Submission on the Australian Data Strategy

Submission to the Department of the Prime Minister and Cabinet

30 June 2022

Dr. Brydon T. Wang
TC Beirne School of Law
University of Queensland
Brydon.Wang@uq.edu.au

Contents

1. Introduction 3

Summary of key points 4

2. Data quality as a key strategy to maximising the value of data 5

2.1 Types of data collected is critical 6

2.2 Data modelling as critical infrastructure 7

3. Data to be handled in Trustworthy manner 9

3.1 What is trustworthiness? 9

3.2 Ability 10

3.3 Integrity 11

3.4 Benevolence 12

3.4.1 Transparent processes to ensure genuine value consensus 12

3.4.2 Transparent seams in automated process to introduce human discretion 13

3.4.3 Transparency built on mutual vulnerability 14

3.5 Increasing data literacy to improve individual propensity to trust 14

4. Author 16

1. Introduction

Thank you for the opportunity to make a submission to the Department of Prime Minister and Cabinet in response to ***Australian Data Strategy***. Author details are set out at the end of the submission in Section 4.

This submission responds to the Strategy in a focused manner that addresses two of the key themes of *maximising the value of data*; and *trust and protection* of data. These two themes frame the structure of the submission with Section 2 examining how value is created from data across its lifecycle and Section 3 considering the importance of trustworthiness in formulating a regulatory approach to ensure that data management policies and regulation are fit-for-purpose and benevolent to society.

This submission focuses primarily on data extracted from the built environment and is structured to reflect the data lifecycle within the smart city. The choice to contextualise the *Australian Data Strategy* within the context of the built environment arises for two key reasons:

- Smart cities are built on the integration of automation and data that enables examination of the value creation process in data and its socio-political impacts. [1]
- Datasets from a range of infrastructure projects and construction sites are now being combined by smart city proponents across public, private and civic sectors to create digital models with ever-increasing urban footprints.

The data collected in our cities contribute to an emerging digital model that offers the possibility of automated decision-making to determine how we allocate infrastructure, resources and services to urban occupants. Consequently, our interactions with data-focused technologies are particularly acute in smart cities and thus provide a strong means of determining how value can be created from data and managed in trustworthy ways.

[1] Brydon T Wang, ‘The Machine Metropolis: Introduction to the Automated City’, in Brydon T Wang and CM Wang (eds) (2021: Springer) *Automating Cities: Design, Construction, Operation and Future Impact* 2.

Summary of key points

The following key points outline the basis of this submission.

- While data is seen to be valuable when it can be appropriately shared and reused, clearly scoping the type of data and output variable will ensure that data remains economically and socially valuable, protected and reusable through the data lifecycle.
- This submission recommends a widely-applied definition of trust and a model of trustworthiness as a strategic framework to organise future regulatory and policy efforts, and to ensure the trustworthy management of data through its lifecycle.
- While the *Australian Data Strategy* seeks to establish standards to keep data safe and secure, its examination of what is ethical use of data through the entire data lifecycle should be undertaken from a clear regulatory lens that prioritises benevolence.
- Benevolent use of data can only be achieved through a specific form of transparency on the part of government, technology developers and users of data. This form of transparency must be based on:
    - value consensus arising from data-literate individuals exercising their digital right to the city. Regulatory and policy efforts generated from shared values will have stronger public support and be perceived as more benevolent;
    - ‘seams’ in any automated process to allow for human exercise of discretion and democratic data governance that allows data subjects to impact policy-making around data management (ie, caution should be taken in any process that seeks to prioritise ‘seamlessness’); and
    - a flexible and responsive approach to reducing the access imbalance to how data is consumed over the data lifecycle. This requires a form of mutual vulnerability that that needs to be accompanied by robust auditing processes funded by users of data.
- A Data Care model is recommended to ensure the public is made aware of risks and the economic and social value of data. This supports transparency built on value consensus to occur. The Data Care model is set out in section 3.5.

2. Data quality as a key strategy to maximising the value of data

The economic and social value of data is inherently linked to its quality and usefulness in decision-making around priorities. In Australia, our data protection and privacy legislative frameworks are oriented on ensuring the accessibility of data for commercial uses while balancing the need to protect personal information of individual data subjects.

