2 October 2018

Australian Human Rights Commission
Level 3, 175 Pitt Street
SYDNEY NSW 2000
GPO Box 5218SYDNEY NSW 2001

Submission re Human Rights and Technology Project

Given my specific areas of expertise, my submission is confined to those aspects of technology that involve the use of information about individuals and groups of individuals to inform decision making that impact on individuals and on the issues raised in Parts 3-5 of the Issue Paper.

What types of technology raise particular human rights concerns? Which human rights are particularly implicated?

Technologies which facilitate the surveillance activities that collect the personal information used to inform decisions and actions affecting individual include:

- Technologies based on GPS (eg as manifest in mobile devices and the applications used on them) – these make it increasingly difficult to move through public spaces without being surveilled – movement data can in some respects be more invasive than communication content data (by revealing who one associates with, patterns of activities etc[1]);
- Technologies based on face recognition – these makes it increasingly difficult to remain anonymous when out in public;[2]
- The Internet of Things – this now generates a vast pool of new information about individuals including health related information (eg via fitbit-type devices), information about personal habits (eg via smart home meters);[3]
- Technologies involving AI, machine learning and algorithms to make decisions or inform decisions that affect individuals (as discussed below);

[1] 'Repeated visits to a church, a gym, a bar or a bookie tell a story not told by any single visit, as does one's not visiting any of those places in the course of a month': *United States v Maynard* 615 F 3d 544, 562 (DC Cir 2012) per Ginsburg J.

[2] Christopher Kuner, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson, 'Face-to-data—another developing privacy threat?' (2013) 13 *International Data Privacy Law* 1.

[3] 'Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics and the Quantified Self 2.0' (2012) 1 *Journal of Sensor and Actuarial Networks* 217 ; Joseph Savirimuthu, 'Smart meters and the information panopticon: beyond the rhetoric of compliance' (2013) 27 *International Review of Law, Computers & Technology* 161; Jacob Morgan, 'A Simple Explanation of "The Internet Of Things"', *Forbes* (online), 13 May 2014 <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyonecan-understand/#2ae232d01d09>.

- Technologies that make use of Big Data to inform activities such as the micro targeting of consumers[4] and electors,[5] which have the potential to be used for manipulation;
- Technologies which facilitate social media scraping, which forms one of the key sources of the personal data in the datasets that inform Big Data Analytics;[6]
- The applications used on mobile and other computer devices – these likewise make up a large portion of the personal data available;[7] and
- New electronic health technologies – these are high risk due to the value of health information, including to those with criminal intent.[8]

A key human right that is implicated is the right to privacy, a right which is broadly defined in international human rights instruments and jurisprudence.[9] However, individuals' loss of control over their personal data also has adverse consequences for other human rights including:

- The right to equality and non-discrimination (for example, where there is discrimination or other forms of bias in algorithmic decision-making)[10]
- Freedom of expression (while freedom of expression can conflict with privacy in some circumstance, it is also important to bear in mind that surveillance – particularly surveillance by governments and others in position of power – produces a freezing effect that impacts adversely on freedom of expression and, in some cases, freedom of association[11]
- Right to a fair trial and fair criminal process (which may occur with the use of AI to inform decision making in the criminal justice context).[12]

These new technologies also have implications for doctrines and concepts that underpin the human rights framework, including the rule of law (as occurs where technology-based decision making is

---

[4] See Sophie C Boerman, Sanne Kruikemeier and Frederik J Zuiderveen Borgesius, 'Online Behavioral Advertising: A Literature Review and Research Agenda' (2017) 46(3) *Journal of Advertising* 363.

[5] See, eg, Frederik J. Zuiderveen Borgesius, Judith Möller, Sanne Kruikemeier, Ronan Ó Fathaigh, Kristina Irion, Tom Dobber, Balazs Bodo, and Claes de Vreese, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) *Utrecht Law Review 8.*

[6] Leah Betancourt, *How Companies Are Using Your Social Media Data* (2 March 2010) *Mashable* <http://mashable.com/2010/03/02/data-mining-social-media/#7XUnW8SqWEqo>.

[7] Enisa, *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR*, November 2017.

8 See Christopher Markou, Why using AI to sentence criminals is a dangerous idea, The Conversation, 16 May 2017,

<>https://theconversation.com/why-using-ai-to-sentence-criminals-is-a-dangerous-idea-77734; Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks' *ProPublica*, 23 May 2016.

