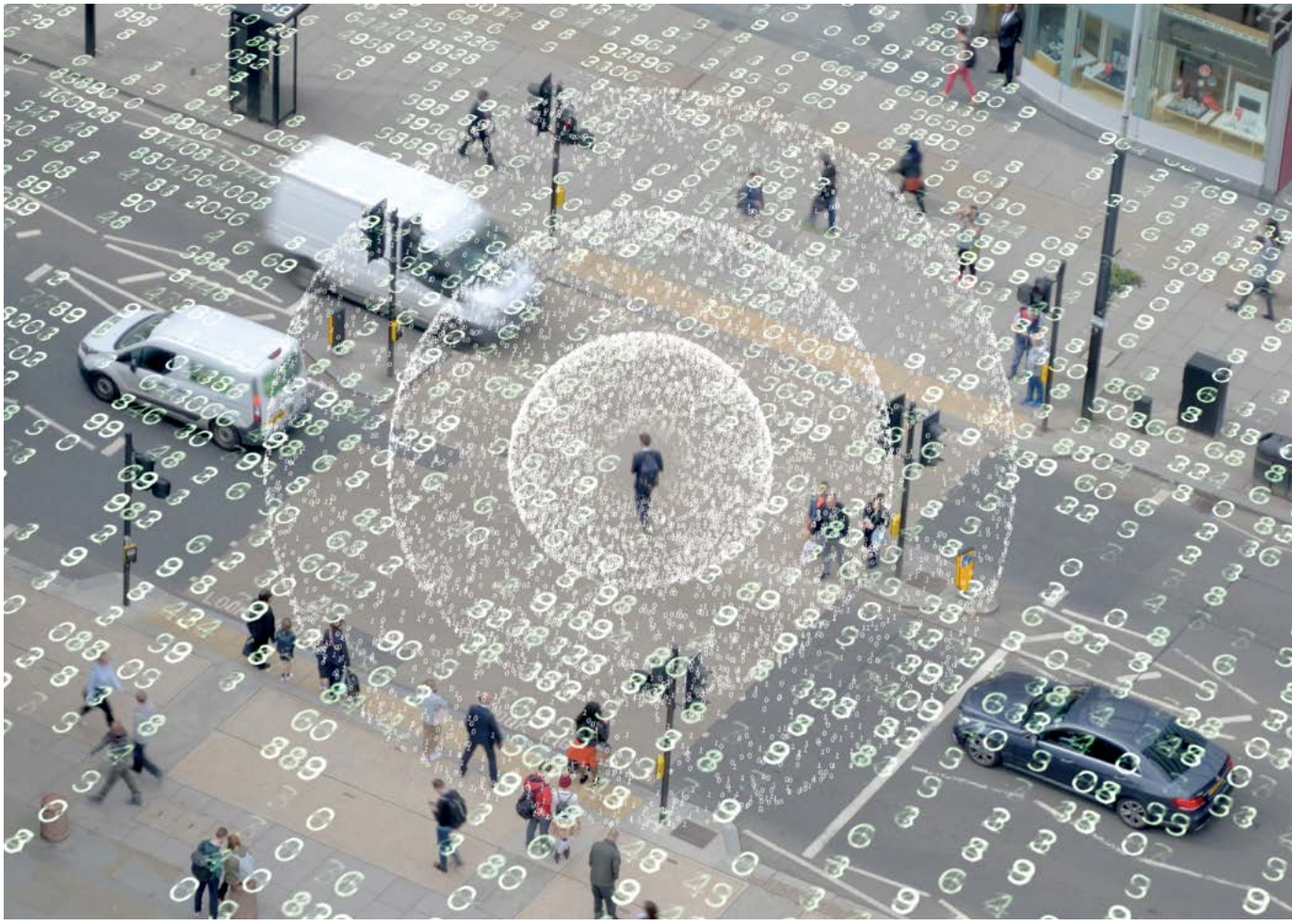
Volume | 465

# Protecting Your Privacy



Edited by Justin Healey

ISSUES IN SOCIETY

# Protecting Your Privacy

Volume | 465

ISSUES IN SOCIETY

Edited by Justin Healey

THE SPINNEY PRESS

First published by

THE SPINNEY PRESS

PO Box 438 Thirroul NSW 2515 Australia
www.spinneypress.com.au



Title: Protecting Your Privacy / edited by Justin Healey.

Series: Issues in Society, Volume 465.

ISBN 978-1-922274-30-4 (paperback)
ISBN 978-1-922274-31-1 (PDF)

NATIONAL LIBRARY OF AUSTRALIA

A catalogue record for this book is available from the National Library of Australia

Cover images courtesy of iStock.

# CONTENTS

# INTRODUCTION

**Protecting Your Privacy is Volume 465 in the 'Issues in Society' series of educational resource books. The aim of this series is to offer current, diverse information about important issues in our world, from an Australian perspective.**

## KEY ISSUES IN THIS TOPIC

Privacy is a fundamental human right; it underpins our freedom of association, thought and expression, and freedom from discrimination. It includes physical privacy, surveillance and information privacy. However, it is not absolute, it is hard to define, and sometimes harder to protect.

What are the principles and laws that apply to privacy and personal information protection? Although privacy laws have expanded in recent years to deal with emerging technologies, there are still flaws and gaps in Australia's regulation. How do tech giants like Facebook and Google profit from personal data, and how accountable are they to consumers and governments? Security cameras, CCTV, drones, ID scanning, smart home devices, GPS, tracing apps, and facial recognition technology – how much surveillance are you really subjected to by governments, corporations, hackers and law enforcement?

This title examines rights and responsibilities in relation to privacy and personal information and shines a light on the growth in digital surveillance. The book also offers advice on how to understand and preserve individual privacy and protect your personal information online. Are we too trusting, at the expense of our precious privacy?

## SOURCES OF INFORMATION

Titles in the 'Issues in Society' series are individual resource books which provide an overview on a specific subject comprised of facts and opinions.

The information in this resource book is not from any single author, publication or organisation. The unique value of the 'Issues in Society' series lies in its diversity of content and perspectives.

**The content comes from a wide variety of sources and includes:**

- Newspaper reports and opinion pieces
- Website fact sheets
- Magazine and journal articles
- Statistics and surveys
- Government reports
- Literature from special interest groups

## CRITICAL EVALUATION

As the information reproduced in this book is from a number of different sources, readers should always be aware of the origin of the text and whether or not the source is likely to be expressing a particular bias or agenda.

It is hoped that, as you read about the many aspects of the issues explored in this book, you will critically evaluate the information presented. In some cases, it is important that you decide whether you are being presented with facts or opinions. Does the writer give a biased or an unbiased report? If an opinion is being expressed, do you agree with the writer?

## EXPLORING ISSUES

The 'Exploring issues' section at the back of this book features a range of ready-to-use worksheets relating to the articles and issues raised in this book. The activities and exercises in these worksheets are suitable for use by students at middle secondary school level and beyond.

## FURTHER RESEARCH

This title offers a useful starting point for those who need convenient access to information about the issues involved. However, it is only a starting point. The 'Web links' section at the back of this book contains a list of useful websites which you can access for more reading on the topic.

# PRIVACY AND PERSONAL INFORMATION

## COURTESY OF THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

## WHAT IS PRIVACY?

Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination. But it's hard to define. Different countries offer different views, as do individuals.

Generally speaking, privacy includes the right:

- To be free from interference and intrusion
- To associate freely with whom you want
- To be able to control who can see or use information about you.

And there are different ways to look at privacy, such as:

- **Physical privacy** (for instance, being frisked at airport security or giving a bodily sample for medical reasons)
- **Surveillance** (where your identity can't be proved or information isn't recorded)
- **Information privacy** (how your personal information is handled).

Information privacy is about promoting the protection of information that says who we are, what we do and what we believe. We regulate the *Privacy Act 1988* (*Privacy Act*) which covers how your personal information is handled by Australian Government agencies and any organisation with an annual turnover of more than $3 million, and some other organisations. The *Privacy Act* doesn't specifically cover surveillance but there are situations where it may apply.

Your right to privacy isn't absolute. Sometimes other concerns are given priority, such as the safety of you or others, or the interests of justice. But it's important. That's why strict rules apply in these situations.

## WHAT IS PERSONAL INFORMATION?

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

For example, personal information may include:

- An individual's name, signature, address, phone number or date of birth
- Sensitive information
- Credit information
- Employee record information
- Photographs
- Internet protocol (IP) addresses
- Voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- Location information from a mobile device (because it can reveal user activity patterns and habits).

The *Privacy Act 1988* doesn't cover the personal information of someone who has died.

### *What is sensitive information?*

Sensitive information is personal information that includes information or an opinion about an individual's:

- Racial or ethnic origin
- Political opinions or associations
- Religious or philosophical beliefs
- Trade union membership or associations
- Sexual orientation or practices
- Criminal record
- Health or genetic information
- Some aspects of biometric information.

Generally, sensitive information has a higher level of privacy protection than other personal information.

Office of the Australian Information Commissioner. *What is privacy?* and *What is personal information?* Retrieved from www.oaic.gov.au on 30 June 2020.

# Privacy Act: rights and responsibilities

**The OAIC explains the following:**

- **What rights an individual has under the *Privacy Act***
- **The organisations and agencies the *Privacy Act* covers and those it doesn't**
- **What privacy laws apply to Australian Capital Territory public sector agencies**

## Who has rights under the Privacy Act?

The *Privacy Act* regulates the way individuals' personal information is handled. As an individual, the *Privacy Act* gives you greater control over the way that your personal information is handled.

The *Privacy Act* allows you to:

- Know why your personal information is being collected, how it will be used and who it will be disclosed to
- Have the option of not identifying yourself, or of using a pseudonym in certain circumstances
- Ask for access to your personal information (including your health information)
- Stop receiving unwanted direct marketing
- Ask for your personal information that is incorrect to be corrected
- Make a complaint about an organisation or agency the *Privacy Act* covers, if you think they've mishandled your personal information.

## Who has responsibilities under the *Privacy Act*?

Australian Government agencies (and the Norfolk Island administration) and organisations with an annual turnover more than $3 million have responsibilities under the *Privacy Act*, subject to some exceptions.

## What is an organisation?

The *Privacy Act* defines an 'organisation' as:

- An individual, including a sole trader (though generally, the *Privacy Act* doesn't apply to an individual acting in a personal capacity)
- A body corporate
- A partnership
- Any other unincorporated association, or
- A trust.

– unless they're a small business operator, registered political party, state or territory authority or a prescribed instrumentality of a state.

## What small businesses are covered?

The *Privacy Act* cover some small business operators (organisations with an annual turnover of $3 million or less), including:

- A private sector health service provider – an organisation that provides a health service includes:
  - A traditional health service provider, such as a private hospital, a day surgery, a medical practitioner, a pharmacist and an allied health professional
  - A complementary therapist, such as a naturopath and a chiropractor
  - A gym or weight loss clinic
  - A child care centre, a private school and a private tertiary educational institution
- A business that sells or purchases personal information
- A credit reporting body
- A contracted service provider for a Australian Government contract
- An employee association registered or recognised under the *Fair Work (Registered Organisations) Act 2009*
- A business that has opted in to the *Privacy Act*
- A business that is related to a business that is covered by the *Privacy Act*
- A business prescribed by the *Privacy Regulation 2013*.

# Privacy: what you can complain about

**You can complain to the OAIC about the handling of your personal information by an Australian Government agency or any organisation the *Privacy Act 1988 (Privacy Act)* covers.**

The *Privacy Act* covers organisations with an annual turnover of more than $3 million, and some other organisations. You can also complain to us about the handling of your personal information by an Australian Capital Territory agency under the *Information Privacy Act 2014 (ACT)*.

'Handling your personal information' means to collect, use or disclose your personal information. The *Privacy Act* doesn't apply to the personal information of a deceased individual. Generally, a complaint must be about a matter that occurred less than 12 months ago.

### *Your sensitive information*

Personal information includes your sensitive information, for example:

- Your My Health Record
- Your individual healthcare identifier
- Your genetic information
- Your credit report
- Your tax file number
- The information the Medicare Benefits Scheme or the Pharmaceutical Benefits Scheme holds about you
- Your criminal record (such as a spent conviction)
- Information the Personal Property Securities Register holds about you.