However, increased production of data and increased accessibility of data needs to be accompanied by greater awareness of how fragmentation of data can create blind spots and compromise overall quality of data. This requires careful examination of:

- the selection criteria of such data. That is, how value is attributed to data to justify its addition and the role it plays in a specific decision-making process;
- how the data is modelled, presented, interrogated, and what data analytical frameworks are applied; and
- the need to signal trustworthiness in the development and deployment of data-focused technologies.

With the datafication of our smart cities, how we bring data into our decision-making processes is critical. First, when we build our decision-making processes around data, we create a data loop that feeds off itself. We extract data from the built environment, analyse and transform this abstract data into decision outputs that return to the built environment to impact the physical fabric where we again draw data from.[2] Data collection becomes the lens through which we understand what is happening in the physical fabric of our cities. This process can lock in certain default narratives and ways of looking at a problem. As data moves through this data lifecycle in a loop that both draws from and feeds into its reality, it is imperative that the extraction of data is performed in a trustworthy manner to ensure data, data-focused technologies, and outputs do not distort the physical world.

Second, the increased production of data types and the volume of data is creating a data scale problem where the quantity and spectrum of data is fast outpacing our ability to understand this information. Without careful choices in how we aggregate and model data, there is a risk that we will be unable to critically evaluate the usefulness of such data and to regulate its use in our decision-making processes.[3] Accordingly, the question of maximising the value of data is not just a question of the appropriate quantities of data that need to be collected, but a question of an appropriate balance of the quality of such data to ensure that what is collected allows an accurate model of the physical world.

This requirement to strike the appropriate balance on data collected still requires us to set a minimum level of quality but it speaks to a need to ensure we remain open to including or excluding different types of data in a way that reflects the shifting needs and values of society. The *Centre for Digital Built Britain* notes that a dynamic standard in quality of data will permit data-focused strategies and

[2] Esther Keymolen and Astrid Voorwinden, ‘Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm’ (2020) 24(3) *International Review of Law, Computers & Technology* 233, 238.

[3] L Wan, T Nochta and JM Schooling, ‘Developing a City-level Digital Twin—Propositions and a Case Study’ (2019) in the proceedings from the *International Conference on Smart Infrastructure and Construction*, 187, 189.

technologies to meet the changing requirements of 'functionality, security and longevity', but it is essential that the quality attributes of data need to be transparent, defined and measured'. [4]

2.1 Types of data collected is critical

The type of data collected is intimately linked to the problem a decision-maker (as data user) intends to solve. In any given data collection process, how a problem is scoped and what goal the decision-maker intends to solve undergoes a translation process where the goal is parsed into clearly defined outcome variables that in turn impact:

- the defining of data type and parameters;
- how such data will be collected (ie its provenance); and
- the value the data is intended to provide to the decision-making process.

This translation into outcome variables then impacts the selection or design of the sensor.[5]

For example, in the case of an autonomous vehicle developer, the problem-solving processes may have a goal of minimising human casualties. But the translation of the goal into a prediction and classification of objects around the autonomous vehicles as 'pedestrian', 'animal' or tree' will dictate the form of output variable, how data is collected through input variables, and what sensors will be developed and deployed.[6]

However, as this process means that the type of and collection of data is pre-defined, it can carry with it bias arising intentionally or unintentionally from assumptions made by technology developers and policymakers that can thwart the effectiveness of data collection and ultimately the value of such data. It is critical to guard against bias to ensure that it does not intrude on the scoping process. In these scenarios, the scope of data collection practices requires interrogation of the validity of assumptions made in the design and deployment stages to ensure that data is not just imbued with economic value, but that the social values that emerge around data are considered as part of democratic data governance.

As indicated above, the increasing use of sensors make correspondingly larger and more complex datasets available to a similarly increasing field of users. A wide spectrum of data is extracted from the built environment through a variety of sensors from connected objects in the internet of things (such as smart street lamps and smart bins), cameras mounted on drones, 3D mobile mapping technology and the use of radio frequency identification technology (***RFID***) etc.[7] The University of Illinois has demonstrated how video footage from camera sensors deployed on a construction site can be fed through a crowdsourcing platform to capture and analyse the length of time a worker spends on a particular work activity.[8] Amazon has also patented designs for a wearable device that would track employee locations and the position of their hands with clear impacts on the future of the workplace.[9]

[4] Centre for Digital Built Britain (2018) *The Gemini Principles* 21, Gemini Principle 6: *Quality*.

