commenting here on the appropriateness of this interpretation of the NHMRC's guidelines.)

The project's research findings were reported at a leading international conference on ethical standards in socio-technical systems. As set out in Table 1, its principal findings were that non-'male' names were consistently underrepresented in every surveyed subfield.

The paper underwent a rigorous review process before being accepted for presentation at the ethics standards conference as a study on the lack of representation of minority groups, using gender classification (male/female and androgynous), in publication. Nevertheless, significant questions were raised at the conference about whether the research represented a study of 'aggregation by algorithm'. The primary point of contention was whether the use of algorithms *per se* silences the voice of minoritized groups, with concerns voiced about the use of algorithms to classify gender (with 'gender neutral' and AI-undetectable names included for comparison). Some of those in the discussion argued that the existing categories insufficiently took account of the full range of genders in the LGBTQIA+ spectrum – with some of those discussants suggesting that unless and until the research could be redesigned, for instance to hand-label individuals' genders based on their self-identification using personal social media accounts/webpages or other sources (adopting a technique that could itself be problematic from a data protection perspective, even apart from the feasibility problem of limited scalability of hand-labeling methods), the project was unacceptable. It was suggested, for example, that a number of academics would object to the use of their authorship records in the project. Furthermore, some individuals raised the prospect of something akin to 'representational harm',[40] insofar as it was seen to perpetuate a false idea that gender is binary, despite multiple and comprehensive disclaimers to the contrary in the paper and in the presentation. For these discussants, the kind of false 'representation' at play in effect was the *absence* of representing gender diverse people who have been and often remain socially invisible.

This illustrative case study points to the sometimes unexpected and fraught ways in which ethical claims may be raised and debated alongside public interest arguments about the value of the research. Although research of this kind may be undertaken with good intent, such as to ameliorate gender discrimination, that does not settle questions about ethical justifiability. For instance, should it be a matter of ethical concern that research projects may be developed and deployed for policy purposes that some of the research subjects themselves might object to, including on their own ethical grounds? In particular, should it matter that some of those whose research is recorded in the project might object to the way the project identifies the genders of the minoritized individuals and groups it profiles? If so, how much credence should be given to those objections in the research scope and design, as well as in any reporting on the research? What are we to make of the idea that publishing data about female inequality could create harms for gender diverse people? And what weight should be given to the benefits of the research despite these contestations and protestations?[41] Where and by whom

[37] See ibid [2.17] and further [5.1.22]-[5.1.23].

[38] See Arnab Sinha, Zhihong Shen, Yang Song, Hao Ma, Darrin Eide, Bo-June Hsu et al., 'An Overview of Microsoft Academic Service (MAS) and Applications' (Proceedings of the 24th International Conference on World Wide Web, Association for Computing Machinery, 2015) 243-246 <https://dl.acm.org/doi/10.1145/2740908.2742839> accessed 7 May 2021.

[39] See Lucía Santamaría and Helena Mihaljević, 'Comparison and benchmark of name-to-gender inference services' (2018) PeerJ Computer Science 4:e156 <https://doi.org/10.7717/peerj-cs.156> accessed 7 May 2021.

[40] See Mohsen Abbasi, Sorelle A Friedler, Carlos Scheidegger and Suresh Venkatasubramanian, 'Fairness in representation: quantifying stereotyping as a representational harm' 2019 arXiv <https://arxiv.org/abs/1901.09565> accessed 7 May 2021.

[41] See Carolina Pía García Johnson and Kathleen Otto, 'Better Together: A Model for Women and LGBTQ Equality in the Workplace' 2019 Frontiers in Psychology <https://doi.org/10.3389/fpsyg.2019.00272> accessed 7 May 2021.

Table 1 – Summarized statistics – accurate to two decimal places – averaged by classification of AoEs diversity (1: low gender diversity versus 2: slightly improved diversity). Bracketed numbers in *italics* illustrate a direct comparison between 'male' and 'female' names.

CSR AoEs, categorized based on gender diversity summary statistics	Average% 'male' names in category	Average% 'female' names in category	Average% 'gender neutral' names in category	Average% names with genders not readily-inferred by AI algorithms
Category 1 AoEs: Low Gender Diversity	74.38 (*84.89*)	13.23 (*15.11*)	8.34	4.04
Category 2 AoEs: Slightly Improved Diversity	69.09 (*76.48*)	21.24 (*23.53*)	6.33	3.34

should these decisions be made? And how can they be made consistently and fairly, taking into account the interests of all relevant stakeholders?