[9] See, eg, Bart van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data' (February 27, 2015). Utrecht Journal of International and European Law, Vol. 31, No. 80, pp.25-50, February 2015. Available at SSRN: https://ssrn.com/abstract=2629118

[10] See, eg, European Union Agency for Fundamental Rights, *Big Data: Discrimination in data-supported decision making*, May 2018 <http://fra.europa.eu/en/publication/2018/big-data-discrimination>.

[11] See Privacy International and Article 19, Privacy and Freedom of Expression In the Age of Artificial Intelligence (April 2018) <https://www.article19.org/wp-content/uploads/2018/04/Privacy-and-Freedom-of-Expression-In-the-Age-of-Artificial-Intelligence-1.pdf>.

[12] See Betsy Anne Williams, Catherine F. Brooks and Yotam Shmargad, 'How Algorithms Discriminate Based on Data they Lack: Challenges, Solutions, and Policy Implications' (2018) 8 *Journal of Information Policy*. 78-115.

lacking in due process) and the concepts of autonomy and dignity which underlie the international human rights framework. For example, autonomy is implicated when personal information is collected and used without the data subject's meaningful consent and dignity is implicated when individuals are reduced to sets of quantifiable attributes and manipulated on the basis of knowledge of their personal vulnerabilities.

Noting that particular groups within the Australian community can experience new technology differently, what are the key issues regarding new technologies for these groups of people (such as children and young people; older people; women and girls; LGBTI people; people of culturally and linguistically diverse backgrounds; Aboriginal and Torres Strait Islander people?

- There is growing evidence that AI based decision-making can be biased against disadvantaged groups, including groups that do not currently receive protection under anti-discrimination laws (for example people of lower socio-economic status and those from disadvantaged backgrounds[13])
- Certain groups (for example, domestic violence victims) are especially vulnerable where data collected for other purposes falls into the hands of those who seek to harm them. [14]
- Aboriginal and Torres Strait Islander people have particular concerns about the collection and processing of their personal information.[15]

How should Australian law protect human rights in the development, use and application of new technologies? In particular:

(a) What gaps, if any, are there in this area of Australian law?

The fact that Australia lacks a constitutional Bill of Rights or even a federal Human Rights Act or Charter makes it difficult to develop regulatory frameworks which provide for a nuanced consideration of human rights issues in the interpretation of legislation and the development to the common law. The way in which the Human Rights Act 1998 (UK) has facilitated the development of a new privacy tort in the UK[16] illustrates that even a law which lacks constitutional underpinning can be very helpful in this respect. This is also illustrated in several of the provisions in the EU Data

---

[13] Nathan Newman, 'How Big Data Enables Economic Harm to Consumers, Especially to Low -Income and Other Vulnerable Sectors of the Population' (2014) 18(6) *Journal of Internet Law* 11; Mary Madden, Michele E. Gilman, Karen Levy & Alice Marwick,' Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans' (2017). 95 *Washington University Law Review* 53.

14 See, eg, Dana McCauley, 'My Health Record a new battleground in family disputes' The Sydney Morning Herald, 31 July 2018< https://www.smh.com.au/politics/federal/my-health-record-a-new-battleground-in-family-disputes-20180731-p4zunr.html>.

[15] See, for example, the submission by the Australian Indigenous Governance Institute to the Data Availability and Use Productivity Commission Issues Paper (July 2016) at <https://www.pc.gov.au/__data/assets/pdf_file/0014/203234/sub060-data-access.pdf>; Tahu Kukutai and John Taylor (eds), *Indigenous Data Sovereignty: Toward an Agenda* (ANU Press, 2016) <http://press-files.anu.edu.au/downloads/press/n2140/html/cover.xhtml?referer=&page=0#>.

[16] See Lord Robert Walker, 'The English Law of Privacy — an Evolving Human Right' (2011) 1 *Victorian Bar Review* 1. This is based on a paper published at https://www.supremecourt.uk/docs/speech_100825.pdf.

Protection Regulation (GDPR), which impose tests based specifically on impact on individual rights and freedoms.

Issues related to information handling are most logically addressed via data protection laws, but the Privacy Act 1988 (Cth) (Privacy Act) is deficient both because of the large number of bodies and activities are excluded from its operation (for example, small business operators,[17] employers in respect of employment records,[18] political parties and practices etc[19]) and because the principles on which it is based are outdated and sparse as compared with those in the GDPR and the many other countries that are signatories to the Data Protection Convention of the Council of Europe, as discussed below.

Anti-discrimination laws do not address all the forms of discrimination that have been identified in relation to AI-based decisions, as discussed above.