[5] David Lehr and Paul Ohm, 'Play with the Data: What Legal Scholars Should Learn about Machine Learning' (2017) 51 *University of California Davis Law Review* 653, 674.

[6] Lehr and Ohm, n 5, 655.

[7] Brydon T Wang, 'The Machine Metropolis: Introduction to the Automated City', n 1, 9.

[8] Will Knight, 'New Boss on Construction Sites Is a Drone, *MIT Technology Review*, 26 August. <https://www.technologyreview.com/2015/08/26/10635/new-boss-on-construction-sites-is-a-drone/>

[9] Mark Engler, 'The Amazon Effect: Sweat, Surveillance, Exploitation' (24 July 2019) *Guardian* 6; and Alessandro Delfanti and Bronwyn Frey, 'Humanly Extended Automation or the Future of Work Seen Through Amazon Patents' (2021) 46(3) *Science, Technology, & Human Values* 655, 655-82.

New data collection practices create new forms of data, each accompanied by a myriad of ways of measuring and analysing such data. This in turn results in a fragmentation of information that provides concurrent views from dispersed vantage points that may differ on what is happening in the built environment.[10] Similarly, data transforms as it is shared, particularly where data collection occurs via secondary disclosure from another dataset. As data is inherently contextual and linked to other datasets, without fully appreciating the context in which data is extracted from and its provenance, there are risks that the quality of data collected and subsequent analysis applied may not result in data that is both economically and socially valuable. Consequently, as data moves, it is important to retain the context or story as to where it has been, to understand how it has been collected, in supporting materials such as its metadata or linked datasets.

In the same vein, the data protection strategy to be deployed to safeguard the value of the data is also deeply linked to the type of data collected and stored. Where data collected is more sensitive (particularly in relation to a critical infrastructure asset or in medical contexts), there is a greater need to ensure the robustness of its protection. Accordingly, while this submission draws examples from the built environment, it is important that data protection strategies are aimed at the type of data collected rather than at specific industries or split across public and private sectors.

While data is seen to be valuable when it can be appropriately shared and reused, clearly scoping the type of data and output variable will ensure that data remains economically and socially valuable, protected and reusable through the data lifecycle.

2.2 Data modelling as critical infrastructure

In response to the fragmentation of data and increasing volume of data collected, new technological methods to handle, process and model collected data promptly and accurately have been in development. For the smart city, common data environments like *building information models* (***BIMs***) and *digital twins* are critical pieces of infrastructure that should be investigated and invested in.

BIMs are a technological platform typically deployed on large infrastructure projects to integrate data-sharing across various project participants (project owner, architects, engineers, quantity surveyors, contractor, operators etc) for the entirety of the lifecycle of the infrastructure asset. This allows the production of a digital model that supports management of data across the spectrum of documentation (building reports, specification, contracts, as-built documentations etc) from inception to decommissioning and demolition of the building.

Digital twins are virtual models of the physical built environment that are connected to real-time information drawn from sensors embedded in the built environment or from sensors in-built in mobile devices. The key characteristic of the digital twin is its model is generated directly from real-time data, creating an ability for digital twin operators to understand and model the effect of different changes on the physical fabric of the built environment. This submission notes that the current state of the technology is still maturing and we do not yet have the infrastructure to model the full volume of data for an entire city. Thus, we are unable to maximise the full value of data collected from the city as limitations on the size and scale of how such data can be modelled affect what types of data can be drawn from the built environment and reduce overall understanding of the wider urban context.

Consequently, technology developers and policy makers behind the development and deployment of these models need to configure data collection and data handling practices to meet the requisite

[10] Mark Austin et al, ‘Architecting Smart City Digital Twins: Combined Semantic Model and Machine Learning Approach’ (2020) 36(4) *Journal of Management in Engineering* 04020026, 1.

quality standard, but also to respond to current and future limitations in the technology. This standard should be flexible and open to modification to suit changing social values and future needs, as well as coming technological advances. For example, the UK approach to digital twin standards requires technology developers ensure that the technological offering is flexible enough to draw from a changing spectrum of sensors, ensure that that the variety of data collected is kept secure and portable.[11]

Technology developers and policy makers must also ensure that data collected, modelled and used produces genuine insight to shape decision-making. That is, there must be a clear demonstration that such models return a better result where data is used in the decision-making process. For example, where the use of an automated decision-making system can model and configure a traffic system to produce better traffic flows.