You can complain about the handling of your sensitive information.

### *Before you complain to us*

Contact the organisation or agency you think has mishandled your personal information to make a complaint. They should generally respond to your complaint in 30 days. If they don't respond to your complaint, or you're not satisfied with their response, you may lodge a complaint with us.

Office of the Australian Information Commissioner. *What you can complain about.* Retrieved from www.oaic.gov.au on 19 June 2020.

## Which acts and practices are covered by the *Privacy Act*?

Particular acts and practices of some other small business operators are covered by the *Privacy Act* including:

- Activities of a reporting entity or authorised agent relating to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and its regulations and rules
- Acts and practices to do with the operation of a residential tenancy database
- Activities related to the conduct of a protected action ballot.

## The *Privacy Act* also covers specified persons handling your:

- Consumer credit reporting information, including a credit reporting body, a credit provider (which includes energy and water utilities and telecommunication providers) and certain other third parties
- Tax file numbers under the Tax File Number Guidelines
- Personal information contained on the Personal Property Securities Register
- Old conviction information under the Commonwealth Spent Convictions Scheme
- My Health Record information under the *My Health Records Act 2012* and individual healthcare identifiers under the *Healthcare Identifiers Act 2010.*

## Who doesn't have responsibilities under the *Privacy Act*?

The *Privacy Act* does not cover:

- State or territory government agencies, including a state and territory public hospital or health care facility (which is covered under state and territory legislation) except:
  - Certain acts and practices related to My Health Records and individual healthcare identifiers
  - An entity prescribed by the *Privacy Regulation 2013*
- An individual acting in their own capacity, including your neighbours
- A university, other than a private university and the Australian National University
- A public school
- In some situations, the handling of employee records by an organisation in relation to current and former employment relationships
- A small business operator, unless an exception applies (see above)
- A media organisation acting in the course of journalism if the organisation is publicly committed to observing published privacy standards
- Registered political parties and political representatives.

## Privacy laws applying to ACT public sector agencies

The *Information Privacy Act 2014 (ACT)* applies to Australian Capital Territory (ACT) public sector agencies. The *Information Privacy Act* includes a set of Territory Privacy Principles (TPPs) that cover the collection, use, disclosure, storage, access to, and correction of, personal information. The TPPs are similar to the Australian Privacy Principles.

The Australian Privacy Commissioner is exercising some of the ACT Information Privacy Commissioner's functions. These responsibilities include investigating privacy complaints about ACT public sector agencies, and receiving data breach notifications from ACT public sector agencies.

Office of the Australian Information Commissioner. *Rights and responsibilities.* Retrieved from www.oaic.gov.au on 25 June 2020.

# AUSTRALIAN PRIVACY PRINCIPLES

**The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the *Privacy Act 1988 (Privacy Act)*. They apply to any organisation or agency the *Privacy Act* covers. There are 13 Australian Privacy Principles and they govern standards, rights and obligations around:**

- The collection, use and disclosure of personal information
- An organisation or agency's governance and accountability
- Integrity and correction of personal information
- The rights of individuals to access their personal information.

The Australian Privacy Principles are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies. A breach of an Australian Privacy Principle is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

Office of the Australian Information Commissioner. *Australian Privacy Principles.* Retrieved from www.oaic.gov.au on 18 June 2020.

## AUSTRALIAN PRIVACY PRINCIPLES: QUICK REFERENCE

| PRINCIPLE | TITLE | PURPOSE |
|---|---|---|
| APP 1 | **Open and transparent management of personal information** | Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy. |
| APP 2 | **Anonymity and pseudonymity** | Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply. |
| APP 3 | **Collection of solicited personal information** | Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information. |
| APP 4 | **Dealing with unsolicited personal information** | Outlines how APP entities must deal with unsolicited personal information. |
| APP 5 | **Notification of the collection of personal information** | Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters. |
| APP 6 | **Use or disclosure of personal information** | Outlines the circumstances in which an APP entity may use or disclose personal information that it holds. |
| APP 7 | **Direct marketing** | An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. |
| APP 8 | **Cross-border disclosure of personal information** | Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas. |
| APP 9 | **Adoption, use or disclosure of government-related identifiers** | Outlines the limited circumstances when an organisation may adopt a government-related identifier of an individual as its own identifier, or use or disclose a government-related identifier of an individual. |
| APP 10 | **Quality of personal information** | An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure. |
| APP 11 | **Security of personal information** | An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances. |
| APP 12 | **Access to personal information** | Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies. |
| APP 13 | **Correction of personal information** | Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals. |

Office of the Australian Information Commissioner. *Australian Privacy Principles quick reference.* Retrieved from www.oaic.gov.au on 19 June 2020.

# Australia should strengthen its privacy laws and remove exemptions for politicians

## THE MAJOR POLITICAL PARTIES HAVE DONE LITTLE OF SUBSTANCE ABOUT PRIVACY RIGHTS, OBSERVES DAVID VAILE

As revelations continue to unfold about the misuse of personal data by Cambridge Analytica, many Australians are only just learning that Australian politicians have given themselves a free kick to bypass privacy laws.

Indeed, Australian data privacy laws are generally weak when compared with those in the United States, United Kingdom and the European Union. They fall short in both specific exemptions for politicians, and because individuals cannot enforce laws even where they do exist.

While Australia's major political parties have denied using the services of Cambridge Analytica, they do engage in substantial data operations – including the Liberal Party's use of the i360 app in the recent South Australian election. How well this microtargeting of voters works to sway political views is disputed, but the claims are credible enough to spur demand for these tools.

Greens leader Richard di Natale told *RN Breakfast* this morning that political parties "shouldn't be let off the hook":

*All political parties use databases to engage with voters, but they're exempt from privacy laws so there's no transparency about what anybody's doing. And that's why it's really important that we go back, remove those exemptions, ensure that there's some transparency, and allow people to decide whether they think it's appropriate.*

### WHY SHOULD POLITICIANS BE EXEMPT FROM PRIVACY LAWS?

The exemption for politicians was introduced way back in the Privacy Amendment (Private Sector) Bill 2000. The Attorney-General at the time, Daryl Williams, justified the exemption on the basis that freedom of political communication was vital to Australia's democratic process. He said the exemption was:

*... designed to encourage that freedom and enhance the operation of the electoral and political process in Australia.*

Malcolm Crompton, the then Privacy Commissioner, argued against the exemption, stating that political institutions:

*... should follow the same practices and principles that are required in the wider community.*

Other politicians from outside the two main parties, such as Senator Natasha Stott Despoja in 2006, have tried to remove the exemptions for similar reasons, but failed to gain support from the major parties.

## WHAT LAWS ARE POLITICIANS EXEMPT FROM?

### *Privacy Act*

The *Privacy Act* gives you control over the way your personal information is handled, including knowing why your personal information is being collected, how it will be used, and to whom it will be disclosed. It also allows to you to make a complaint (but not take legal action) if you think your personal information has been mishandled.

"Registered political parties" are exempt from the operation of the *Privacy Act 1998*, and so are the political "acts and practices" of certain entities, including:

- Political representatives – MPs and local government councillors;
- Contractors and subcontractors of registered political parties and political representatives; and
- Volunteers for registered political parties.

This means that if a company like Cambridge Analytica was contracted to a party or MP in Australia, their activities may well be exempt.

### *Spam Act*

Under the *Spam Act 2003*, organisations cannot email you advertisements without your request or consent. They must also include an unsubscribe notice at the end of a spam message, which allows you to opt out of unwanted repeat messaging. However, the Act says that it has no effect on "implied freedom of political communication".

### *Do Not Call Register*

Even if you have your number listed on the Do Not Call Register, a political party or candidate can authorise a call to you, at home or at work, if one purpose is fundraising. It also permits other uses.

## HOW DO AUSTRALIAN PRIVACY LAWS FALL SHORT?

### *No right to sue*

Citizens can sue for some version of a breach of privacy in the UK, EU, US, Canada and even New Zealand. But there is still no constitutional or legal right that an individual (or class) can enforce over intrusion of privacy in Australia.After exhaustive consultations in 2008 and 2014, the Australian Law Reform Commission (ALRC) recommended a modest and carefully limited statutory tort – a right to dispute a serious breach of privacy in court. However, both major parties effectively rejected the ALRC recommendation.

### *No 'legal standing' in the US*

Legal standing refers to the right to be a party to legal proceedings. As the tech giants that are most adept at gathering and using user data – Facebook, Google, Apple, Amazon – are based in the US, Australians generally do not have legal standing to bring action against them if they suspect a privacy violation. EU citizens, by contrast, have the benefit of the *Judicial Redress Act 2015* (US) for some potential misuses of cloud-hosted data.

### *Poor policing of consent agreements*

Consent agreements – such as the terms and conditions you agree to when you sign up for a service, such as Gmail or Messenger – waive rights that individuals might otherwise enjoy under privacy laws. In its response to the Cambridge Analytica debacle, Facebook claims that users consented to the use of their data.

But these broad user consent agreements are not policed strictly enough in Australia. It's known as "bad consent" when protective features are absent from these agreements. By contrast, a "good consent" agreement should be simple, safe and precautionary by default. That means it should be clear about its terms and give users the ability to enforce them, should not be variable, and should allow users to revoke consent at any time.

New laws introduced by the EU – the *General Data Protection Regulation* – which come into effect on May 25, are an example of how countries can protect their citizens' data offshore.

### *Major parties don't want change*

Privacy Commissioner Tim Pilgrim said today in *The Guardian* that the political exemption should be reconsidered. In the past, independents and minor party representatives have objected to the exemption, as well as the weakness of Australian privacy laws more generally. In 2001, the High Court said that there should be a right to sue for privacy breach.

But both Liberal and Labor are often in tacit agreement to do nothing substantial about privacy rights. They have not taken up the debates around the collapse of IT security, nor the increase in abuse of the "consent" model, the dangers of so called "open data", or the threats from artificial intelligence, Big Data, and metadata retention.

One might speculate that this is because they share a vested interest in making use of voter data for the purpose of campaigning and governing. It's now time for a new discussion about the rules around privacy and politics in Australia – one in which the privacy interests of individuals are front and centre.

**DISCLOSURE STATEMENT**

**David Vaile is a Board or Committee Member of Internet Australia, the Australian Privacy Foundation, the Association of Social and Market Research Organisation, and various professional, government and civil society and policy organisations.**

**David Vaile is Teacher of cyberspace law, UNSW.**

THE CONVERSATION

Vaile, D (22 March 2018). *Australia should strengthen its privacy laws and remove exemptions for politicians.* Retrieved from http://theconversation.com on 19 June 2020.

# HERE'S HOW TECH GIANTS PROFIT FROM INVADING OUR PRIVACY, AND HOW WE CAN START TAKING IT BACK

## YOUR ONLINE ACTIVITY CAN BE TURNED INTO AN INTIMATE PORTRAIT OF YOUR LIFE – AND USED FOR PROFIT, CAUTIONS KATHARINE KEMP

Australia's consumer watchdog has recommended major changes to our consumer protection and privacy laws. If these reforms are adopted, consumers will have much more say about how we deal with Google, Facebook, and other businesses.

The proposals include a right to request erasure of our information; choices about whether we are tracked online and offline; potential penalties of A$10 million or more for companies that misuse our information or impose unfair privacy terms; and default settings that favour privacy.

The report from the Australian Competition and Consumer Commission (ACCC) says consumers have growing concerns about the often invisible ways companies track us and disclose our information to third parties. At the same time, many consumers find privacy policies almost impossible to understand and feel they have no choice but to accept.

My latest research paper details how companies that trade in our personal data have incentives to conceal their true practices, so they can use vast quantities of data about us for profit without pushback from consumers. This can preserve companies' market power, cause harm to consumers, and make it harder for other companies to compete on improved privacy.