There are insufficient safeguards in relation to government use of AI-based decision-making (eg, as illustrated via the Robodebt incident). As argued by Justice Melissa Perry and Alexander Smith: "Achieving efficiencies should not be allowed to compromise society's commitment to an administrative law system that is fair, transparent and accountable and that operates according to the rule of law. Safeguards need to be in place in order to ensure that the individual's right to hold decision makers to their obligations is preserved'.[20]

(b) What can we learn about the need for regulating new technologies, and the options for doing so, from international human rights law and the experiences of other countries?

There are three international regimes which offer useful insights.

(1) The EU General Data Protection Regulation[21]

The GDPR, which came into operation on 25 May 2018, is specifically designed to improve data subjects' control over their data. While there are many aspects of its protection that are more extensive than that under the Australian Privacy Act, noteworthy features that are important in the light of the issues identified above include:

- High bars for collection, use and disclosure for protection of personal data that falls outside the categories that receive special protection. In particular, while the GDPR allows for data collection and handling without the consent of the data subject based on the interests of the collector, it requires that such legitimate interests are not 'overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child'.[22]
- Requirements for privacy by design coupled with clear guidance in Recital 26 on issues relating to reidentification. The privacy by design requirements mandate the implementation of appropriate technical and organisational measures which are designed to implement data-

[17] Privacy Act, s 6C(1).
[18] Privacy Act, s 7B(3).
[19] Privacy Act, ss 6C(1) and 7C.
[20] See Justice Melissa Perry and Alexander Smith, 'iDecide: the legal implications of automated decision-making' [2014] *Federal Judicial Scholarship* 17.
[21] The key features identified are drawn from a joint article with Maeve McDonagh, 'Data protection in an era of Big Data: The challenges posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* forthcoming.
[22] GDPR, art 6(1)(f).

protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements in the Regulation and protect the rights of data subjects. Furthermore, the specific requirements in each case must be determined having regard to 'the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'.[23]

- Requirements to conduct Data Protection Impact Assessments where 'a type of processing … is likely to result in a high risk to the rights and freedoms of natural persons[24].
- Requirements for privacy by default, mandating implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.[25]
- Specific requirements designed to regulate profiling based on automatic processing – ie:
    - Obligations to inform data subjects inter alia about 'the existence of [any] automated decision making [and] … profiling' and also with a 'meaningful explanation about the logic involved, as well as the envisaged consequences of such processing as well as of the significance and the envisaged consequences of such processing' for them.[26]
    - Rights for data subjects to object to data processing in specified circumstances[27] which must be 'explicitly brought to the attention of the data subject' at the time of the first communication with them;[28] and
    - Rights for data subjects to object at any time to the processing of their data for direct marketing purposes 'which includes profiling to the extent that it is related to such direct marketing'.[29]
- A right of erasure which allows data subjects to require erasure of their personal information in specified circumstances, including where the only justification for collection of processing the data is based on consent and that consent has been withdrawn,[30] or where 'there are no overriding legitimate grounds for the processing, or the data subject objects to the processing' or where 'there are no overriding legitimate grounds for the processing, or the data subject objects to the processing'.[31]

(2) The Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)[32]

Convention 108 is a Council of Europe Treaty open to any country in the world. It has been ratified by 53 countries, including 6 non-members of the Council of Europe. It has recently been modified via a protocol which opened for signature on 25 June 2018.[33] This contain a number of rights and protections similar to those discussed above in relation to the GDPR, including rights for data subjects -

---

[23] GDPR, art 25(1).
[24] GDPR, art 35(1).
[25] GDPR, art 25(2).
[26] GDPR, art 13(2)(f).
[27] GDPR, art 21(1) and (2).
[28] GDPR, art 21(4).
[29] GDPR, article 21(2).
[30] GDPR, art 17(1)(b).
[31] GDPR, art 17(1)(c).
[32] The amending protocol for this Convention can be accessed at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.
[33] The Convention as amended is referred to as Convention 108+.

- not to be subjected to a decision which significantly affects them based solely on an automated processing of data without having their views taken into consideration;[34]
- to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to them the communication in an intelligible form of information needed in order to ensure required transparency of processing;[35]
- to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to them;[36]
- to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override their interests or rights and fundamental freedoms;[37]
- to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of the Convention;[38]

It also contains requirements both privacy by design and privacy by default.