Finally, in order to maximise the value of data, there needs to be transparency as to what types of data are collected; the journey of its collection; and how such data is then modelled, analysed and presented for interrogation. This would preclude the use of generic big data models that are built to imbibe ‘any available sensor data, for any purpose and for any given time’.[12] Instead, transparency is necessary to ensure technology developers and policy makers are in position to be held accountable to the public and to clearly demonstrate trustworthiness in data management principles and processes. The next section considers how the Government can potentially improve the signals of trustworthiness in its regulatory approach to data.

[11] Brydon T Wang and Mark Burdon, ‘Automating Trustworthiness in Digital Twins’, in Brydon T Wang and CM Wang (2021: Springer) *Automating Cities: Design, Construction, Operation and Future Impact*. 355–6.

[12] Wang and Burdon, *Automating Trustworthiness in Digital Twins*, n 11, 355.

3. Data to be handled in Trustworthy manner

3.1 What is trustworthiness?

The *Australian Data Strategy* sets out the 'trust and protection' of data as one of its three key themes. However, the concept of 'trust' itself is not defined within the Strategy. While defining 'trust' is often challenging,[13] this submission recommends that trust be defined as an attitudinal willingness to be vulnerable to the risk posed by another party either in action or inaction.[14]

A potential recipient of trust (a ***trustee***) needs to convey signals of trustworthiness to the giver of trust (a ***trustor***), who in turn *may* develop an attitudinal willingness to be vulnerable (trust) based on their propensity to trust. To maximise the value of data, rather than focusing on the wider aim of developing public trust (which will require further study on individual propensity to trust within a given population), a more focused approach would be to consider how new data-focused systems are developed and deployed in a trustworthy manner. That is, the focus of the Government's regulatory approach should be on the signals of trustworthiness that policy makers, technology developers and users of data need to provide to individual data subjects and the wider public. Section 3.5 provides an example of how the Government could potentially address individual propensity to trust through the *Data Care* model.

Section 2.2 of the Strategy notes three 'drivers of public trust'. These drivers are a useful starting point in considering how trustworthiness may provide a more robust means to examine how public trust can be achieved. The three elements of trustworthiness—*ability*, *integrity* and *benevolence*[15]—roughly align with the three drivers of public trust set out in the strategy paper (see Table 1 below).

Table 1: The drivers of public trust mapped onto the elements of trustworthiness

Trustworthy element	Definition of the trustworthy element	Driver of public trust identified in the *Australian Data Strategy*
Ability	demonstration of the required skill set defined by the trust scenario	robust and appropriate privacy and security system and processes
Integrity	the trustee's demonstration of compliance with the same set of values and social norms as the trustor	a strong record of performance and delivery
Benevolence	the perception of the trustee's intent to mean the trustor well and look out for their best interest	transparent and meaningful engagement with Australians on data collection, use and sharing

[13] G Elofson, 'Developing Trust with Intelligent Agents: An Exploratory Study' (1998), in *Proceedings of the First International Workshop on Trust* 125. See also: Thomas W Simpson, 'What Is Trust?' (2012) *Pacific Philosophical Quarterly* 550, 550; Mila Hakanen and Aki Soudunsaari, 'Building Trust in High-Performing Teams' (2012) 2(6) *Technology Innovation Management Review* 38, 38.

[14] This definition of trust is adapted from the definition proposed by Mayer, Davis and Schoorman in 1995 that is built into their widely-applied model of trust. This model of trust was formulated from trust literature drawn across multiple social disciplines and has been cited more than 26,000 times in numerous disciplines.

[15] These three trustworthy elements are drawn from the model of trust proposed by Mayer, Davis and Schoorman in 1995.