### PRIVACY POLICIES ARE BROKEN

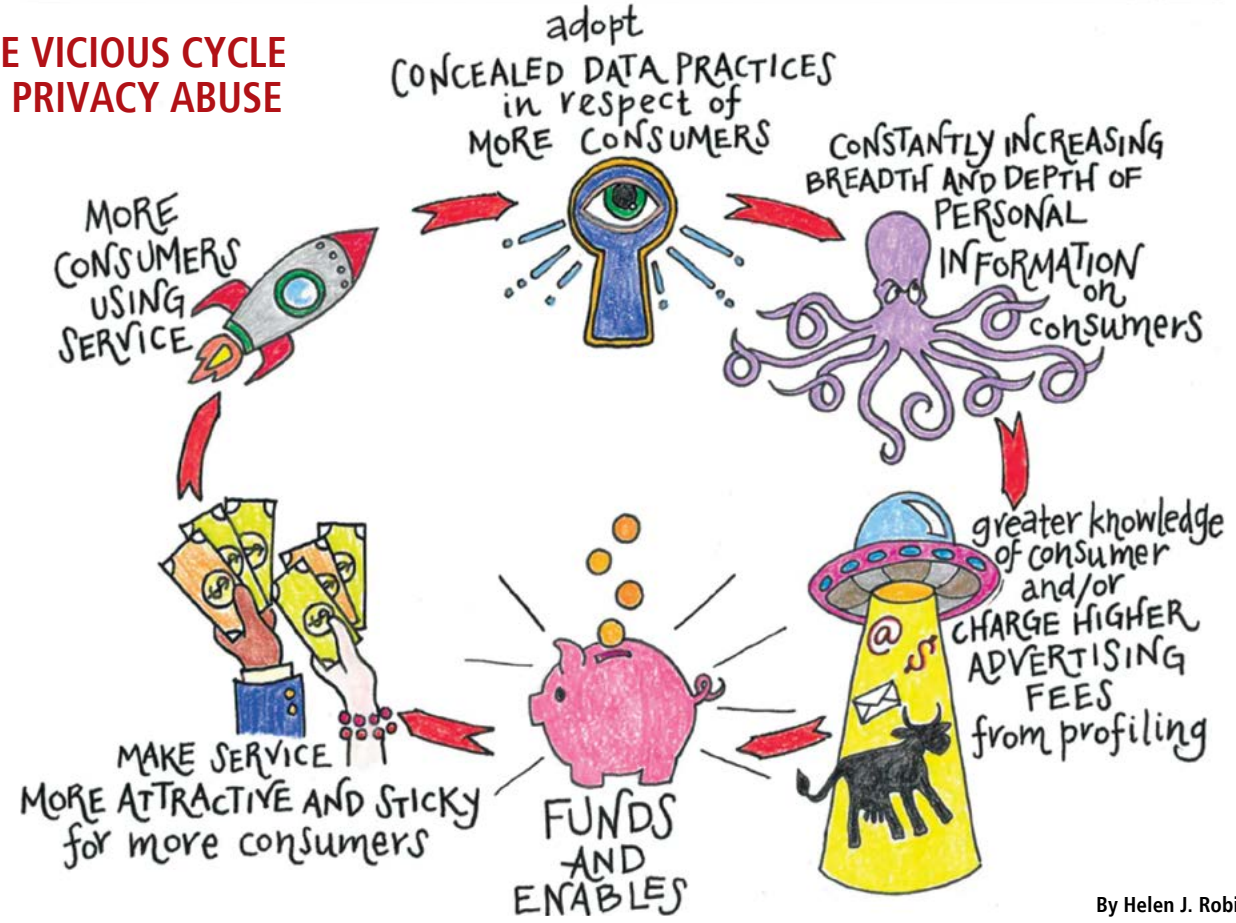
The ACCC report points out that privacy policies tend to be long, complex, hard to navigate, and often create obstacles to opting out of intrusive practices. Many of them are not informing consumers about what actually happens to their information or providing real choices.

Many consumers are unaware, for example, that Facebook can track their activity online when they are logged out, or even if they are not a Facebook user.

Some privacy policies are outright misleading. Last month, the US Federal Trade Commission settled with Facebook on a US$5 billion fine as a penalty for repeatedly misleading users about the fact that personal information could be accessed by third-party apps without the user's consent, if a user's Facebook "friend" gave consent.

If this fine sounds large, bear in mind that Facebook's share price went up after the FTC approved the settlement.

### THE VICIOUS CYCLE OF PRIVACY ABUSE




By Helen J. Robinson.

The ACCC is now investigating privacy representations by Google and Facebook under the Australian Consumer Law, and has taken action against the medical appointment booking app Health Engine for allegedly misleading patients while it was selling their information to insurance brokers.

## NOTHING TO HIDE ...?

Consumers generally have very little idea about what information about them is actually collected online or disclosed to other companies, and how that can work to their disadvantage.

A recent report by the Consumer Policy Research Centre explained how companies most of us have never heard of – data aggregators, data brokers, data analysts, and so on – are trading in our personal information. These companies often collect thousands of data points on individuals from various companies we deal with, and use them to provide information about us to companies and political parties.

Data companies have sorted consumers into lists on the basis of sensitive details about their lifestyles, personal politics and even medical conditions, as revealed by reports by the ACCC and the US Federal Trade Commission. Say you're a keen jogger, worried about your cholesterol, with broadly progressive political views and a particular interest in climate change – data companies know all this about you and much more besides.

So what, you might ask. If you've nothing to hide, you've nothing to lose, right? Not so. The more our personal information is collected, stored and disclosed to new parties, the more our risk of harm increases.

Potential harms include fraud and identity theft (suffered by 1 in 10 Australians); being charged higher retail prices, insurance premiums or interest rates on the basis of our online behaviour; and having our information combined with information from other sources to reveal intimate details about our health, financial status, relationships, political views, and even sexual activity.

In written testimony to the US House of Representatives, legal scholar Frank Pasquale explained that data brokers have created lists of sexual assault victims, people with sexually transmitted diseases, Alzheimer's, dementia, AIDS, sexual impotence or depression. There are also lists of "impulse buyers", and lists of people who are known to be susceptible to particular types of advertising.

## MAJOR UPGRADES TO AUSTRALIAN PRIVACY LAWS

According to the ACCC, Australia's privacy law is not protecting us from these harms, and falls well behind privacy protections consumers enjoy in comparable countries in the European Union, for example. This is bad for business too, because weak privacy protection undermines consumer trust.

Importantly, the ACCC's proposed changes wouldn't just apply to Google and Facebook, but to all companies governed by the *Privacy Act*, including retail and airline loyalty rewards schemes, media companies, and online marketplaces such as Amazon and eBay.

Australia's privacy legislation (and most privacy policies) only protect our "personal information". The ACCC says the definition of "personal information" needs to be clarified to include technical data like our IP addresses and device identifiers, which can be far more accurate in identifying us than our names or contact details.

Whereas some companies currently keep our information for long periods, the ACCC says we should have a right to request erasure to limit the risks of harm, including from major data breaches and reidentification of anonymised data.

Companies should stop pre-ticking boxes in favour of intrusive practices such as location tracking and profiling. Default settings should favour privacy.

Currently, there is no law against "serious invasions of privacy" in Australia, and the *Privacy Act* gives individuals no direct right of action. According to the ACCC, this should change. It also supports plans to increase maximum corporate penalties under the *Privacy Act* from A$2.1 million to A$10 million (or 10% of turnover or three times the benefit, whichever is larger).

## INCREASED DETERRENCE FROM CONSUMER PROTECTION LAWS

Our unfair contract terms law could be used to attack unfair terms imposed by privacy policies. The problem is, currently, this only means we can draw a line through unfair terms. The law should be amended to make unfair terms illegal and impose potential fines of A$10 million or more.

The ACCC also recommends Australia adopt a new law against "unfair trading practices", similar to those used in other countries to tackle corporate wrongdoing including inadequate data security and exploitative terms of use.

So far, the government has acknowledged that reforms are needed but has not committed to making the recommended changes. The government's 12-week consultation period on the recommendations ends on October 24, with submissions due by September 12.

**DISCLOSURE STATEMENT**

**Katharine Kemp receives funding from The Allens Hub for Technology, Law and Innovation. She is a Member of the Advisory Board of the Future of Finance Initiative in India, the Centre for Law, Markets and Regulation and the Australian Privacy Foundation.**

**Katharine Kemp is Senior Lecturer, Faculty of Law, UNSW, and Co-Leader, 'Data as a Source of Market Power' Research Stream of The Allens Hub for Technology, Law and Innovation, UNSW.**

THE CONVERSATION

Kemp, K (12 August 2019). *Here's how tech giants profit from invading our privacy, and how we can start taking it back.* Retrieved from http://theconversation.com on 18 June 2020.

# THE ACCC IS SUING GOOGLE OVER TRACKING USERS. HERE'S WHY IT MATTERS

**The government's consumer watchdog has been highly critical of how many large digital platforms use data, reports Katharine Kemp**

The Australian Competition and Consumer Commission (ACCC) today announced it is suing Google for misleading consumers about its collection and use of personal location data. The case is the consumer watchdog's first move against a major digital platform following the publication of the Digital Platforms Inquiry Final Report in July.

The ACCC follows regulators in countries including the US and Germany in taking action against the way "tech giants" such as Google and Facebook harvest and exploit their users' data.

## What did Google do?

ACCC Chair Rod Sims said Google "collected, kept and used highly sensitive and valuable personal information about consumers' location without them making an informed choice".

The ACCC alleges that Google breached the Australian Consumer Law (ACL) by misleading its users in the course of 2017 and 2018, including by:

- Not properly disclosing that two different settings needed to be switched off if consumers did not want Google to collect, keep and use their location data
- Not disclosing on those pages that personal location data could be used for a number of purposes unrelated to the consumer's use of Google services.

Some of the alleged breaches can carry penalties of up to A$10 million or 10% of annual turnover.

A spokesperson for Google is reported to have said the company is reviewing the allegations and engaging with the ACCC.

## Turning off "Location History" did not turn off location history

According to the ACCC, Google's account settings on Android phones and tablets would have led consumers to think changing a setting on the "Location History" page would stop Google from collecting, keeping and using their location data.

The ACCC says Google failed to make clear to consumers that they would actually need to change their choices on a separate setting titled "Web & App Activity" to prevent this location tracking.

## Location data is used for much more than Google Maps

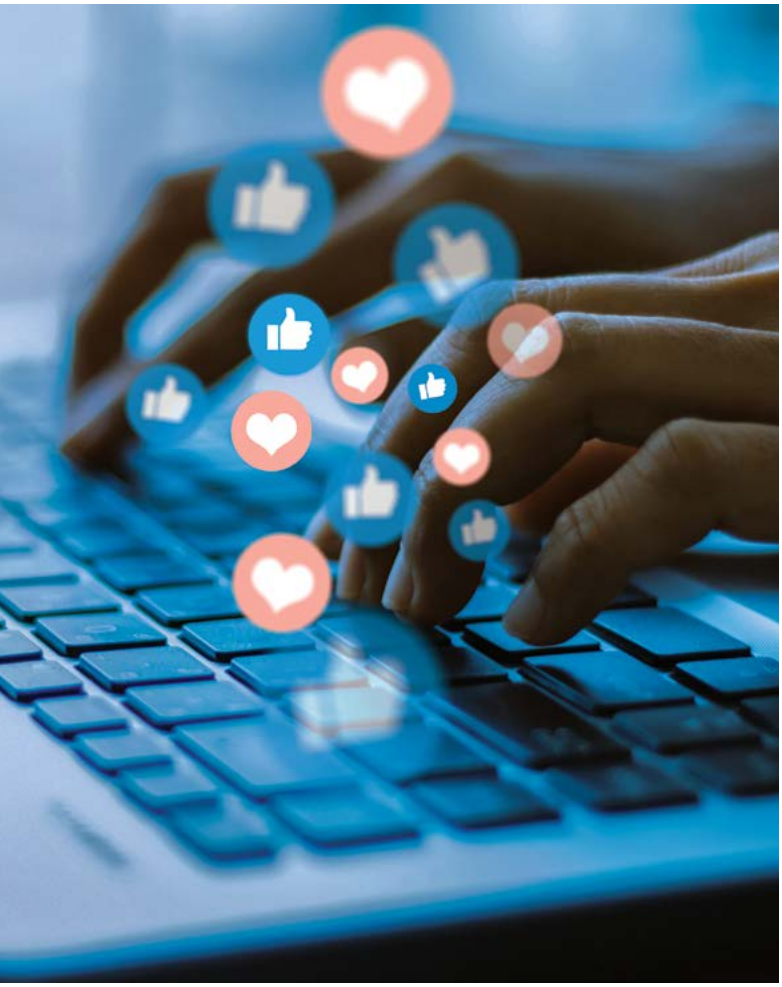
Google collects and uses consumers' personal location data for purposes other than providing Google services to consumers. For example, Google uses location data to work out demographic information, target advertising, and offer advertising services to other businesses.