As the above case study illustrates, determinations about how ethical standards should be construed and applied to research involving public data may not be clear-cut. Thus, establishing clear policy and procedures is crucial, in order to mediate between competing claims and interests of all stakeholders – and ideally before the research is undertaken and the results are publicly revealed.

4. Towards a critical data governance perspective

The field of critical data studies (CDS) emerged in the 2010s as a formal attempt to develop a body of research that adopts a critical perspective on CSR.[42] As Metcalf and Crawford note in an early article, a substantial challenge for CDS from its inception was the discontinuity between the research practices of CSR and traditional research ethics governance systems.[43] Specifically:

> Critical data studies is in its infancy, but it faces a substantial challenge: as the practice of data science surges ahead, we lack a strong and rigorous sense of ethical parameters for scientific research. There are several problems emerging. First, there is a growing divide between established systems of research ethics in more traditional disciplines and the dynamic norms and research methods of Big Data … Second, US research regulations … exempt projects that make use of already existing, publicly available datasets on the assumption that they pose only minimal risks to the human subjects they document. But this assumption is founded on a misconception. Publicly available data can be put to a wide range of secondary uses, including being combined with other data sets, that can pose serious risks to individuals and communities. This is one of several risks that are being overlooked in the current debates about the ethics of Big Data studies.[44]

As Metcalf and Crawford point out, a critical data governance perspective can stretch our concepts of what constitutes ethical research in significant ways, 'mov[ing] ethical inquiry away from traditional harms such as physical pain or a shortened lifespan to less tangible concepts such as information privacy impact and data discrimination. It may involve the traditional concept of a human subject as an individual, or it may affect a much wider distributed grouping or classification of people'.[45] At the same time, the perspective can stretch our ideas of what constitutes 'governance' to accommodate the multiple ways in which ethical ideas of 'good' conduct may effectively influence legal standards concerning, inter alia privacy, data protection and discrimination (including instances where discourses of human rights are employed to frame legal standards, treating 'human rights' as a particularly complicated enmeshing of legal and ethical standards).[46] For it is often only at the latter stage that researchers and other relevant stakeholders may feel compelled to 'weigh the scientific and societal interests of their research against the interests of any third parties whose rights may be infringed'.[47] Further, given that, as van Dijk says 'people have faith in the institutions that handle their (meta)data on the presumption that they comply with the rules set by publicly accountable agents',[48] there is value in maintaining trustworthy systems for monitoring information flows in academia as in business and government.

Applying these principles to the treatment of CSR involving public data, to repeat the language of Metcalf and Crawford, there is a need for effective data governance as even '[*p*]ublicly available data can be put to a wide range of secondary uses, including being combined with other data sets, that can pose serious risks to individuals and communities'.[49] Moreover, effective data governance can be understood broadly to encompass not only the standards that may be prescribed and enforced through the 'hard law' of legislation, administrative and judicial decisions, but also the 'soft law' standards that may be promulgated and applied within research communities bolstered by institutional apparatus to compel compliance. Thus,

[42] See Andrew Iliadis and Federica Russo, 'Critical Data Studies: An Introduction' (2016) 3(2) Big Data & Society 1-7.

[43] Jacob Metcalf and Kate Crawford, 'Where are Human Subjects in Big Data Research? The Emerging Ethics Divide' (2016) 3(1) Big Data & Society 1-16.

[44] ibid 1.

[45] ibid 2.

[46] See Lawrence O Gostin, 'Public Health, Ethics, and Human Rights: A Tribute to the Late Jonathan Mann' (2001) 29 Journal of Law, Medicine & Ethics 121.

[47] 'Ethical and Legal Aspects of Infomatics Research – Advisory Report' (Royal Netherlands Academy of Arts and Sciences, 2016) 8 <www.sapea.info/wp-content/uploads/Ethical-and-legal-aspects-of-informatics-research.pdf> accessed 7 May 2021.

[48] José van Dijck, 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology' (2014) 12 Surveillance and Society 197, 198.

[49] Metcalf and Crawford (n 43) 1.

as boyd and Crawford argue in another early article,[50] soft law research ethics standards, along with their institutional apparatus, 'provide a framework for evaluating the ethics of a particular line of research inquiry and to make certain that checks and balances are put into place to protect subjects', with practices like 'informed consent' and privacy and data protections for research subjects 'intended to empower participants in light of earlier abuses in the medical and social sciences' – adding that although research ethics boards 'cannot always predict the harm of a particular study – and, all too often, prevent researchers from doing research on grounds other than ethics – their value is in prompting researchers to think critically about the ethics of their project': and '[t]he process of evaluating the research ethics cannot be ignored simply because the data are seemingly public'.[51]