The following sections of the submission aim to demonstrate the potential use of the three elements of trustworthiness to articulate how trustworthiness is being conveyed and structure future development of policy and the *Australian Data Strategy*. Each of the following sections examines the Strategy from the specific trustworthy element of ability, integrity or benevolence and provides recommendations on how to provide a stronger signal of trustworthiness.

3.2 Ability

Within the context of law and regulation, there is a blurring of boundaries between the trustworthy elements of ability and integrity. This blurring occurs when a trustee is not perceived as competent because their behaviour does not comply with the legislative requirement to demonstrate value alignment with the law, industry standards and social norms. For the government, ability is demonstrated in good enforcement mechanisms to ensure compliance with regulatory frameworks. For the regulated entities, ability is demonstrated in clear evidence of compliance with regulatory frameworks.

The *Australian Data Strategy* noted that the majority of Australians surveyed indicated a problem with how their personal information had been used between 2019-20. The Government has indicated a need for a more robust regulatory approach to communicate sufficient signals in regulatory ability to safeguard the individual data subject's personal information and ensure that regulation of data keeps apace with the development of data-focused technologies.

To convey a stronger signal in the trustworthy element of ability, this submission recommends the Government's regulatory approach should be aimed at enforcing greater technical or functional ability in regulated entities. An example is the Notifiable Data Breaches scheme under the *Privacy Act 1988* (Cth). The regulatory framework is oriented on penalising a failure to inform on a data breach but does not penalise for the data breach itself. Clear regulatory reform targeting and recognising the significant risk associated with certain breaches should be encapsulated in the Government's regulatory framework to ensure that data protection and cybersecurity is clearly within the corporate governance agenda. This will signal to the public that organisations collecting, using, disclosing and storing critical data are put on notice that they will be held accountable for their ability to set in place appropriate data management processes.

Recommendation

This submission submits that to improve signals of regulatory ability in respect of data, the Government's regulatory approach needs enforce greater technical or functional ability in regulated entities and not focus just on a failure to inform. In doing so, regulated entities will also be able to convey improved signals of technical ability to the individual data subject and general public.

3.3 Integrity

The Government signals the trustworthy element of integrity through enacting coherent legislation and introducing policy frameworks that demonstrate alignment with the values of the individual data subject and wider public. The *Australian Data Strategy* steps through the key legislative frameworks that sit within the Australian regulatory landscape around data. These frameworks seek to establish the Government's integrity by communicating a shared value around privacy and compliance with various domestic and international law. These have largely been located under the umbrella term 'data ethics', by which the Government outlines a number of its approaches (among others):

- the Government's review of the *Privacy Act 1988* (Cth) to assess if the regulatory mechanism is sufficiently scoped and its enforcement mechanisms are fit-for-purpose;
- the data ethics framework developed by a number of Australian Government agencies;
- compliance with the Australian Public Service code of conduct (***APS code of conduct***) and the 'continued application of ethical practices by monitoring and identifying ways to govern new technologies, such as machine learning and artificial intelligence';
- the four values that emerge from the *International Cyber and Critical Technology Engagement Strategy* (ICCTES) in relation to cross-border data flows and usage; [16]
- Australia's AI Ethics Framework; and
- reforms to 'strengthen privacy protections online with the proposed introduction of a new binding code for certain online platforms, such as social media entities'.

There will be increasing pressure to harmonise and demonstrate coherence in the Governments regulatory efforts to meet the community's expectations and, given the ease with which data flows across boundaries, international expectations. However, it is critical that attention is also paid to the interface of domestic and international law and in formulating regulatory and policy efforts to ensure that any Governmental approach aligns with domestic values. Despite cross-boundary expectations of how data is to be collected, used, disclosed, stored and disposed of, careful calibration of regulatory responses is required to critically evaluate foreign regulatory approaches and such influences on Australian laws and its data landscape.

Foreign regulatory approaches should be carefully researched to examine if they align with local values. For example, there needs to be greater research to examine whether the Australian strategy on machine learning and artificial intelligence would benefit from greater alignment with international approaches, particularly the Trustworthy AI frameworks currently being developed in the EU. Likewise, further research is needed to increase understanding of what the impacts and harms to society a failure in ability to regulate data effectively will entail. As an example, open access and open data concepts have inherent economic and social values. However, they also come with potential for significant harm that is still relatively unknown despite recent events of data misuse demonstrating the magnitude of risk. Research communities within both legislative and policy fields must work in an interdisciplinary way with data scientists and data protection experts to foster sustained collaboration on new regulatory approaches that will keep apace with emerging technologies.