Digital platforms increasingly track consumers online and offline to create highly detailed personal profiles on each of us. These profiles are then used to sell advertising services. These data practices create risks of criminal data breaches, discrimination, exclusion and manipulation.

### KEY POINTS

- The ACCC said Google's instructions on how to stop personal data being harvested were misleading.
- The allegations go to the heart of the tech giant's business model of using data unrelated to a consumer's use of Google services.
- The ACCC says it is a world-first action and it is seeking fines and compliance orders against Google in a crackdown on digital platform disclosures.

Digital platforms increasingly track consumers online and offline to create highly detailed personal profiles on each of us. These profiles are then used to sell advertising services. These data practices create risks of criminal data breaches, discrimination, exclusion and manipulation.



## Concealed data practices under fire around the world

The ACCC joins a number of other regulators and consumer organisations taking aim at the concealed data practices of the "tech giants".

This year, the Norwegian Consumer Council published a report – Deceived by Design – which analysed a sample of Google, Facebook and Microsoft Windows privacy settings. The conclusion: "service providers employ numerous tactics in order to nudge or push consumers toward sharing as much data as possible".

The report said some aspects of privacy policies can be seen as "dark patterns", or "features of interface design crafted to trick users into doing things that they might not want to do".

In Canada, an investigation into how Facebook gets consent for certain data practices by the Office of the Privacy Commissioner of Canada was highly critical.

It found that the relevant data use policy "contained blanket statements referencing potential disclosures of a broad range of personal information, to a broad range of individuals or organisations, for a broad range of purposes". The result was that Facebook users "had no way of truly knowing what personal information would be disclosed to which app and for what purposes".

## Is Facebook next?

The ACCC was highly critical of the data practices of a number of large digital platforms when the Final Report of the Digital Platforms Inquiry was published in July this year. The platforms included Facebook, WhatsApp, Twitter and Google.

The report was particularly scathing about privacy policies which were long, complex, difficult to navigate and low on real choices for consumers. In its words, certain common features of digital platforms' consent processes: leverage digital platforms' bargaining power and deepen information asymmetries, preventing consumers from providing meaningful consents to digital platforms' collection, use and disclosure of their user data.

The report also stated the ACCC was investigating whether various representations by Google and Facebook respectively would "raise issues under the ACL".

The investigations concerning Facebook related to representations concerning its sharing of user data with third parties and potential unfair contract terms. So far no proceedings against Facebook have been announced.

## Will this change anything?

While penalties of up to A$10 million or 10% of annual turnover (in Australia) may sound significant, last year Google made US$116 billion in advertising revenue globally.

In July, the US Federal Trade Commission settled with Facebook on a US$5 billion fine for repeatedly misleading users about the fact personal information could be accessed by third-party apps without the user's consent, if a user's Facebook "friend" gave consent. Facebook's share price went up after the FTC approved the settlement.

But this does not mean the ACCC's proceedings against Google are a pointless exercise. Aside from the impact on Google's reputation, these proceedings may highlight for consumers the difference between platforms which have incentives to hide data practices from consumers and other platforms – like the search engine DuckDuckGo – which offer privacy-respecting alternatives.

**DISCLOSURE STATEMENT**

**Katharine Kemp receives funding from The Allens Hub for Technology, Law and Innovation. She is a Member of the Advisory Board of the Future of Finance Initiative in India, the Centre for Law, Markets and Regulation and the Australian Privacy Foundation.**

**Katharine Kemp is Senior Lecturer, Faculty of Law, UNSW, and Co-Leader, 'Data as a Source of Market Power' Research Stream of The Allens Hub for Technology, Law and Innovation, UNSW.**

THE CONVERSATION

Kemp, K (29 October 2019). *The ACCC is suing Google over tracking users. Here's why it matters.* Retrieved from http://theconversation.com on 19 June 2020.

# Australia's privacy watchdog is taking Facebook to court. It's a good start

**Facebook and other online platforms are focused on extracting personal data at the expense of privacy. Consumers should hope this is only the first of many more actions by the privacy regulator, observe Katharine Kemp and Kayleen Manwaring**

On Monday, the Office of the Australian Information Commissioner (OAIC) brought proceedings against Facebook in the Federal Court, asking the court to impose financial penalties for serious interference with the privacy of more than 300,000 Australians. To our knowledge, this is the first time the privacy regulator has sought civil penalty orders under the *Privacy Act*.

Facebook responded by saying it had made "major changes" to its platforms "in consultation with international regulators". This response is none too comforting, given Facebook's current data practices (which include collecting data of consumers who have never used Facebook). The company also has a history of misrepresentations regarding data privacy.

## WHAT IS FACEBOOK BEING SUED FOR?

In 2014, Facebook users were offered an app called "This is Your Digital Life", which paid users to take a personality quiz. The app harvested the data not only of the person taking the quiz but also of their Facebook friends, who had no knowledge of the app or the data collection.

The app developer then sold that information to a political lobbying company, Cambridge Analytica, which used the personal data for political profiling. This profiling was apparently used to aid in the election of US President Donald Trump in 2016, among other things.

Worldwide, approximately 87 million Facebook users were affected. In Australia, only 53 users downloaded the app, but still, around 311,000 people were affected.

The OAIC alleges that Facebook contravened the *Privacy Act* by allowing users' personal data to be used for purposes that were not properly disclosed, and by failing to take proper steps to protect users' personal data.

## BETTER LATE THAN NEVER

The OAIC's action follows similar action against Facebook by regulators around the world. In 2018, the UK privacy regulator fined Facebook the maximum GBP 500,000 over the Cambridge Analytica breach. Last year, the US Federal Trade Commission (FTC) settled with Facebook on a record-breaking US$5 billion payment in respect of related conduct.

While the OAIC's action should be encouraged, we should not overestimate the impact on Facebook.

### KEY POINTS

- The information commissioner alleges Facebook committed "serious and/or repeated interferences" with privacy.
- The allegations relate to an app that shared data with notorious data analysis firm Cambridge Analytica.
- Facebook has already been fined in the UK, among other countries, over the data misuse scandal.


If the Federal Court finds the alleged contraventions occurred, Facebook could face fines of up to A$1.7 million for each contravention. (There is likely to be debate over what constitutes a single contravention, and therefore how many contraventions there were.) That may sound hefty, but we should put it in context. When the US$5 billion settlement with the FTC was announced last year, Facebook's share price went up. The settlement represented only about 7% of Facebook's 2019 revenue of more than US$70 billion.

## FACEBOOK IS STILL COLLECTING DATA ABOUT NON-FACEBOOK USERS

Facebook responded to this week's announcement of the OAIC action by saying it has upgraded privacy protections:

*We've made major changes to our platforms, in consultation with international regulators, to restrict the information available to app developers, implement new governance protocols and build industry-leading controls to help people protect and manage their data.*

But has the leopard changed its spots? While Facebook has made some adjustments to the settings available to Facebook users, it continues, for example, to track the activities of consumers on third-party websites, when a Facebook user is not logged in, and even when the consumer has never been a Facebook user.

Facebook says it collects information about anyone who visits a website or app that uses "Facebook Products", which includes anywhere you see Facebook "Like" buttons or an option to "sign in with Facebook". You don't need to click on the "Like" button or sign in with Facebook for this to happen. According to Facebook, it collects this information "without any further action from you".

Facebook does this by placing a cookie on your computer or device when you visit the third-party website. It then collects data about what you do online, including your use of other websites and apps, and information about your device, which can be highly individual.

As the Australian Competition and Consumer Commission pointed out last year, it's unlikely non-Facebook users could even find out about this practice.

## WHAT COULD THEY DO WITH OUR DATA?

According to its Cookie Policy, Facebook can broadly use this data to offer you products and to "understand the information we receive about you, including information about your use of other websites and apps, whether or not you are registered or logged in".

In 2018, Facebook told the US House of Representatives that it does "not use web browsing data to show ads to non-users or otherwise store profiles about non-users". However, its Cookie Policy does not reflect these claims, and it has not said it will stop collecting this data.

More than that, Facebook has in the past claimed it will limit data use, before going back on it later. When Facebook acquired WhatsApp in 2014, it told regulators it would be unable to automatically match Facebook and WhatsApp user accounts after the merger. The European Commission has since fined Facebook for making incorrect or misleading representations in this respect.

Similarly, the action brought by the US FTC referred to repeated misrepresentations by Facebook about the extent to which users could control the privacy of their data.

Facebook may have made some changes, but it is still an advertising business with a history of privacy infringements that makes tens of billions of dollars each quarter from collecting and monetising oceans of personal data.

Other companies are similarly focused on extracting personal data at the expense of privacy. Consumers should hope this is only the first of many more actions by the privacy regulator.

**DISCLOSURE STATEMENT**

**Katharine Kemp receives funding from The Allens Hub for Technology, Law and Innovation. She is a Member of the Advisory Board of the Future of Finance Initiative in India, the Centre for Law, Markets & Regulation and the Australian Privacy Foundation. Kayleen Manwaring has received funding from the International Association of Privacy Professionals. She is a member of The Allens Hub for Technology, Law and Innovation, the Centre for Law, Markets & Regulation and is NSW Co-ordinator for the IEEE Society for Social Implications of Technology (Australia Chapter).**

**Katharine Kemp is Senior Lecturer, Faculty of Law, UNSW, and Academic Lead, UNSW Grand Challenge on Trust, UNSW.**

**Kayleen Manwaring is Senior Lecturer, School of Taxation & Business Law, UNSW.**

THE CONVERSATION

Manwaring, K and Kemp, K (11 March 2020). *Australia's privacy watchdog is taking Facebook to court. It's a good start.* Retrieved from http://theconversation.com on 22 June 2020.

# PROPOSED PRIVACY LAW REFORMS

**In 2019, the Australian Competition and Consumer Commission produced a wide-reaching report on the operation of digital platforms in Australia, which included a review of Australia's privacy laws, offering numerous recommendations for change. In response, the Australian Government has accepted the need for reform and has announced that it will consider a number of significant changes to Australia's privacy laws, subject to further consultation and review.**

- 12 December 2019: the Australian Government released its response to the ACCC's Final Report for the Digital Platforms Inquiry.
- The Final Report made a number of recommendations across a range of policy areas, much of which related to changes to Australia's privacy laws and strengthening consumer protection. The recommendations were largely across the economy; only one recommendation was specific to digital platforms.
- The Australian Government accepted the need for privacy reform and largely supported the ACCC's recommendations in relation to reforming privacy and data regulations.

- The government has stated that it will look to strengthen consumer protection under Australia's *Privacy Act 1988 (Cth) (Privacy Act)* by:
  - ***Increasing penalties:*** Increasing the penalties for breaches of the *Privacy Act* to the greater of (i) $10 million AUD, (ii) three times the value of the benefit obtained through the misuse of information or (iii) 10% of the company's annual turnover.
  - ***Definition of personal information:*** Amending the definition of personal information to capture technical data and other online identifiers (e.g. IP addresses, device identifiers, location data and any other online identifiers).
  - ***Strengthening existing notice and consent requirements:*** For example, by requiring collection notices to be concise, transparent, intelligible and easily accessible, written in clear and plain language, and provided free of charge.
  - ***Introducing direct right of action:*** Providing individuals with a direct right to bring actions to seek compensation for interferences with their privacy.
  - ***Binding code:*** Developing a binding privacy code applicable to social media and other online platforms trading in personal information.

- The Government indicated that consultation and the subsequent introduction of draft legislation to Parliament to address the above reforms will occur in 2020 (*Note: this was stated before the coronavirus pandemic, which has subsequently delayed most government legislative business*).
- The Government has also stated that it will undertake a comprehensive review of the *Privacy Act* in 2020, to be completed by 2021, which it has flagged will include consideration of the introduction of the right of erasure of personal information and a statutory tort for serious invasions of privacy.
- The Government's response indicates that Australia's privacy landscape is set to significantly change over the coming years. However, it also appears that there will be considerable opportunity for stakeholders to engage with government and regulators on the substance and form of these proposed changes.