Our approach is similar to that of boyd and Crawford (and Metcalf and Crawford) in that our critical data governance perspective is focused on the ways in which not just formal legal standards but the soft law of research ethics standards is, and ideally should be adapted and applied to researching public data in academic CSR scenarios, such as the research project described in the previous section of this article. We are also interested in the fact that governance standards applicable to academic research projects involving public data are currently variable across different jurisdictions – ranging from a US-style system of self-regulation which largely leaves it to researchers and their institutions to decide whether or not to comply with self-prescribed ethical standards in their research, to quite stringent EU-style formal legal regulation, to industry-level regulation as the option currently preferred in Australia but without being necessarily rigorously applied. In the discussion that follows, we analyze costs and benefits of these models, and recommend a multifaceted approach which draws on the strengths of each of the individual approaches.

4.1. *Self-regulation*

In stating that researchers need 'to think critically about the ethics of their project' (that is, '[t]he process of evaluating the research ethics cannot be ignored simply because the data are seemingly public'), boyd and Crawford suggest that self-regulation is a viable technique in the absence of other (more intrusive) forms of 'regulation'. Indeed, their comment that research ethics boards 'cannot always predict the harm of a particular study – and, all too often, prevent researchers from doing research on grounds other than ethics' might be taken to imply that self-regulation may actually be more desirable in this context than regulation by research ethics boards. Appointments of high-quality inhouse ethicists such as boyd and Crawford (both principal researchers at Microsoft Research), and Timnit Gebru and Margaret Mitchell (until recently co-leaders of the AI ethics group at Google) have lent a welcome air of ethics being taken seriously as a dimension of business CSR that we might hope to see emulated within government and academic circles. Unfortunately, the recent firings of Gebru[52] and Mitchell[53] from Google – after they collaborated with academic researchers on a paper discussing ethical issues raised by recent advances in developing powerful AI language models,[54] including their environmental costs and their replication of biased language on gender and race found online, with Gebru also noting Google's resistance to arguments for more diversity in the Research group[55] – shows just how fragile their status and influence can be against other research objectives.

Of course, we hope that universities and their affiliated researchers will be able to be more resilient in the face of such pressures. Even so, relying on individual computer science researchers and their institutions to self-police ethical standards for their research is a risky affair.[56] Thus, while we consider that encouraging and empowering researchers to think critically about the ethics of their projects is an excellent move in personal and professional terms, we argue that is not sufficient in this context.

4.2. *Formal legal regulation*

On the other hand, also problematic is the EU's highly regulatory approach of adhering to the principle that scientific research involving personal data must follow the general standards laid out in the GDPR. As described above, as a gesture towards accommodating scientific research that might otherwise be unreasonably constrained by the GDPR's rigor, Article 89 establishes a two-level framework to enable derogations where scientific research is concerned – providing that, first, the derogations be subject to safeguards and, second, the research complies with standards imposed through Union or Member State law.[57] Nevertheless, on the whole, the GDPR continues to place significant - if still rather uncertain - restraints on research with 'little insight or guidance contained within the GDPR as to the appropriate safeguards [for ethical research] that must be in place'.[58] Much uncertainty remains about how the Regulation will be construed and applied with

[50] danah boyd and Kate Crawford, 'Critical Questions For Big Data' (2012) 15 Information, Communication & Society 662.
[51] ibid 672.
[52] Tom Simonite, 'A prominent AI ethics researcher says Google fired her' (Wired, 12 March 2020) <www.wired.com/story/prominent-ai-ethics-researcher-says-google-fired-her> accessed 7 May 2021.
[53] Charlie Osborne, 'Google fires top ethical AI expert Margaret Mitchell' (ZDNet, 22 February 2021) <www.zdnet.com/article/google-fires-top-ethical-ai-expert-margaret-mitchell> accessed 7 May 2021.
[54] Emily M Bender, Timnit Gebru, Angelina McMillan-Major and Margaret Mitchell, 'On the dangers of stochastic parrots: Can language models be too big?' (ACM FAccT Conference 2021, 3-10 March 2021, Virtual Event, Canada) <https://faculty.washington.edu/ebender/papers/Stochastic_Parrots.pdf> accessed 7 May 2021.
[55] Simonite (n 52).
[56] See for instance the heated academic debate reported on GeekWire about the relevance of ethics to AI research: Taylor Soper, 'Retired UW computer science professor embroiled in Twitter spat over AI ethics and "cancel culture"' (GeekWire, 16 December 2020) <www.geekwire.com/2020/retired-uw-computer-science-professor-embroiled-twitter-spat-ai-ethics-cancel-culture>.
[57] See Article 89 (n 20).
[58] Ciara Staunton, Santa Slokenberga and Deborah Mascalzoni, 'The GDPR and the Research Exemption: Considerations on the

this framework resting on the uncertain boundary to the right to data protection spelt out in Article 8 of the EU Charter.