[16] Pages 5 and 55 of the *Australian Data Strategy*.

Further recommendations

This submission notes that integrous data use requires harmonisation within the national privacy landscape across state and territories to:

- align individual ethical frameworks developed by various public entities;
- bring consistency and coherence between national frameworks and those in other key international jurisdictions. At the same time, there needs to be greater attention paid to data localisation to reduce misalignment between national and international values around data;
- create a consistent data classification across local, state and federal levels. This will reduce misalignment in how data is treated between various public entities; and
- align how unethical and illegal use of data is pursued nationally, with the uniform enforcement mechanism or strategy clarified and articulated to the industry.

3.4 Benevolence

The *Australian Data Strategy* recognises that one of the drivers of public trust is the 'transparent and meaningful engagement with Australians on data collection, use and sharing'. That is, active and meaningful participation of the public as data subjects will articulate the shared values and allow genuine consensus to emerge to help build public trust. Such a regulatory approach takes into account the democratic rights of individual data subjects to participate in shaping how data is collected, used, disclosed and stored in the data lifecycle. Where such processes are observed by the public, benevolence is conveyed as these transparent processes send a clear signal of positive orientation to the public.

Benevolence is a germinal factor that defines the integrity and ability elements of trustworthiness. The reason that benevolence is antecedent to the other two trustworthy elements is that it encompasses processes that result in value consensus that then informs what standards regulated entities are held to. In turn, compliance with these standards demonstrate value alignment and integrity, and are articulated in the functional and technical briefs that determine ability.

This submission argues that in order to signal benevolence to the public, transparency must take a specific form that:

- sets in place clear processes to ensure genuine value consensus occurs;
- deprioritises seamlessness in the data lifecycle from data extraction, aggregation and modelling, analysis through to decision-output; and
- positions the Government and other technology developers in a place of mutual vulnerability to ensure accountability to the individual data subject and wider public.

3.4.1 Transparent processes to ensure genuine value consensus

While commitment to transparency is a demonstration of value alignment that signals the trustworthy element of integrity, it also enables participation by the public to exercise their democratic right to influence policy decision-making. Transparency builds into the fabric of society processes that are antecedent to reaching value consensus, with the visibility of these processes signalling benevolence. It is from this specific form of transparency as benevolence that genuine value articulation and consensus emerge.

This submission contends that benevolence arises from the availability and the exercise of an urban occupant's 'digital right to the city'.[17] This right enables urban occupants to exercise discretion, autonomy and selfhood development. In permitting this digital right to the city, urban occupants are transformed from data subjects captured in a myriad of data points in fragmented datasets to involved digital citizens participating in the scoping, developing and the giving of permission to how their data is being used to drive decision-making.

A regulatory approach that seeks to demonstrate benevolence through transparent processes or policy frameworks will not communicate benevolence if it does not achieve genuine value consensus. In scenarios where there is no value consensus, public buy-in or appetite for the proposed regulatory frameworks will be blunted due to insufficient signals of positive orientation towards the individual data subject. Where there is no broad support for such regulatory intervention, the Government's regulatory efforts will not demonstrate true value alignment (or integrity) to the public, and any demonstration of technical ability against these regulatory frameworks would not send sufficient signals of trustworthiness to build trust.

In a co-authored study of the implementation of the COVIDSafe app, Associate Professor Mark Burdon and the author found that the diminished performance of the COVIDSafe app was due to a lack of transparent engagement with the public.[18] This was in part due to the urgency associated with the development and deployment of the contact-tracing app. The campaign around the adoption of the contact-tracing app was further built on certain preconceived notions and assumptions on what was valued by the community when it came to their personal data. This led to the diminished ability for the Government to convey benevolence that muted uptake of the COVIDSafe app. Despite the Government's efforts in implementing robust privacy guardrails around the app, without the public buy-in at the start (ie value consensus), there was insufficient signals of benevolence, integrity and ability to build sufficient public trust. Thus, the study demonstrated that a pure focus on enhancing legal protections to demonstrate assumed shared values (ie a demonstration of integrity) without meaningful engagement will not yield trust formation. This submission strongly supports the key theme of 'transparent and meaningful engagement with Australians on data collection, use and sharing' in the *Australian Data Strategy* and recommends that this be articulated to the public as their digital right to the city.