**SOURCES**

Corrs Chambers Wesgarth (4 March 2020). *Widespread changes to privacy laws set to follow ACCC Digital Platforms Inquiry final report*.
PricewaterhouseCoopers Legal (April 2020), *2020 Australian Privacy Outlook*.

**Compiled by The Spinney Press.**

# RIGHT TO PRIVACY AND FREEDOM FROM SURVEILLANCE

## LIBERTY VICTORIA BELIEVES AUSTRALIA SHOULD MEET ITS INTERNATIONAL OBLIGATIONS AND LEGISLATE FOR A GENERAL RIGHT TO PRIVACY

The right to privacy is the right to be free from undue surveillance by government or anyone else. Surveillance by the state should only occur if absolutely necessary and where authorised by an independent judicial officer. Personal information should only be collected and kept by the state and anyone else for a legitimate purpose authorised by law.

Australia's privacy laws have expanded in recent years, but are still fundamentally flawed. They lack uniformity, they fail to recognise a right to privacy and they do not apply generally to individuals or small businesses.

Once collected, personal information should be destroyed as soon as it is no longer required. Not only would this protect privacy, it would also improve security. If personal information is only collected when absolutely necessary, it is less likely to fall into the wrong hands. If it is destroyed when it is no longer required, it is less likely to become incorrect and out of date.

Australia's privacy laws have expanded in recent years, but are still fundamentally flawed. They lack uniformity, they fail to recognise a right to privacy and they do not apply generally to individuals or small businesses. This means that private individuals and small businesses are largely unregulated when it comes to the collection and use of personal information about other people.

The spread of new technologies such as CCTV and GPS presents new threats to privacy which have outpaced the law.

The majority of democratic countries have recognised that privacy is a fundamental human right which needs to be protected. Article 17 of the ICCPR recognises privacy as a basic human right, but Australia, despite being a signatory to the ICCPR, does not recognise privacy as an actionable human right.

Liberty believes Australia should meet its international obligations and legislate for a general right to privacy. An actionable right to privacy would enable individuals to take action against the inappropriate and illegal collection, use or disclosure of their personal information. It would not prevent the lawful collection and use of personal information for legitimate purposes.

The spread of new technologies such as CCTV and GPS presents new threats to privacy which have outpaced the law. It is futile to try to stop the spread of many of these technologies. However, the legal environment in which they spread should discourage the misuse of personal information.

The most effective deterrent to the misuse of personal information would be a liability to compensate people whose privacy has been compromised for no legitimate purpose. The right to privacy is associated with the rights to freedom of speech, freedom of movement, freedom from discrimination and the principle of government accountability.

---

Liberty Victoria. *Right to privacy and freedom from surveillance.* Retrieved from http://libertyvictoria.org.au on 18 June 2020.

# YOUR PRIVACY RIGHTS: SURVEILLANCE AND MONITORING

**There are some situations where your personal information, including your image or identity information, is legally allowed or required to be collected, explains the Office of the Australian Information Commissioner**

## SECURITY CAMERAS

An organisation or agency that uses a surveillance device, such as a security camera or CCTV, generally must follow several laws. If the *Privacy Act 1988 (Privacy Act)* covers the organisation or agency, then any personal information they collect through a surveillance device must comply with the Australian Privacy Principles. The *Privacy Act* covers Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations.

Such an organisation or agency must:

- Tell you that your image may be captured before you're recorded
- Make sure recorded personal information is secure and destroyed or de-identified when it is no longer needed.

State and territory surveillance and monitoring laws also cover surveillance devices. For more information, contact the Attorney-General's Department in your state or territory.

### *Residential security cameras*

If your neighbour has a security camera pointed at your house and you're worried about your privacy, first try to talk to your neighbour. If this doesn't fix the problem, you could ask your local community justice or neighbourhood mediation centre for help (*see the table above*).

The *Privacy Act* doesn't cover a security camera operated by an individual acting in a private capacity but state or territory laws may apply. For more information, contact the Attorney-General's Department in your state or territory. However, if you're concerned about your safety, contact the police.

You could also contact your local council to find out if the practice contravenes any local laws. Some councils require planning permission for security cameras. If your property is part of a strata title, check the by-laws to see if they cover installing or using security cameras.

## DRONES

Several laws cover the use of drones in Australia. If you've been photographed or filmed by a drone and the operator is an organisation or agency the *Privacy Act 1988 (Privacy Act)* covers, then they must comply with the Australian Privacy Principles. The *Privacy Act* covers Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations.

Such an organisation or agency must:

- Tell you that your image may be captured before you're recorded
- Make sure recorded personal information is secure and destroyed or de-identified when it is no longer needed.

The *Privacy Act* does not apply to individuals acting in a private capacity. Civil Aviation Services Australia regulates the use of recreational drones. Visit their website (www.casa.gov.au) for a list of rules an individual must follow when operating a drone.

If your neighbour is using a drone and you're concerned about your privacy, see *Security Cameras* www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/security-cameras/#ResidentialSecurityCamera.

If a media or news outlet has used a drone to capture your image without permission, see *Photos and Videos at* www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/photos.

### HELP HANDLING A DISPUTE

| If you live in | Contact |
|---|---|
| Australian Capital Territory | Conflict Resolution Service Phone: 02 6162 4050 |
| New South Wales | Community Justice Centres Attorney-General's Department Phone: 1800 990 777 |
| Northern Territory | Community Justice Centre Department of Justice Phone: 1800 000 473 |
| Queensland | Dispute Resolution Branch Department of Justice and Attorney-General Phone: 07 3239 6007 |
| South Australia | Uniting Communities Mediation Service Phone: 08 8342 1800 |
| Tasmania | Department of Justice Phone: 03 6173 0210 |
| Victoria | Dispute Settlement Centre Department of Justice Phone: 1800 658 528 |
| Western Australia | Legal Aid Western Australia Phone: 1300 650 579 |

## ID SCANNING

When an organisation or agency takes an electronic copy of a document that proves your identity, such as your driver licence, this is called ID scanning.

If the organisation or agency doing the ID scanning is an organisation or agency that the *Privacy Act 1988* (*Privacy Act*) covers, then they must comply with the Australian Privacy Principles when collecting your personal information. The *Privacy Act* covers Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations.

If the organisation or agency is not covered by the *Privacy Act*, state or territory privacy laws may cover ID scanning. Such organisations or agencies include state or territory public sector agencies, local councils and universities.

### *When can your ID be scanned?*

An organisation or agency may only scan your identity documents (ID) if it's reasonably necessary for their business activities. If your ID contains sensitive information you must also consent to the scanning.

In some situations, the law may authorise or require an organisation to scan your ID. For example, liquor licensing or anti-money laundering laws may require an organisation to ask for your ID before they can give you information or supply a service.

### *What information on your ID can be scanned?*

An organisation or agency may only collect information from your ID that is reasonably necessary for one or more of their functions or activities.

For example, an organisation or agency can only scan the government-related identifier (such as a driver licence number, a Centrelink reference number, a Medicare number or a passport number) on your ID if it's reasonably necessary to prove your identity.

An organisation or agency can't collect more information than is reasonably necessary because it's convenient or they think it might be useful in the future. For example, they shouldn't scan your ID if sighting it would be sufficient.

### *What you must be told before your ID is scanned*

An organisation or agency must take reasonable steps to tell you why they need to scan your ID and what will happen if you don't consent to them to scanning your ID. This information must be easily available and done in a lawful and fair way.

For more information, see *Collection of Personal Information* at www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/collection-of-personal-information/#MakeSureKnow.

### *How is your scanned information protected?*

An organisation or agency that the *Privacy Act* covers must take reasonable steps to protect your scanned information from misuse, interference, loss, unauthorised access, modification and disclosure. The information must also be destroyed or de-identified once it is no longer needed.

For more information, see *Guide to Securing Personal Information* www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information.

You may also want to read the organisation or agency's privacy policy. It should explain:

- What information is scanned
- How the scanned information is kept secure
- How long the scanned information is kept
- How the scanned information will be destroyed or de-identified.

### *If you think your scanned information has been mishandled*

If you think your scanned information has been mishandled by an organisation or agency covered by the *Privacy Act*, contact them to lodge a complaint.

If you're not happy with an organisation or agency's response, you can lodge a complaint with us (www.oaic.gov.au/privacy/privacy-complaints).

## BIOMETRIC SCANNING

Biometric information scanning is when an organisation or agency takes an electronic copy of your biometric information, which includes any features of your:

- Face
- Fingerprints
- Iris
- Palm
- Signature
- Voice.

An organisation or agency may only scan your biometric information as a way to identify you or as part of an automated biometric verification system, if the law authorises or requires them to collect it or it's necessary to prevent a serious threat to the life, health or safety of any individual.

Under the *Privacy Act 1988* (*Privacy Act*) your biometric information is sensitive information. This means that if the *Privacy Act* covers the organisation or agency collecting it then they must first ask for your consent, with some exceptions, and also make sure it has a high level of privacy protection. The *Privacy Act* covers Australian Government agencies and any organisation with an annual turnover of more than $3 million, and some other organisations.

### *If you think your scanned information has been mishandled*

If you think your scanned information has been mishandled by an organisation or agency covered by the *Privacy Act*, contact them to lodge a complaint.

If you're not happy with an organisation or agency's response, you can lodge a complaint with us (www.oaic.gov.au/privacy/privacy-complaints).

Office of the Australian Information Commissioner. *Surveillance and monitoring.* Retrieved from www.oaic.gov.au on 19 June 2020.

# Australians are increasingly concerned about expansion of surveillance powers

***Polling commissioned by Digital Rights Watch shows that Australians have a high level of concern over legislation that has made it easier for the government and law enforcement agencies to access their private personal digital information***

The polling, commissioned by Digital Rights Watch and undertaken by Essential Research, has revealed:

- 76% of people expressed concern that telecommunication companies retain data on every Australian
- 71% had concerns that law enforcement agencies have the power to break into encrypted communications systems
- 74% of people are concerned about the recent raids by Australian Federal Police on the homes and offices of journalists who reported on national security issues.

"We know that people are concerned about the raft of powers that have been given to law enforcement over the past few years. There is a glaring lack of transparency and oversight over how these powers are used," said Tim Singleton Norton, Chair of Digital Rights Watch.

"In the last year alone, government agencies made more than 300,000 requests for metadata, with only 5 of these requests being refused. That's a huge disparity, and one that points to what we've known all along – for the government to suggest this is anything other than blanket surveillance of the Australian population is ridiculous."

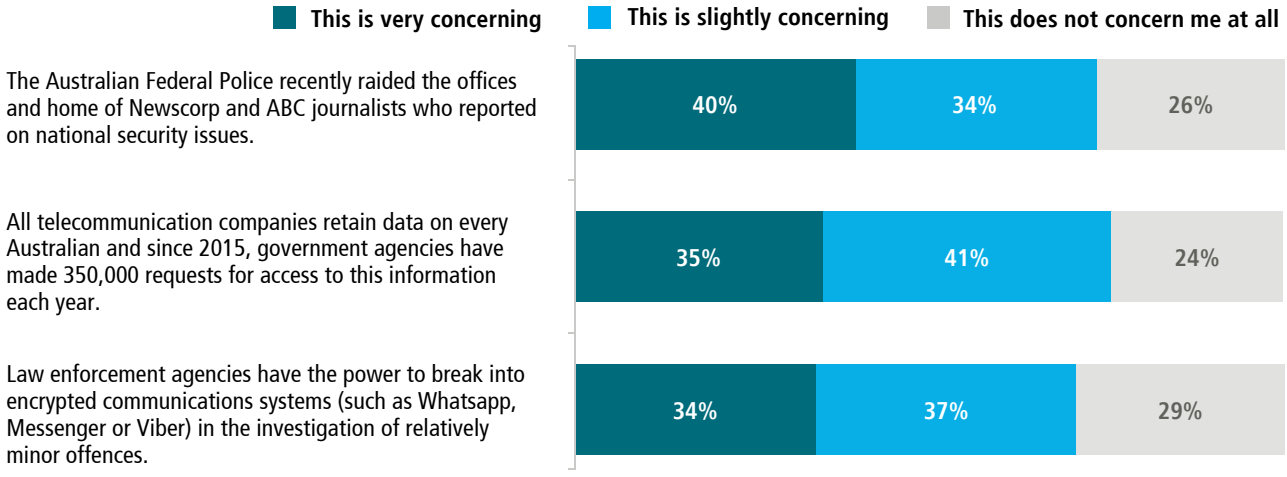
"The recent Commonwealth Ombudsman's report has revealed the true extent of metadata requests across the country and the complete lack of due process from law enforcement agencies. A huge number of requests for access to metadata were completely unauthorised and unwarranted – and the public are right to be concerned about this."