California Consumer Privacy Act (CCPA)[39]

The CCPA, which was enacted in June 2018 and then amended in August 2018, comes into operation on 1 January 2020. Features of the Act which are relevant to the consultation include that it confers on "consumers" (ie natural persons who are residents of California) the following four basic information rights;

1. the right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold;[40]
2. the right to "opt out" of allowing a business to sell their personal information to third parties (or, for consumers who are under 16 years old, the right not to have their personal information sold absent their, or their parents', opt-in);[41]
3. the right to have a business delete their personal information, subject to some exceptions;[42] and
4. the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.[43]

(5) Local Law No. 49/2018 of the New York City Council[44] (NNYC Local Law 49/2018)

---

[34] Convention 108+,art 2(1)(a).
[35] Convention 108+,art 2(1)(b).
[36] Convention 108+,art 2(1)(c).
[37] Convention 108+,art 2(1)(d).
[38] Convention 108+,art 2(1)(e).
[39] AB375, Title 1.81.5 < https://www.isipp.com/resources/full-text-of-the-california-consumer-privacy-act-of-2018-ccpa/>.
[40] CCPA §1798.110 and §1798.115.
[41] CCPA § 1798.125.
[42] CCPA §1798.105.
[43] CCPA §1798.120(a).
[44] <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0>.

This local law, which was passed by the New York City Council in December 2017, establishes a task force to study how New York city agencies use algorithms to make decisions that impact on the public. The role of this taskforce is to report back to the Council and make recommendations concerning

- procedures for enabling affected individuals to request and receive explanations of such decision and the basis on which they are made;[45]
- procedures for determining whether automated decision systems impact disproportionately based on age, race, creed, colour, religion, national origin, gender, disability, marital status, partnership status, caregiver status, sexual orientation, alienage or citizenship status;[46]
- procedures for addressing instances in which a person is harmed by an agency automated decision system if any such system is found to disproportionately impact persons based upon those categories;[47]
- criteria for identifying which agency automated decision systems should be subject to one or more of these procedures;[48]
- development and implementation of a process for making information publicly available to enable the public to meaningfully assess how the systems of each of these agencies functions and is used by the city, including making technical information about such system publicly available where appropriate;[49] and
- the feasibility of the development and implementation of a procedure for archiving agency automated decision systems, data used to determine predictive relationships among data for such systems and input data for such systems.[50]

(6) Insights from Human Rights frameworks

Rights to privacy and data protection by their nature are not absolute rights – they will generally involve some conflict with other competing rights and interests. Human Rights frameworks provide a useful model for dealing with such conflicts via the requirements of legitimate aim, necessity and proportionality.

(c) What principles should guide regulation in this area?

The broad principles that are important include:

- Autonomy/control/informed consent
- Procedural fairness
- Rationality
- Equality/non-discrimination/lack of bias
- Transparency
- Legality

In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?

[45] NYCC Local Law 49/2018, art 3(1)(a).
[46] NYCC Local Law 49/2018, art 3(1)(b).
[47] NYCC Local Law 49/2018, art 3(1)(c).
[48] NYCC Local Law 49/2018, art 3(1)(d).
[49] NYCC Local Law 49/2018, art 3(1)(e).
[50] NYCC Local Law 49/2018, art 3(1)(f).

The ethical frameworks that apply to human research demonstrate that codes of ethics can play a useful role.[51] However, what is significant about them is that they are enforced by universities and publisher of research. Efforts by those with vested interests in maintaining the status quo to push for an ethics-based approach need to be viewed with caution.

It is important that human rights and data protection considerations are taken into account when new technology is designed as it is difficult and expensive to adapt systems once they have been created. That is why requirements of data protection by design and default are both very important.

It is important that IT students (and student cohorts more generally) are educated about these issues as part of their training.

How well are human rights protected and promoted in AI-informed decision making? In particular, what are some practical examples of how AI-informed decision making can protect or threaten human rights?

There are no laws in Australia which impose limitations on use of AI in decision-making except indirectly where:

- an individual has an enforceable right to natural justice and that is not excluded by legislation;
- the organisation is subject to the limitations on data handling in the Privacy Act and related state laws or
- to the extent it gives rise to rights that are protected under existing anti-discrimination legislation.

Depending on the context AI-informed decision making can deprive individuals of procedural rights (eg, where it affects criminal penalties or administrative consequences) and can also subject them to discrimination and bias, including on a group basis (as discussed below).

How should Australian law protect human rights in respect of AI-informed decision making? In particular:

(a) What should be the overarching objectives of regulation in this area?
To protect autonomy and dignity and to prevent unfairness and abuse of power.

(**b) What principles should be applied to achieve these objectives?**
While not necessarily enough in themselves, public law principles – ie, transparency, rationality, procedural fairness/due process and legality – can provide a useful way forward. It is arguable that they are relevant beyond the public sector because their focus is to control the exercise of power over the individual and that is relevant in relation to many aspects of AI decision-making.