3.4.2 Transparent seams in automated process to introduce human discretion

For a digital right to the city to be made available, seamlessness in the automated decision-making processes that seek to extract and realise the value of data needs to be examined and re-evaluated. Information privacy regulation produces an ability to introduce 'seamful stopgaps' in the data lifecycle. This requires the introduction of 'seams' or hold points within the various processes that automate data management, such as at the point of collection, at the point where data is then aggregated and modelled, when the data is subjected to multiple iterations of analysis, and particularly at the point where any outputs are used to make policy decisions and implement change. While such an approach may slow down the overall automated use of data, it will create a human-centred process that increases the value of data and convey signals of benevolence with the introduction of human discretion.

However, where such seamful transparent processes might run into issues is in relation to the design and deployment of artificial intelligence and automated decision-making systems. These systems tend to be opaque and certain algorithmic functions are not easily translated to human logic, that then run seamlessly from data collection to decision output, reducing the ability of the public (and regulators) to have oversight over how data is used to drive decision-making. This submission recommends further research into how seamfulness could be designed into the development and deployment of such automated decision-making systems.

[17] Brydon Wang, 'The Seductive Smart City and the Benevolent Role of Transparency' (2021) 48 *Interaction Design and Architecture(s) Journal* 100.

[18] Mark Burdon and Brydon Wang, 'Implementing COVIDSafe: The Role of Trustworthiness and Information Privacy Law' (2021) 3(1) *Law, Technology and Humans* 1

Further, the seamlessness in data management processes that operate across the data lifecycle is built on a power imbalance where technology developers and policy makers have full visibility of data, while individual data subjects are faced with a black box. This creates an 'access asymmetry' that makes 'seamful stopgaps' critical to trustworthy data management processes. To enable seams in the automated process (that in turn allow value consensus to occur), there must be a diminution of this access asymmetry that is built on a regulatory and design approach of mutual vulnerability.

3.4.3 Transparency built on mutual vulnerability

Transparency is not just fully detailing processes and setting in place hold points or seams to reduce risks associated with seamlessness. Instead, transparency also requires transparency of power structures that requires parties to be mutually vulnerable.[19] This submission suggests that a position of mutual vulnerability in the context of regulation would be for the government to acknowledge the significant power imbalance that is baked into the current data landscape that makes it difficult for data subjects to participate in democratic participation around policy-making around data management. This imbalance pervades the system where data subjects are subjected to significant unequal bargaining positions against technology developers and users of data.

One of the ways in which the Government can demonstrate transparency built on mutual vulnerability is to significantly invest in educating and raising the data literacy of the public. This may render the Government more vulnerable to an increased public appetite for regulation and further restrictions on how data can be collected, used, disclosed and stored, shifting the balance away from the current regulatory default. However, for transparency to produce the signals of benevolence to the public, this mutual vulnerability in relation to raising data literacy of data subjects is required and may potentially increase individual propensity to trust.

3.5 Increasing data literacy to improve individual propensity to trust

In trust formation, a trustor's *propensity to trust* affects their ability to perceive the factors of trustworthiness to produce trust as attitudinal willingness. In order for signals of trustworthiness along the elements of ability, integrity and benevolence to be strongly received by data subjects, the public needs to be sufficiently data-literate. This will allow data subjects to understand *how* and *why* the Government has set in place fit-for-purpose privacy practices and data management processes.

In the author's co-edited collection *Automating Cities: Design, Construction, Operation and Future Impact*, Foth and colleagues proposed a Data Care model that was built around a physical location in the city where the public could learn and meaningfully engage with proposed data management strategies and data-focused technologies potentially earmarked for deployment. [20] The Data Care model was proposed as a framework, rather than a technological solution, to gradually embed good data practices in the city. The principle of the framework is built on the need for data management policies to be led by the public. That is, achieving value consensus on how data-focused technologies should be integrated in cities based on what individual members of the public need, what their shared vision of the data future of the city is, and aligning the technology to those needs and goals rather than creating technology as answers in search of questions and attempting to create new 'markets'.