"The passage of encryption-breaking powers last year was a complete debacle, and caused a great amount of distrust in the political system – which this polling is showing loud and clear. The majority of Australians are not at all comfortable with the scope and implementation of these powers, and they have every right to feel this way," he concluded.

Digital Rights Watch (25 June 2019). *Australians are increasingly concerned about expansion of surveillance powers.* Retrieved from http://digitalrightswatch.org.au on 22 June 2020.

## CONCERN DUE TO CHANGES IN ACCESS TO DIGITAL INFORMATION LEGISLATION

Q. In recent years, changes to legislation has made it easier for the government and law enforcement agencies to access digital information of individuals in the interest of national security. To what extent are you concerned with the following implications of these changes?



# AUSTRALIANS ACCEPT GOVERNMENT SURVEILLANCE, FOR NOW

## AUSTRALIANS ARE SUBJECT TO INCREASING LEVELS OF SURVEILLANCE BY THE GOVERNMENT, EXPLAIN ANNA BUNN AND NIK THOMPSON

**Australians tend to accept government surveillance, particularly if they think it necessary or trust the government, according to a recent study.**

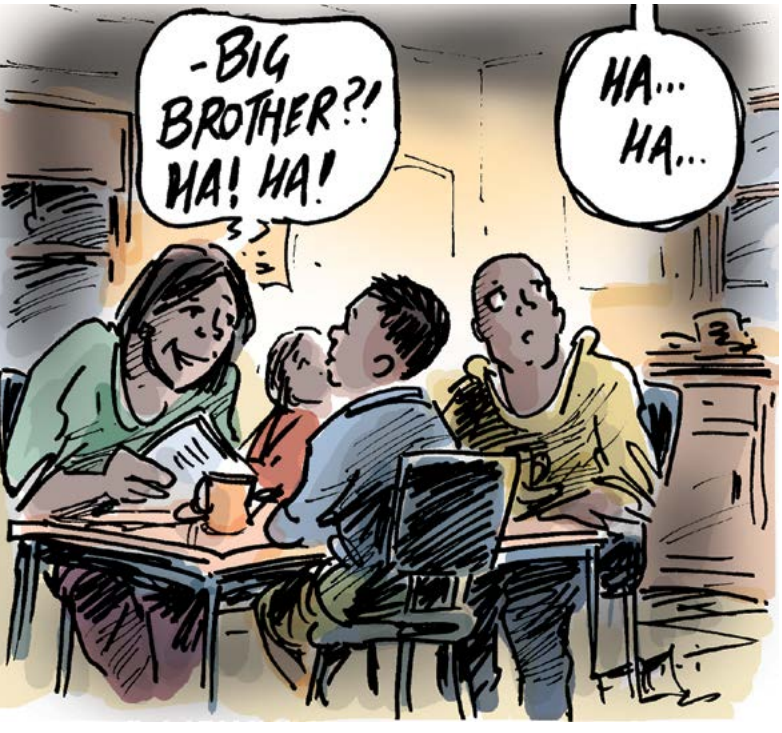
But they're only lukewarm about it. So if such surveillance continues to increase, people might reach a turning point and adopt some basic measures to "hide" themselves.

Australians are subject to ever-increasing levels of government surveillance. It is generally justified as necessary to protect us from criminal or terrorist activities. Under certain circumstances, various intelligence agencies, as well as federal and state police, can request access to your telephone and internet records. This can reveal information about your location and who you talked to, emailed or messaged.

Proposed legislation would allow the Department of Home Affairs to share photographs and other identifying information "between government agencies and, in some cases, private organisations". Not only can this information be shared for reasons of national security, it can also be used for general law enforcement, and even road safety.

The government recently passed the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, which allows government agencies greater access to encrypted messages, like those sent over WhatsApp.

Technology companies and civil society groups say they are concerned and can't believe these increased powers. But what about the public? Although Australians have generally accepted the collection of telecommunications metadata or driver licence photos, little is known about the factors that influence their acceptance of government surveillance.




### MILD ACCEPTANCE

Our research aimed to address this by surveying 100 Australian residents about their views on government surveillance. Just more than half (52) said they accept government surveillance.

The overall strength of acceptance tells a similar story. On a scale from 1 (strongly reject) to 5 (strongly accept) the average response was 3.1. This shows respondents are on the fence, but leaning slightly towards acceptance. Two main factors influenced acceptance of surveillance.

#### 1. *Is surveillance needed?*

The most influential factor was if they thought the surveillance necessary. This has practical implications as lawmakers capitalise on people's emotional responses to tragic events to justify new legislation, particularly around the time these events occur. For instance, in the six years after 9/11, the Howard government pushed through a new anti-terror statute every 6.7 weeks on average.

More recently, Australia's attorney-general mentioned the recent terrorist attack in Melbourne to garner support for the new encryption laws:

*The need for the powers in this bill has become more urgent in the light of the recent fatal terrorist attack in Melbourne and the subsequent disruption of alleged planning for a mass casualty attack by three individuals last month – also, sadly, in Melbourne. Individuals in both of these cases are known to have used encrypted communications.*

#### 2. *Do I trust the government?*

People's overall trust in the government also strongly determined their acceptance of surveillance. This is interesting given trust in the Australian government is generally relatively low.

People might be more influenced by their general view of the government than their views of specific policies and practices. If so, events that diminish that trust may also threaten the acceptance of surveillance policies. This is something for politicians to consider before calling for the next leadership spill.

As expected, the research also showed, that on average, people didn't particularly trust the government to

# SURVEILLANCE CAPITALISM AND SMART HOME DEVICES

**Are our appliances spying on us? Just don't ask Alexa or Siri for the answer, unless you are happy to share more of your personal behavioural data to large corporations**

*Surveillance capitalism* refers to an economic system centred around the commodification of personal data with the core purpose of profit-making. Since personal data can be commodified it has become one of the most valuable resources on Earth. The concept of surveillance capitalism arose as advertising companies, led by Google's AdWords, saw the possibilities of using personal data to target consumers more precisely.

The Internet of Things (IoT) is a key component of home automation and smart homes, connecting computers, smartphones and everyday home appliances including clocks, speakers, lights, doorbells, cameras, window blinds, hot water heaters, cooking utensils, etc. These appliances can all communicate, send information, and take commands.

When you speak to a voice-controlled internet-connected gadget like your virtual home assistant – including Amazon Alexa speaker device, Google Assistant speaking through its Home devices, and Apple's Siri delivered through HomePod – staff may be listening in. Although these firms claim that they carefully guard the privacy of customers, it is noteworthy that these occasional human intercepts are in addition to the computerised monitoring and data extraction applied to *all* of these conversations.

The primary reason these digital assistants exist is not to assist you, but rather to make money for Amazon, Google and Apple. Every clue you give your device is seized and processed by these corporations; while some interactions are used to refine the service on offer, the rest are fed into machine intelligence software and fabricated into prediction products that anticipate what you will do now, soon and later. These data-driven products are then traded in a sort of marketplace for behavioural predictions. End consumers will never know exactly who is buying what in this marketplace, or how it will be used to shape their buying behaviour.


**SOURCES**

Wikipedia, *Surveillance capitalism*, retrieved from https://en.wikipedia.org/wiki/Surveillance_capitalism on 22 September 2020.

Hartcher, P, 'Welcome to the age of surveillance capitalism', *The Sydney Morning Herald* (16 April 2019).


**Compiled by The Spinney Press.**

manage data. The large number of people choosing to opt out of My Health Record tells us people are concerned about how their information is managed.

Yet, surprisingly, there was no link between people's level of trust in the way the government manages data and their acceptance of surveillance.

Perhaps people feel they have nothing to hide, or believe the broader benefits of surveillance outweigh the risks.

## CAUSE FOR CONCERN

Given the vast amounts of information gathered through surveillance, it might seem reasonable to assume that individuals will never be scrutinised unless they raise suspicion (one hopes, reasonably).

However, improvement in data-processing capabilities means this is not necessarily true. For example, artificial intelligence can analyse CCTV video footage without human input.

And when face recognition is used to identify suspects, there are often multiple records of images of people who are a close match to the suspect. This can result in a high error rate, posing a risk that innocent people are accused of criminality and wrongdoing.

But perhaps more worrying is the threat of repurposing – when information collected for one purpose is used for another. For example, concerns that insurance companies could access and use information from My Health Record led to the government amending legislation to prevent this.

But, unlike My Health Record data, surveillance data collection is indiscriminate and has no "opt out". Consider the two years' worth of communications metadata currently stored for the entire nation, which is accessible to many agencies without a warrant. It's not certain how this data might be reused in the future.

## WHAT NEXT?

The Law Council of Australia says:

*It is unacceptable to assume the majority of Australians, who are not criminals and have the expectation to be kept safe by the state, are willing to succumb to heightened surveillance.*

However, our findings suggest, at least for now, Australians generally accept government surveillance, albeit relatively weakly. This means that if surveillance continues to increase, people may try to "hide" themselves.

This might be by using virtual private networks (VPNs), privacy protection sufficient to prevent the government from collecting your online metadata.


**DISCLOSURE STATEMENT**

**The authors do not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and have disclosed no relevant affiliations beyond their academic appointment.**



**Anna Bunn is Senior Lecturer, Curtin Law School, Curtin University.**

**Nik Thompson is Senior Lecturer, Curtin University.**


THE CONVERSATION


Bunn, A and Thompson, N (5 February 2019). *Australians accept government surveillance, for now.* Retrieved from http://theconversation.com on 19 June 2020.

# A 'pandemic drone' and other technology could help limit the spread of coronavirus and ease restrictions sooner, but at what cost?

**According to this ABC News report by Nadia Daly, a pandemic drone can be used to track temperatures, fever and social distancing**

If you don't feel comfortable signing up to the government's COVIDSafe tracking app, then you probably won't be happy to hear about the pandemic drone. Software being developed at the University of South Australia in conjunction with Canadian drone manufacturer Draganfly could see drones used to monitor the health of people, including spotting sneezes and tracking whether they have a fever.

It is just one way technology could be used to track and slow the spread of a virus like COVID-19. But experts warn that new surveillance technologies must include privacy safeguards before they are adopted.

### HEART RATE CAN BE DETECTED WITHIN 8 METRES

Professor Javaan Chahl, who holds positions with the University of South Australia and the Department of Defence, is developing software for the pandemic drone. The device uses thermal cameras and artificial intelligence to measure some of the indicators of coronavirus in groups of people: heart rate, body temperature, coughing and sneezing.

"Heart rate can be measured in two different ways," he told *7.30*.

"From a drone, we normally would measure it by a subtle change in skin tone that's associated with each heartbeat.

"And it's caused by changing the volume of blood in the skin. It also causes slight movement."

The drone would also be able to detect a cough from "15-20 metres away", while heart rate can be detected within 6-8 metres with only a "very small" margin of error. It could also be used to monitor social distancing.

While still six months from completion, Professor Chahl hoped it would be used to collect data on a large scale and track patterns of behaviour to paint a broad picture of the spread of COVID-19 in a city, rather than monitor individuals.

"When you look at thousands of people, or millions of people, you'll start to see a trend," he said.

"And I think we don't have systems in place to surveil for that, particularly.

"It would be very useful to know how many people are suffering from symptoms associated with respiratory distress.

"So, if you see a lot of people coughing and sneezing and with elevated heart rates and breathing rates and fever, okay, that's good to know.

**KEY POINTS**

- New technology is making mass tracking of people and their health easier.
- A pandemic drone can pick up heart rate, body temperature and monitor social distancing.
- But the technology is also increasing concerns about privacy and data collection.

"And if that's increasing, that's very important to know."