Notwithstanding the obvious challenges in appropriately weighing seemingly diverging policy aims, the objective of facilitating access to data (even sensitive personal data) in the public interest, such as for academic research purposes, seems well-intentioned. Likewise, the proposed introduction of the concept of 'data altruism' or the facilitation of the voluntary sharing of data for the 'common good' in the proposed DGA seemingly aims to allow for the better sharing of data in the public interest. Data altruism is defined in Article 2(1) of the proposed DGA 'as the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services.'[59] At the same time, however, this proposal seemingly relies on the capacity to provide a 'secure processing environment' to allow access to sensitive datasets held by the public sector for scientific research or other beneficial purposes. Further, the distinction between academic research and commercial research is not always clear-cut in the proposed DGA, and the potential for misapplication or commercial uses is always possible or adjacent to academic work. Irrespective of the intense compatibility/consistency debates that will inevitably occur in the balancing of the policy interests behind the GDPR and the proposed DGA, the proposal is an excellent demonstration of the range of ethical and methodological concerns that relate to the use of public data in research and, further, the ways in which data sharing in the public interest such as for research purposes can be legitimized.

Finally, we note that increasing attention is being paid to the role of research ethics committees as part of the EU regulatory matrix. In a recent Preliminary Opinion on Data Protection and Scientific Research, the European Data Protection Supervisor (EDPS) stated that the flexibility afforded to Member States, while not yet 'precisely delineated', 'cannot be applied in such a way that the essence of the right to data protection is emptied out, and this includes data subject rights, appropriate organizational and technical measures against accidental or unlawful destruction, loss or alteration, and the supervision of an independent authority'.[60] Likewise, '[*a*]ny limitations to fundamental rights in law are to be interpreted restrictively and cannot be abused'.[61] At the same time, the EDPS clarified what it saw as the essential role of research ethics committees or Institutional Review Boards in supporting ethical research. The EDPS pointed out that national research ethics committees, as established by universities and other institutions for instance, have established codes of practice and examined the rights of the research subjects and wider societal implications in thorough reviews of individual research project applications, adding that '[t]hese standards are even more essential now that vast quantities of data are available. There is growing awareness that what has become possible through digital technology is not necessarily sustainable or justifiable'.[62] While a useful step, much needs to be worked out about how research ethics committees can usefully contribute to regulation in this space rather than simply adding another layer to a highly regulatory EU approach.

4.3. *Industry regulation ('soft law')*

That governance of academic CSR research in Australia operates largely on a soft law basis with universities following the standards prescribed in the NHMRC, adopting what we have termed an 'industry-regulation model', is a testament to the influence of Australian social researcher John Braithwaite's work on responsive regulation.[63] As well as framing a tiered approach to regulation, so that it is only when the lower-level regulation is judged as one that 'fails to solve specific problems sufficiently, [that] the regulator … starts to move up a pyramid',[64] Braithwaite shows a distinct preference for regulatory options that sit between self-regulation and full (formal) legal regulation on social, political and economic grounds, explaining that '[r]esponsive regulation is about "tripartism" in regulation. It highlights the limits of regulation as a transaction between the state and business. It argues that unless there is some third party (or a number of them) in the regulatory game, regulation will be captured and corrupted by money power'.[65] As such, Braithwaite offers a mediatory approach that seems well-adapted to academic research ethics processes, involving as they do close-knit actors operating on common norms and a mechanism of public sanctions for non-compliance.[66] In other words, it is an approach that should work relatively effectively in Australian academic research circles but may be less effective in wider business and government circles.

However, this does not mean that the existing academic research ethics processes cannot be improved. As Braithwaite says, a 'storytelling orientation' can assist in thinking about how effective a mode of regulation is and how it could be improved.[67] Stories such as the illustrative case study discussed

Necessary Safeguards for Research Biobanks' (2019) 27 European Journal of Human Genetics 1159.

[59] In order to facilitate this consent, Article 22 of the proposed Regulation allows the Commission to adopt implementing acts to develop consent forms. However, despite the clear aim of this proposal to facilitate the sharing and use of data, there appear to be obvious questions regarding its overlaps with the GDPR in particular in relation to the respective roles of consent and the role of legitimate/public interest-based means of legitimizing (sensitive) personal data processing.

[60] European Data Protection Supervisor, 'A preliminary opinion on data protection and scientific research' (6 January 2020) 18 <https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf> accessed 7 May 2021.

