Australian
National
University

National Security College

POLICY OPTIONS PAPER
No 10, January 2019

From secrecy to agency: Trust and policy implications of shifting public attitudes to privacy

Adam Henschke, Ryan Young, Maia Gould and Hannah Smith

Key points

- The public typically trusts governments to protect personal data more than they trust the private sector. Social media companies are among the least trusted.
- In response to changes in technologies, public attitudes towards privacy are changing. A traditional focus on secrecy is giving way to a focus on control of information and maintaining dignity.
- People are generally happy to share information, and for organisations to do more with the information they hold, provided this occurs in a way that maintains trust.
- Privacy concerns are not just about potential harms, but also potential inequalities and injustices where information is used differently to why it was collected.
- Organisations can build trust by giving individuals control over their information (where possible), providing clarity about how they use information, assuring people that it is treated with care, and demonstrating competence in what they do.

Policy recommendations

- To build trust, government departments should communicate consistently how they use and protect personal information, rather than simply state that they comply with legislation.
- Departments can increase data-sharing while maintaining trust, provided they focus on the purpose for which information was originally collected.
- Where possible, departments should use analytic tools that allow automated extraction and sharing of relevant data and reports, rather than entire data sets.

Surveyed attitudes to government

While public trust in government generally has been falling,[1] trust in governments to manage personal information has remained steady, and strong in comparison to other organisations. For example, 58% of participants in the 2017 Australian Community Attitudes to Privacy Survey rated both federal and state government departments as trustworthy stewards of personal information.[2] This was well ahead of trust in most areas of the private sector, including charities (38%) and retailers (28%), but behind trust in health service providers (79%) and financial institutions (59%). Most notably, the social media industry ranked lowest, with only 12% of participants considering it a trustworthy manager of personal information.

These attitudes are supported by reported actions. In 2017, only 16% of Australians stated that they had decided not to deal with a government organisation because of privacy concerns. By contrast, a majority of Australians (58%) have decided not to deal with a business because of privacy concerns.

Notably, survey data suggests that lack of trust in government competence is the reason why people might oppose government agencies sharing their information. When asked to explain why they would not be in favour of agencies sharing their information, 62% of Australians and 67% of New Zealanders responded: "it's not clear to me how government would use my data".[3]

Evolving public attitudes to privacy

The research on trust raises some puzzling questions. Only 12% of Australians consider that social media companies are trustworthy with their information, yet it is estimated, for example, that about two thirds of Australians (15 million) use Facebook at least monthly.[4] Why do so many provide their information to social media companies when they do not consider them to be trustworthy?

A key to the puzzle is to understand the way that public attitudes to privacy are, and have always been, shifting in response to developments in technology.

For example, the notion of privacy as a (legal) right was developed at the end of the 19th century in response to surveillance fears—at that time the invention of portable photography.[5] As surveillance technologies advanced, and data became computerised, attitudes to privacy have also evolved.

Before we as online humans cast such long data shadows, we tended to focus on privacy as a right and in terms of **secrecy**. On this view, keeping something private is to keep it secret, and we all have the right—unless we consent otherwise—to have certain things about us kept secret.[6]

An additional way to understand privacy is that it is about having **control** over one's personal information and being treated with dignity.[7] On this view, information is private if I believe I should have some control over who can access it. If I have given someone access, I expect that they will treat it with care and respect—and not use it for something I wouldn't want it used for.

Given the ongoing erosion of secrecy due to a range of technologies, it seems likely that the public today is adopting this second, more pluralistic conception of privacy.

This helps explain people's high use, but low trust, of social media. Context matters. People may be willing to share information with a specific group, but are horrified when they find out that others can access this information.

People are also willing to accept certain uses of their data in exchange for fair value—typically, access to online services. We should also expect public perceptions of what is a fair exchange to change over time, for example as people begin to appreciate the value of their personal information.

Once we understand privacy as not being primarily about secrecy, we expect people to be willing to share personal information. However, they will expect appropriate action in return, in particular:

1. to retain some **control** over how it is used and further shared,
2. **clarity** regarding how it is used,
3. that it is treated with **care**, and
4. with a level of **competency**.

Injustice, not just harm

A second aspect to the concept of privacy is to understand why people want privacy, or alternatively what privacy seeks to prevent.

The traditional analysis tends to focus on avoiding direct losses—or harms. These include financial, reputational and legal costs that arise when privacy is breached.

But focusing on harms makes limited sense of public reactions to privacy issues. For example, in June 2017, Google announced that it would no longer scan personal emails in Gmail to better target advertising following negative public reactions.[8] Few direct harms could have arisen from Gmail targeting advertising in this way. Personal information was not shared outside of Google and, arguably, users benefitted by receiving ads they were more likely to be interested in.

People's concerns about privacy are broader than simply preventing harm. One framework identifies four types of concerns that people might have:[9]

- Information-based harms,
- Informational inequality,

- Informational injustice, and
- Encroachment on moral autonomy.

An informational inequality occurs when someone gets unequal access to a service or product. An informational injustice occurs when information intended for one context is used for another.

The backlash against Gmail scanning emails is a textbook example of an informational injustice. Google deciding to scan the contents of personal emails—information only provided to Google as a carrier, not as a receiver—to target advertising, is a case of using information intended for one context for a different one. This may help explain why so many people were uncomfortable with it.[10]

Communicate clearly and assure the public

Government departments and agencies generally do a good job at ensuring personal information is treated appropriately.

Indeed, their safeguards at times appear to be stronger than the public expects or wants. For example, nine out of ten citizens assume that agencies are already sharing personal information, especially basic data like demographics and tax file numbers.[3] However, as government officials know, it is often difficult to share any information about citizens between departments.[11]

This gap between what the public expects and what occurs is a result of poor communication by agencies. Too often, they default to explanations about how they treat personal information that refer to compliance with the *Privacy Act* rather than explaining in simple language what they actually do.