### CONCERNS ABOUT 'BIG BROTHER SURVEILLANCE'

Professor Chahl does acknowledge the technology could also be used to watch and target individuals if a future user wanted to.

"All such technologies carry a risk with them," he said.

"I might think it's a very bad idea to use drones to chase people around who might be sick. But perhaps others might have different ideas.

"And it's very hard to restrain them from using it like that once the genie is out of the bottle."

Police in the US city of Westport, an hour north of New York, were trialling the software along with Draganfly, but pulled out last week over privacy concerns.

"There's a lot of discussion going on at the moment about how we manage that privacy so that you don't take away people's freedom, or start imposing on them unnecessarily," Professor Chahl said.

"But you do want to watch for the presence of this infectious disease. So there's a lot of challenges."

Artificial intelligence expert Professor Toby Walsh urged a cautious approach towards adopting technologies like the pandemic drone.

"I think the devil is in the detail: how it's rolled out, what safeguards are put in place," he said.

"There's every reason that this technology could be a useful tool in our armoury with rolling back the restrictions and allowing people to go about somewhat more normal lives.

"But, equally, there are concerns that you'd have about people's privacy and about whether when normality has returned, that we are not finding ourselves in a 'Big Brother' surveillance state."

### SURVEILLANCE TECH ALREADY USED OVERSEAS

Several places in east Asia, including Hong Kong, Taiwan and South Korea, have taken a more technology-driven approach to fighting coronavirus, successfully slowing the rate of transmission without enforcing the same strict lockdowns seen in Australia and some European countries, and keeping shops and restaurants open.

Everyone who lands in Hong Kong must download a mandatory phone app and wear a wristband for two weeks while in compulsory quarantine. The app and wristband work together to track the user's whereabouts, along with regular video calls from health officials.

Professor Walsh doubts that level of surveillance would go down well in Australia.

"These are extraordinary times, but I think those are extraordinary measures that I suspect most people in Australia would find too much down the road to taking us to what [authors] George Orwell, Huxley and other people have warned us about the surveillance state that we could be in," Professor Walsh said.

Another distinct feature of Hong Kong's tech-driven approach to tackling the virus is the routine use of temperature checks, which are a common sight at the entrance to restaurants, offices, shopping malls and government buildings across the city.

## FEVER SCANNING

Australian entrepreneur Rustom Kanga hopes that temperature-taking technology will soon be more widespread here. His company iOmniscient has developed an automated fever scanning system which can operate through CCTV cameras to check the temperatures of people in crowds. He claimed it was accurate "to about 0.2 of a degree Celsius".

"Now and in the future, we will be releasing the lockdown, there'll be lesser restrictions," he told *7.30*.

"And in those environments we are going to still have to keep track of everyone.

"We are going to have to monitor people to make sure that there is no one around with a fever, because the fever is the first external indication, usually, of an infection of the coronavirus."

Dr Kanga said the software used artificial intelligence, including facial recognition, to automatically read the body temperature of "hundreds of people" at once in a crowd and alert authorities if someone had a fever. The system could then track them through a network of cameras until they could be identified by a staff member or official.

"It uses what is called a thermographic camera, which is a camera that can detect the heat of things in the environment," he said.

"In this case, it's detecting the temperature of a person's skin."

Dr Kanga believed the technology could be useful in places where people are still gathering in groups such as schools, pharmacies, shops, defence facilities, hospitals and prisons.

"Today there is no real checking in public areas of whether people have fevers," he said.

"A system like this will give them an early indication that there's someone who potentially has a fever."

## WE WON'T BE ABLE TO 'GO BACK TO OUR NORMAL LIVES'

The use of facial recognition technology is highly controversial and concerns have long been raised by civil liberties groups about its use in public spaces and about the potential for authorities to use it to track citizens. But Dr Kanga said his software "anonymised" faces by default and people would only be identified when requested by the user.

The use of facial recognition technology is highly controversial and concerns have long been raised by civil liberties groups about its use in public spaces and about the potential for authorities to use it to track citizens.

"Everyone's face can be redacted so that nobody sees anything," he said.

"However, if there's a person with a fever, that person's image is sent to the smartphone or the paramedic so that he can be checked out."

Professor Walsh said technologies like this could be part of Australia's approach, but won't replace the need for social distancing.

"It's worth pointing out those modern technologies are not going to be a panacea," he said.

"They're not going to allow us to go back to our normal lives, we are still going to have to social distance, we are still going to have to keep ourselves isolated physically as much as possible from each other until we have a vaccine.

"And, until that point, our lives are going to be somewhat on hold."



Daly, N (1 May 2020). 'A 'pandemic drone' and other technology could help limit the spread of coronavirus and ease restrictions sooner, but at what cost?', *ABC News*. Retrieved from www.abc.net.au/news on 22 June 2020.

# THE DANGER OF SURVEILLANCE TECH POST COVID-19

**Facial recognition is one tool in the fight against COVID-19, but once the pandemic ends, is surveillance technology going to stick around as part of the 'new normal'?**
**By Dr Niels Wouters and Dr Ryan Kelly**

Unlike the early 1900s during the Spanish Flu outbreak, the world can now fight COVID-19 with an unprecedented arsenal of medical, scientific, economic and social tools. But as governments move to leverage technology to fight COVID-19, we should be mindful that this scramble could open the door to technologies that will impact society in ways that are more profound and far-reaching than the pandemic itself.

Consider the use of facial recognition technologies. These are systems that scan images and videos for people's faces, and either attempt to classify them or make assessments of their character.

Some of the world's leading technology and surveillance companies have recently released new facial recognition tools that – with a high degree of accuracy – claim to be able to identify people even when they are wearing masks.

Similarly, thermal imaging equipment is being proposed to identify potential COVID-19 carriers by tracking the temperature of their face. In fact, London Heathrow Airport has just announced it will use the technology to carry out large-scale passenger temperature checks.

This capability is increasingly being retrofitted into ubiquitous CCTV systems. China, Russia, India and South Korea are notorious leaders in this space.

Some authorities are now able to identify patients with an elevated temperature, revisit their location history through automated analyses of CCTV footage, and automatically identify (and notify) those who may have been exposed to the pathogen.

And, yes, some of these are positive moves in an effort to rid societies of COVID-19. It is challenging to argue that this in itself is not a noble cause.

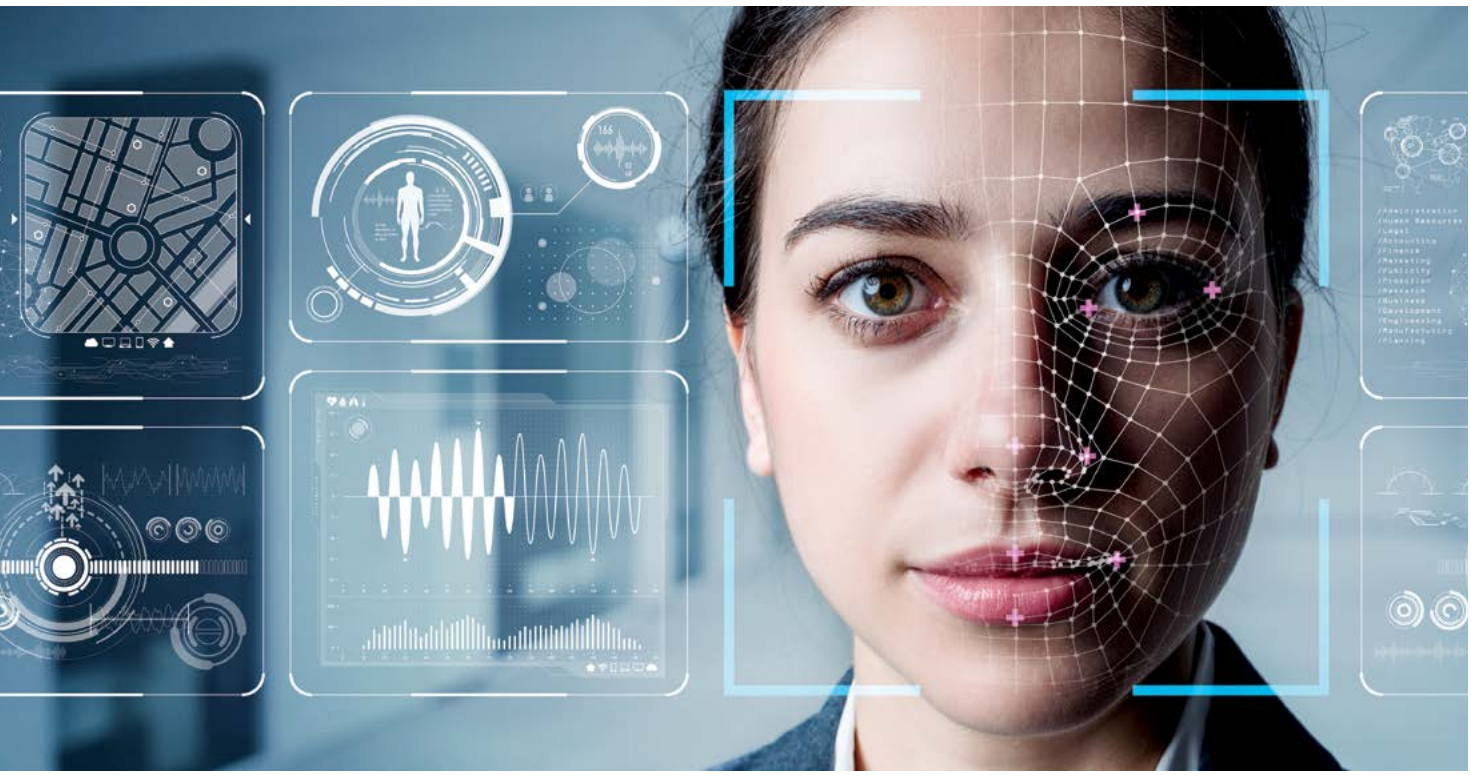
Indeed, the enormous uptake of contact tracing applications around the world is a sign that many of us seem willing to surrender some of our privacy in order to curb the spread.

But a real concern is the unanswered legal, constitutional and democratic questions that these apps introduce.

So, let's pause for a minute, because now is the right time to question these technologies, review some historical precedents and think about what the 'new normal' may be when the world attempts to return to its former state.

## FALSE POSITIVES AND DISCRIMINATION

Most of these new facial recognition tools ignore the significant risk for discrimination and persecution, the possibility of false positives or negatives and general



inaccuracy of the technology due to insufficient testing.

Picture the consequences of an automated system falsely identifying you as someone with an elevated body temperature, just as you return from a weekly grocery run.

These false positives are not unlikely. Infrared imaging equipment may be broken or used incorrectly, readings can be misinterpreted by a human reviewer or – even worse – by an automated process over which you have no control.

When facial recognition is involved, false positives are even more likely as datasets may have been too small to begin with or haphazardly developed.

In most democratic nations, these occurrences may 'only' lead to a benign outcome like compulsory self-quarantine, but other governments may decide to publicly shame those that have violated rules or limit their freedom to move.

## WE'VE BEEN HERE BEFORE

The application of facial recognition systems to fight COVID-19 adds another blot to the CV of this technology. Recent examples that have been widely criticised include systems that use facial images to distinguish sexual preferences, identify a person's ethnic group and spot academics in a crowd.

Studies emphasise that the practice of classifying humans based on visible differences has a troubled past with roots in eugenics – a movement or philosophy that believes things like selective breeding can improve the genetic composition of the human race.

It's a belief that has resulted in numerous examples of oppression in the past.

The practice of 'reading' human portraits began under Swiss minister Johann Kaspar Lavater in the late-1700s and English scientist Sir Francis Galton in the mid-1800s. Championing eugenics, Galton put in motion a global movement to quantify facial characteristics as indicators of a person's psychology.

But the early 1900s saw a new, worrying twist. During an already unsettled time in Europe, Italian criminologist Cesare Lombroso proposed pre-screening and isolation of people with "disciplinary shortcomings" to be enshrined in law. Physiognomy, the practice of presuming mental character from facial appearance, was now mainstream. Only a few decades later physiognomic thought proved influential in the rise of Nazi Germany.