The physical space in the city would be used to run four key service programmes targeting:

- **data awareness:** a one-to-few clinic where individual data subjects benefit from advice and guidance from data scientists trained in good data practices. For example, an individual could bring in data downloaded from the various digital platforms they are users on and be guided through the data set through participatory data visualisation tools. These tools could convert their data into graphic models and lists to visualise data such as location history as heat maps, or length of interaction as graphs or network maps. The aim of the clinic is to help individual data subjects understand how their data is

[19] Burdon and Wang, above n 18, 12.

[20] Marcus Foth, Irina Anastasiu, Monique Mann, and Peta Mitchell, 'From Automation to Autonomy: Technological Sovereignty for Better Data Care in Smart Cities', in Brydon Wang and CM Wang (eds) (2021: Springer) *Automating Cities: Design, Construction, Operation and Future Impact* 319.

being collected, used and disclosed, stored and how deep insights could be generated from seemingly fragmented data points;

- **data literacy:** where public seminars are run in the physical space to take members of the public through various social and legal issues. For example, seminars could cover the basics of the difference between click-wrap and browse-wrap agreements, how the law defines 'informed consent' of a user on a digital platform; how to use data analysis tools, or how technological sovereignty is beneficial to society;
- **data action:** by using the physical space to enable various community groups and small businesses to access data tools and experts to make their case for various data strategies. Foth and colleagues provided an example of a cycling group utilising the facilities at the physical space to visualise location data captured in their cycling journeys, ensuring the data was only stored locally and temporarily, and through aggregation of the data, model the network of cycling paths used in the city to advocate for additional cycling infrastructure in areas of high use; [21] and
- **data futures:** where various stakeholders from across industry and civic groups are brought it to engage with decision-makers from the public sector to consider the impact of new data-focused technologies proposed for the built environment. This will add to the level of transparency and meaningful engagement that is sought under the *Australian Data Strategy*.

By increasing data literacy, individual data subjects are given the opportunity to appreciate the negative personal consequences of data misuse and the means of exercising their digital right to the city to influence data management policy. While this may raise individual propensity to trust in such transparent processes around data management policies, the Government is also demonstrating vulnerability in being transparent about its processes and working through its decision-making on data-focused technologies with stakeholders. Along with transparent processes based on establishing value consensus and embedding hold points where human discretion is brought into automated systems, such a regulatory and policy approach to data management will convey benevolence to individual data subjects and the wider public.

In conclusion, a greater understanding of transparency as benevolence is required to build sustainable regulatory structures that are capable of adapting to continual societal changes wrought by attempts to extract and create economic and social value from data.

Further recommendations

This submission recommends that in order to increase reception of any signals on the Government's trustworthy ability to regulate data, the Government should tackle the lack of digital and data literacy, ensuring that understanding of data management practices goes beyond just compliance with the regulation and law around data use both domestically and internationally.

[21] Foth et al, above n 20, 335.

4. Author

Dr. Brydon T. Wang
TC Beirne School of Law, University of Queensland

https://www.linkedin.com/in/brydonwang/

Brydon Wang is a lawyer and scholar researching at the confluence of technology, law and smart cities. He has practised as a technology and construction lawyer with top-tier law firm Allens advising a range of clients including NBN Co, Vodafone Hutchison Australia, Chubb, and Google, across a range of obligations including the *Public Governance, Performance and Accountability Act 2013* (Cth), the Protective Security Policy Framework, the *Telecommunications (Interception and Access) Act 1979* (Cth), carriage service provider and internet service provider requirements, and on digital currencies. He has twenty years in infrastructure delivery and the construction industry, and recently co-edited the book *Automating Cities: Design, Construction, Operation and Future Impact* (Springer, 2021). His research interest lies in regulating to enhance trustworthiness in the design and deployment of automated decision-making systems in cities (BIMs, Digital Twins) and the automation of infrastructure delivery. Brydon also holds a Master of Public Policy and Management.

Contact details

Brydon T. Wang
E **brydon.wang**@uq.edu.au
W uq.edu.au

CRICOS Provider Number 00025B