Moreover, the emphasis in government communication tends be on keeping information secret. Communications should clearly identify what data is collected, and how it will be managed and treated with care.

Share, but with care

As the informational injustice concept suggests, if information is used for the same purpose that it was shared for, then people are generally comfortable.

More detailed research is required to understand the public perceptions and ethical boundaries around what constitutes the 'same purpose'. A useful starting point is to consider that government collects personal data for four broad purposes:

- Improving policy and decision-making (e.g. ABS data)
- Service delivery (e.g. health or veterans records)
- Improving compliance (e.g. tax or Centrelink data)
- Security (e.g. data collected by ASIO, AFP or ASD)

Slippage of data between categories—particularly between category 1 (where data is generally de-identified and used in aggregate) and other categories (where individuals are identified)—is generally viewed extremely badly. If, for example, data collected to improve policy and/or service delivery is later used for compliance, the public reaction may be negative and trust will be broken.

However, if data is shared for purposes within the same category, and there are good reasons for it, it is more likely that the public will accept that as legitimate.

Increasingly, information systems allow for more sophisticated and precise information sharing. Systems are increasingly being developed which allow personal information to be securely stored separately, while analytic layers are built on top that allow reports to be shared easily without the underlying data. This enables data to be shared while maintaining better control over data and reducing the opportunities for injustices and harms.

Competence, not just compliance

The challenge for governments is to focus on what it means to be competent in protecting privacy, in the context of it being impossible to guarantee complete secrecy.

Banks and financial institutions provide a useful case-study. As noted above, they are routinely ranked near the top of institutions which Australians trust with privacy and data. This is at odds with general public distrust in banks, particularly around financial advice. It is also potentially at odds with levels of financial fraud, such as theft of and misuse of credit card details, which in 2017 cost Australians an estimated $540 million.[12]

In this difficult environment, banks respond by actively treating customers' information with care, communicating with clarity and seeking to ensure customers have control over information. For example, they monitor bank accounts and credit cards actively, quickly notify people when they see a problem, rectify any losses and proactively lock cards and accounts to prevent loss.

Notably, banks do not pretend that information is fully secure but maintain public trust by being transparent when breaches occur and by rectifying losses to the extent possible.

This suggests an important lesson: competence in managing data is no longer just about protecting it from theft or misuse, it is also about responding quickly and appropriately when something goes wrong.

While the privacy issues government faces are not entirely analogous to protecting financial information, agencies must focus on acting quickly in response to privacy issues—including data breaches and uses that are challenged in public. Testing processes to respond to particular scenarios and embedding reflex processes within teams will assist departments to respond more quickly as situations arise. Slow responses create space to allow public fears to grow—particularly when questions arise about if and when an agency knew and why it didn't tell anyone.

Further work is needed

The treatment of personal data is one key aspect of the trust between citizens and governments which government actions can significantly influence. In an era where trust is declining and foreign governments are seeking to exploit this distrust, building public trust through better approaches to personal data is a significant opportunity.

However, the research base on trust and personal data remains thin. To take advantage of this opportunity, further research is needed to better understand what types of personal information people are comfortable sharing and for what purposes. More work also needs to be done to understand public perceptions of data sensitivity in different contexts. Additionally, understanding whether there are differences between countries, particularly within the Five Eyes, will be important to enable better collaboration and data-sharing.

Endnotes

[1] See Edelman Trust Barometer 2018, and Grattan Institute, *A Crisis of Trust: The Rise of Protest Politics in Australia*, 2018.

[2] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey*, p8, 2017.

[3] Unisys, *Connected Government Survey*, p9, 2018.

[4] Cowling, D, Social Media Statistics Australia, *Social Media News*, June 2018.

[5] Warren, S and Brandeis, L, The Right to Privacy, *Harvard Law Review*, 4.5, pp193-220, 1890.

[6] Henschke, A, Ethics in an Age of Surveillance, *Cambridge University Press*, pp28-53, 2017.

[7] Among others, see Innes, J, Privacy, Intimacy and Personhood, *Philosophy and Public Affairs* 6.1, pp26-44, 1976; Griffin, J, On Human Rights, *Oxford University Press*, pp225-241, 2008; and, McCartney, M, Privacy is not Secrecy, *BMJ* 352, p.i1759, 2016.

[8] Fung, B, Gmail will no longer snoop on your emails for advertising purposes, *The Washington Post*, 26 June 2017.

[9] van den Hoven, J, Privacy and the Varieties of Informational Wrongdoing, in *Computer Ethics* edited by John Weckert, pp317-330, *Aldershot: Ashgate Publishing*, 2007.

[10] For example, in a Roy Morgan survey, 69% of Australians say it is very unacceptable for companies to scrape the contents of messages or emails.

[11] See Productivity Commission, *Data Availability and Use*, Report 82, p121, 31 March 2017.

[12] Australian Payments Network, *Payment Fraud Statistics* pp1-5, 2017.

About this publication

This series of National Security College Policy Options Papers offers short, evidence-based and forward-looking insights for policy-makers on topical security, foreign affairs and geostrategic issues facing Australia domestically, in the Indo-Pacific region and globally. We seek contributions from and collaborations with qualified researchers and experts in these fields.

T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au

@NSC_ANU
National Security College

CRICOS Provider #00120C

About the authors

Dr Adam Henschke is Senior Lecturer and Graduate Convenor at the ANU National Security College.

Dr Ryan Young is the Senior Advisor, Futures Hub at the ANU National Security College.

Maia Gould is the Engagement & Impact Lead, at the ANU 3A Institute.

Hannah Smith is a researcher with the ANU National Security College.

MO_NSC16797