(c) Are there any gaps in how Australian law deals with this area? If so, what are they?

These are as discussed above.

[51] These are discussed in Moira Paterson and Normann Witzleb, 'The Privacy-related Challenges Facing Medical Research in an Era of Big Data Analytics: A Critical Analysis of Australian Legal and Regulatory Frameworks' (2018) 26(1) *Journal of Law and Medicine* forthcoming.

(d) What can we learn from how other countries are seeking to protect human rights in this area?

- The value of having some form of constitutional or legislative protection of human rights
- Data protection laws should not be focussed only on privacy
- The potential value of, and intersections with, consumer protection laws in offering (indirect) protection.[52]

In addition to legislation, how should Australia protect human rights in AI-informed decision making? What role, if any, is there for:

(a) An organisation that takes a central role in promoting responsible innovation in AI informed decision making?

(b) Self-regulatory or co-regulatory approaches?

(c) A 'regulation by design' approach?

An ideal model would be to implement a regulatory model that draws on the regime recommended by the 2010 VLRC in its *Surveillance in Public Places* report.[53] This included a new role for an independent regulator, provision for both voluntary best practice standards and mandatory codes, a licensing system for specific types of surveillance, further measures to provide for civil and criminal sanctions and a set of overarching set of principles to inform and guide regulation.

I submit that good privacy regulation requires a mix of the measures in Ayres and Braithwaite's "regulatory pyramid",[54] including soft measures such as education, guidance and persuasion, mild administrative functions and harder more punitive measures such as civil and criminal sanctions. Ideally, such a regime is overseen and enforced by a central regulator.

The model under the Privacy Act 1988 whereby the Commissioner has a range of guidance related, monitoring related and advice related functions,[55] as well as ability to apply for the imposition of civil sanctions[56] provides a good starting point. The Act now contains provision for the imposition of civil sanctions and allows organisation to develop their own codes of principles, subject to approval. However, the scope of the Act would need to be expanded (by removing a range of existing exemptions) and amended to better deal with the issue of AI-informed decision-making drawing of the insights from the international laws described above. In other words, it would need to be expanded so that it protects not just privacy per se but also against the other harms that can result from AI-based decision-making, as has occurred in data protection laws in many other countries.

---

[52] See, eg, Francisco Costa-Cabral and Orla Lynskey, 'Family ties: the intersection between data protection and competition in EU Law' (2017) 54 (1) *Common Market Law Review* 11-50; Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54(5) Common Market Law Review. Available at SSRN: https://ssrn.com/abstract=3048844

[53] <http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report>.

[54] This was developed in Ian Ayers and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992) < http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf>.

[55] Privacy Act, ss 28-28B.

[56] Privacy Act, Pt VIB.

This would require that the OAIC be given a broader remit and appropriate funding to enable it to perform this expanded role.

Given that some of the expanded rights would be difficult to apply in the absence of a Bill of Rights or a Human Rights Act or Charter, there could be value in specifically including references to the relevant international human rights in the Privacy Act and requiring that they be taken into account (together with relevant jurisprudence concerning their interpretation) in interpreting an expanded set of Australian Privacy Principles.

Concluding comments

There are two privacy-related issues raised by new technologies which require further multidisciplinary research and input because they challenge the underlying assumptions of privacy laws that that privacy is a right that belong to individuals (and not groups of individuals) and that cannot be violated if an individual is not identifiable.

The issue of group privacy arises because much of modern data analytics relies on classification and the analysis of defined groups for the purpose of making predictions about them or seeking to influence their behaviour. These groups do not necessarily align with the classes or attributes protected under existing anti-discrimination laws[57] and members may be discriminated against on the basis of their membership of one of these groups without even none of their personal information was handled and without them being aware that they have been classified as belonging to a group.

A related issue is that it is organisations are increasingly able to action or make decisions that 'control and steer individuals without the need to identify them'.[58] They are able to do so because 'the records maintained by especially large institutions – records that contain no identifying information – may become so rich that they subvert the very meaning of anonymity'.[59]

Both of these developments raise human rights considerations because they undercut autonomy by reducing the ability of individuals to control their identities and because they have the potential to undermine the fair and equitable treatment of individuals.

In addition, we need to understand better what can be done in terms of achieving algorithmic transparency.

[57] Some of these group attributes may be proxies for protected attributes, but this may be difficult to detect based on the complexity of the processing.

[58] Serge Gutwirth and Paul de Hert, 'Regulating Profiling in a Democratic Constitutional State' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer, 2008) 271, 289.

[59] Solon Barocas and Helen Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press, 2014) 44, 54.