[61] ibid 18.

[62] ibid 13-14.

[63] See especially Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992).

[64] John Braithwaite, 'The Essence of Responsive Regulation' (2011) 44 University of British Colombia Law Review 475, 481.

[65] John Braithwaite, 'Responsive regulation' via <http://regnet.anu.edu.au/our-people/academic/john-braithwaite>.

[66] Cf Graham Greenleaf, 'Responsive Regulation of Data Privacy: Theory and Asian Examples' in David Wright and Paul de Hert (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer 2016) 240-241.

[67] ibid 240.

in this article suggest that Australian ethical research standards for academic research need to be reassessed in light of experience of the risks and harms associated with the use of public data, including subjective 'harms' that research subjects may experience – for instance, in terms of their ethical positions on the research project or its processes – versus the public benefit of the research. These are difficult ethical questions that we contend are best handled with the benefit of the collective expertise of university research ethics committees rather than being left to be dealt with by individual researchers. This points to the need for a more rigorous and uniform approach to the NHMRC ethical standards. At the same time, formal legal standards need to be strengthened so they can reinforce and where necessary supplement the soft-law standards – in particular, removing the broad public data exemptions in Australian state and territory regimes and adopting a uniform approach to the research exemptions for public interest research in these regimes and in the federal Act. Ideally, the latter exemptions, like the current s 95A of the federal Act, should explicitly authorize the NHMRC ethical standards as the appropriate standard for public interest research involving humans. Finally, the experience of the GDPR and the proposed DGA, once the latter is enacted and comes into effect, may provide useful general guidance in further refining those exceptions down the track

5. Conclusion and recommendations

Our starting point in this article was the insight that attempts to measure diversity using public data may themselves raise legal and ethical questions about the research methods adopted and their treatment of diversity. To this extent, we posed the following research question: *How can the exposure or appropriation of personal diversity data in the processing of public data be managed?* Our next step was to frame an illustrative case study centered on an academic CSR project at an Australian university that used public academic citation data to measure diversity in academic CSR communities, and was considered sufficiently low risk not to be submitted to the university's ethics review process but was subsequently criticized at an international ethics conference for its algorithmic approach of obtaining approximate gender statistics from author lists on academic citations (which was seen as failing to offer a sufficiently granulated approach to measuring diversity). This led us to conclude that a critical data perspective should be focused on the ways in which not just formal legal standards, but the 'soft law' of university research ethics standards are and ideally ought to be adapted and applied to researching public data in academic research scenarios. Thus, we support a mixture of formal legal regulation and soft law research ethics standards, ideally working in harmony to foster expert, flexible and adaptive approaches. Indeed, we argue that this is becoming essential, given the proliferating use of AI and ML and other techniques of data analysis in CSR, the potential speed and scale of the impact of such research, and the risks and harms to individuals and communities as identified in this article.

The above arguments are not intended to derogate from the value of self-help measures adopted by CSR researchers and their own communities. Our illustrative case study makes clear that it would be preferable to have issues picked up at an early stage, even before research projects are submitted for ethics assessment and ideally at their design stage. For instance, CSR departments within universities could establish their own data stewards with legal and computer science domain expertise to assess big data analytics projects from inception to design with a view to ensuring that ethical requirements for using public data are met. Moreover, as boyd and Crawford argue, CSR researchers themselves could be usefully engaged in thinking critically about the ethics of their big data projects.[68] Indeed, they could go a significant distance in focusing their attention and expertise in framing their research projects to address real-world situations and in finding solutions to potential issues concerning their research methods and subject-matter that will meet the ethical standards of research subjects and the broader community.[69] It is only when a holistic approach is adopted to data governance, with standards not only explicated, promulgated and enforced at the institutional level but internalized by the researchers responsible for framing and carrying out the research, that we can reasonably expect research subjects to have trust in the institutions that handle their data. Hopefully our recommendations for a combination of formal legal regulation and soft-law research ethics standards will go some way to inculcating the necessary 'ethics sensibilities'.

Declaration of Competing Interest

Rachelle Bosua, on behalf of all the authors of the manuscript titled: Using Public Data to Measure Diversity in Computer Science Research Communities – A Critical Data Governance Perspective declares that there is no conflict of interest associated with the manuscript; i.e., there was no funding received or financial gains in conducting the work, and all researchers involved in this research share similar and complementary research expertise and interests on the topic of data privacy.

[68] boyd and Crawford (n 50) 672.

[69] Cf Ben Wagner, 'Accountability by Design in Technology Research' (2020) 37 Computer Law & Security Review (Special Issue on Legal and Ethical Challenges of Data Processing in the Research Field) 105398.