These ideas from the past have proven to be remarkably tenacious. They reappeared in a now-withdrawn 2016 article on using artificial intelligence (AI) to distinguish criminal faces from noncriminal faces. Even in 2020, a recent article inspired by Lombroso's work claimed that it was possible to determine criminal tendency by analysing the shape of a person's face, eyebrows, top of the eye, pupils, nostrils, and lips in a dataset of 5,000 greyscale 'poker faces'.

And suddenly, it seems we're back in 18th century Europe.

## MAKE FACIAL RECOGNITION GREAT AGAIN?

More than ever, the COVID-19 pandemic illustrates that we're at a crossroads. Technologies are being developed and used to fight an invisible enemy and counteract the spread of a terrible disease; but we're also at risk of irreversibly releasing oppressive systems onto society that are not in the best interest of public life.

*When the COVID-19 pandemic ends, we must be mindful of the type of future society we want to live in. Do we want our old one back, or do we want a new one where widespread surveillance is the norm in the name of public health?*

The team at the Interaction Design Lab developed Biometric Mirror, a speculative and deliberately controversial facial recognition technology designed to get people thinking about the ethics of new technologies and AI.

Thousands of people tried our application, from schools to the World Economic Forum and World Bank, as well as the Science Gallery Melbourne and NGV.

What we found is that there is no widespread public understanding of the way facial recognition technology works, what its limitations are and how it can be misused.

This is worrying.

The Australian Government's 2018 commitment to support the delivery of artificial intelligence programs in schools is a welcome response. As young people face growing needs to be technologically literate, school programs must respond to emerging innovations, trends and needs.

School programs must also empower young people to think critically about innovations, how they work and how they are compromised.

But questions remain over whether budgets will allow for future growth of these programs.

When the COVID-19 pandemic ends, we must be mindful of the type of future society we want to live in. Do we want our old one back, or do we want a new one where widespread surveillance is the norm in the name of public health?

**Dr Niels Wouters is Research Fellow, Interaction Design Lab, School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne; Head, Research and Emerging Practice for Science Gallery Melbourne.**

**Dr Ryan Kelly is Research Fellow, Interaction Design Lab, Melbourne School of Engineering, University of Melbourne.**

**First published on 24 May 2020 in *Engineering & Technology*.**

Wouters, N and Kelly, R (24 May 2020). *The danger of surveillance tech post COVID-19*. Retrieved from http://pursuit.unimelb.edu.au on 22 June 2020.

# DRONES AND AUSTRALIAN LAW

**Are you allowed to spy on your neighbour? Know the rules around recreational drones. Article reproduced courtesy of CHOICE, written by Andy Kollmorgen**

**If the rise of drone technology in everyday life makes you a little uneasy, it may comfort you to know that pilots of commercial drones weighing two kilograms or more need to be registered with the Civil Aviation Safety Authority (CASA) and have an operator's certificate before their RPA (remotely piloted aircraft) goes zipping through the public airspace. But it's a different story with smaller recreational drones – the ones you can now buy at retailers across Australia.**

## Drones and personal surveillance

Recreational drones are rising in number, and the rules around their use are well laid-out, for the most part. CASA has put together a handy quick-reference guide that breaks down all the flight regulations for new pilots.

But what if you're on the receiving end of a drone's gaze? It's no secret that many recreational drones are equipped with cameras – and that people can be nosy. As it stands, your protection against unauthorised surveillance is limited.

The *Privacy Act*, for instance, only applies to organisations with an annual turnover of $3 million or more. Most recreational drone owners, it's fair to say, wouldn't meet that criteria.

So if you're wondering whether you can legally spy on your neighbours or other persons of interest with a drone, the answer is currently unclear. Anti-stalking legislation may forbid such activity in some cases, and some legal experts say recording activity on private property would be illegal in most states. Others say there really are no hard and fast rules at the moment. In any case, there's nothing encoded in law regarding recreational drones and privacy.

## The law around drones

In search of clarification, we turned to Matthew Craven, a partner at the law firm HWL Ebsworth, who has researched and written about drone privacy issues.

"I am not aware of any case in Australia where a private individual has successfully taken action against a drone pilot for breaching their privacy, whether under the *Privacy Act* or under any other law," Craven tells us.

Unless the drone pilot is working for an organisation with at least $3 million in annual revenue, "it is not possible for a private individual to take action against an individual drone pilot under the *Privacy Act* as it currently stands".

Other laws may apply, but it could be a long shot to mount a case.

"Depending on the conduct and how the drone has been flown, other laws, such as trespass to property, may provide an avenue for redress in certain circumstances," Craven says.

And a pilot could breach state surveillance laws – such as Victoria's *Surveillance Devices Act* – if they use a drone to record private conversations or activities in someone's home. But again, the rules are fuzzy.

"In Victoria at least, taking video footage, without recording audio, of what is happening out in the open in your neighbour's backyard does not contravene the *Surveillance Devices Act*," says Craven.

The Office of the Australian Information Commissioner (OAIC) suggests that neighbourhood security camera legislation could apply, though only under some circumstances and after taking initial steps such as talking to your neighbour or seeking a local community justice or mediation centre for help if that doesn't work.

## New rules on the way

Meanwhile, other state and territory legislation around surveillance is piecemeal, inconsistent, and in some cases outdated. No one's really sure how existing privacy laws apply to recreational drones.

The Civil Aviation Safety Authority tells us it plans to review recreational drone regulations and potentially have new ones in place by the end of the decade, although the federal agency has no jurisdiction over privacy issues.

"This will take several years at least and involve public and aviation industry consultation," CASA's

manager of corporate communications Peter Gibson tells us.

Gibson says personal drones have yet to become a public menace. "With the number of recreational drones increasing we are seeing more safety incidents, but there isn't a flood of complaints by any means."

CASA has issued infringement notices to recreational drone users and delivered warnings for drone safety breaches, but very few in proportion to the number of drones out there. Penalties for illicit drone activity vary depending on the circumstances, but can include fines as high as approximately $10,500 and possible jail time.

If you can, join a local model aero club. Members are likely to be the most educated about where the laws are at for drone operation and when they change, and there could be other benefits, such as insurance cover. Plus you'll get to hang out with people who are just as enthusiastic about drones as you are.

## Redefining privacy

Tighter drone regulations would be a welcome development for the Australian Association for Unmanned Systems, which released a report in May 2015 calling for a ban on the use of drones to record private activity, or activity that happens when people wouldn't expect to be watched or recorded.

And a 2014 federal government report recommended that retailers who sell drones include a pamphlet that "should highlight remotely piloted aircraft users' responsibility not to monitor, record or disclose individuals' private activities without their consent". It also recommended that new legislation be introduced to protect against privacy invasion by drones by July 2015, although that hasn't happened.

## What are the current drone operation rules?

The basic dos and don'ts of recreational drone flying are laid out clearly by the Australian Civil Aviation Safety Authority (CASA).

Recreational drones weighing 2kg or less cannot fly:

- Higher than 120 metres in any airspace
- Closer than 30 metres to anyone not involved in flying or navigating the drone during take-off, flight or landing
- Over groups of people, including beaches, parks, sports ovals and public events
- At night, into a cloud or in fog
- Out of line of site with an unaided eye
- Within 5.5km of a non-controlled aerodrome if there is a manned aircraft operating to, or from, the aerodrome – if your drone weighs more than 100g
- If you become aware of manned aircraft within 5.5km of a helicopter landing pad or smaller aerodrome without a control tower (if you do, land your drone as soon as safely possible)
- In the area of a public safety or emergency operation, for example a bushfire, police, or search and rescue operation
- In a manner that endangers any person, property or other aircraft.

Make sure wherever you plan to fly your drone isn't a restricted area by checking with your local or state governments.

## No VR

Despite many drones' ability to stream video to a screen or even virtual reality (VR) headset, you aren't allowed to use this to navigate the drone. You must have line of site with an unimpeded view – VR headsets are a big no-no.

## Flying over your own land

If operating a drone over your own property, you may be able to apply for the "Flying over your own land" excluded category. The same safety rules apply, but the weight restriction is different.

To be eligible, your drone must:

- Weigh between 100g and 25kg
- Be owned by you (the landowner or leaseholder)
- Only fly over your own property.

No money can be paid for operation of the drone.

If you or the person flying on your behalf holds a remote pilot's licence (RePL), the drone can weigh up to 150kg.

For more information about flying over your own land, head to casa.gov.au. Be sure to keep records of your flights – CASA can ask to see them at any time.

## There was an app for that

Unfortunately, CASA retired its "Can I fly there" app, which had information about restricted areas and safety regulations. CASA now suggests you use OpenSky by Wing Aviation LLC. However, this app has very poor reviews on both the Apple and Android app stores, with some users claiming it lacks important information.

Even if you do use and trust OpenSky, you should still check if any local government, environmental or state government rules or regulations apply.

## Recreational drones dos and don'ts

*Q:* **Can I drop off a parcel or other item with a recreational drone?**

*A:* Yes, as long as the operation doesn't pose a risk to people, property or another aircraft.

*Q:* **Can I fly my recreational drone over a sporting event, a busy beach or other heavily populated areas?**

*A:* No.

*Q:* **Can I take photos or videos of people with a personal drone?**

*A:* The legal view on this varies depending on who you talk to. Whatever the case, there's currently no specific piece of legislation that protects the privacy of individuals against recreational drones. However, you can make a privacy complaint to the Office of the Australian Information Commissioner.

*Q:* **Can I use my recreational drone for commercial purposes?**

*A:* Yes, but you'll need to give CASA five days notice that you plan to do so, apply for an aviation reference number, and follow the rules that apply to all recreational drones.

*Q:* **Can my neighbour take video footage of what's going on in my backyard without my knowledge?**

*A:* The legal view on this varies depending on who you talk to. Whatever the case, there is currently no specific piece of legislation that protects the privacy of individuals against recreational drones. At any rate, we don't recommend you record footage of anyone without seeking permission first.

*Q:* **Can I fly my drone over an airfield?**

*A:* Recreational drones weighing more than 100g can't get any closer than 5.5km to a towered airfield or other high-security area.

*Q:* **Can I wear virtual reality style, first-person goggles while I pilot the drone?**

*A:* No. Some brands send a live video feed to first-person goggles worn around the head, to provide an immersive viewing experience. It's illegal to wear these while piloting your drone, as CASA regulations require you to maintain a direct line of sight at all times. In this instance, a friend or family member can wear the goggles.

*Q:* **Can I fly more than one recreational drone at a time?**

*A:* No.

## Drone accidents

Drones have been used in Australia by law enforcement agencies, the CSIRO and other science organisations, the media, animal rights groups and others. But drones have also run amok. In 2013, a recreational drone crashed into the Sydney Harbour Bridge, resulting in an $850 fine for the operator. In 2014, a triathlete in WA was allegedly struck by a malfunctioning drone, and in February 2016, a personal drone crashed during a ceremony at the Australian War Memorial in Canberra.

## Reporting unsafe drone use

You can report drones operated unsafely to CASA, though the agency has no jurisdiction over privacy issues.

---

CHOICE (14 February 2020). *Drones and Australian law.* Retrieved from www.choice.com.au on 22 June 2020.

# BIG BROTHER IS WATCHING: HOW NEW TECHNOLOGIES ARE CHANGING POLICE SURVEILLANCE

**Surveillance is changing from being static, fixed and reactive to being flexible and proactive. The enhanced capabilities helps law enforcement fight crime, rather than just solve it, explains Terry Goldsworthy**

When we think of surveillance, we tend to imagine traditional surveillance tools like CCTV systems run by local authorities. The use of CCTV has certainly increased since I was a young constable on the Gold Coast in the early 1990s. From a CCTV network of 16 cameras when they were first introduced to the city precinct, the network has grown to more than 500 cameras today.

But surveillance is much more than just CCTV. It now includes things like private home or business security systems, police body-worn cameras (BWC) and the use of helicopters and drones. And we all have the capacity to conduct surveillance and gather evidence using the technology contained in our mobile phones.

These new technologies are changing the way police approach surveillance. Rather than using surveillance tools reactively to catch criminals caught in the act on camera, police are now proactively seeking out criminals in the process of offending and recording the evidence on the spot.

## CCTV HELPS SOLVE CRIME, NOT PREVENT IT

Most studies show that CCTV by itself does not necessarily prevent crime, but it does assist in responding to and solving crime.

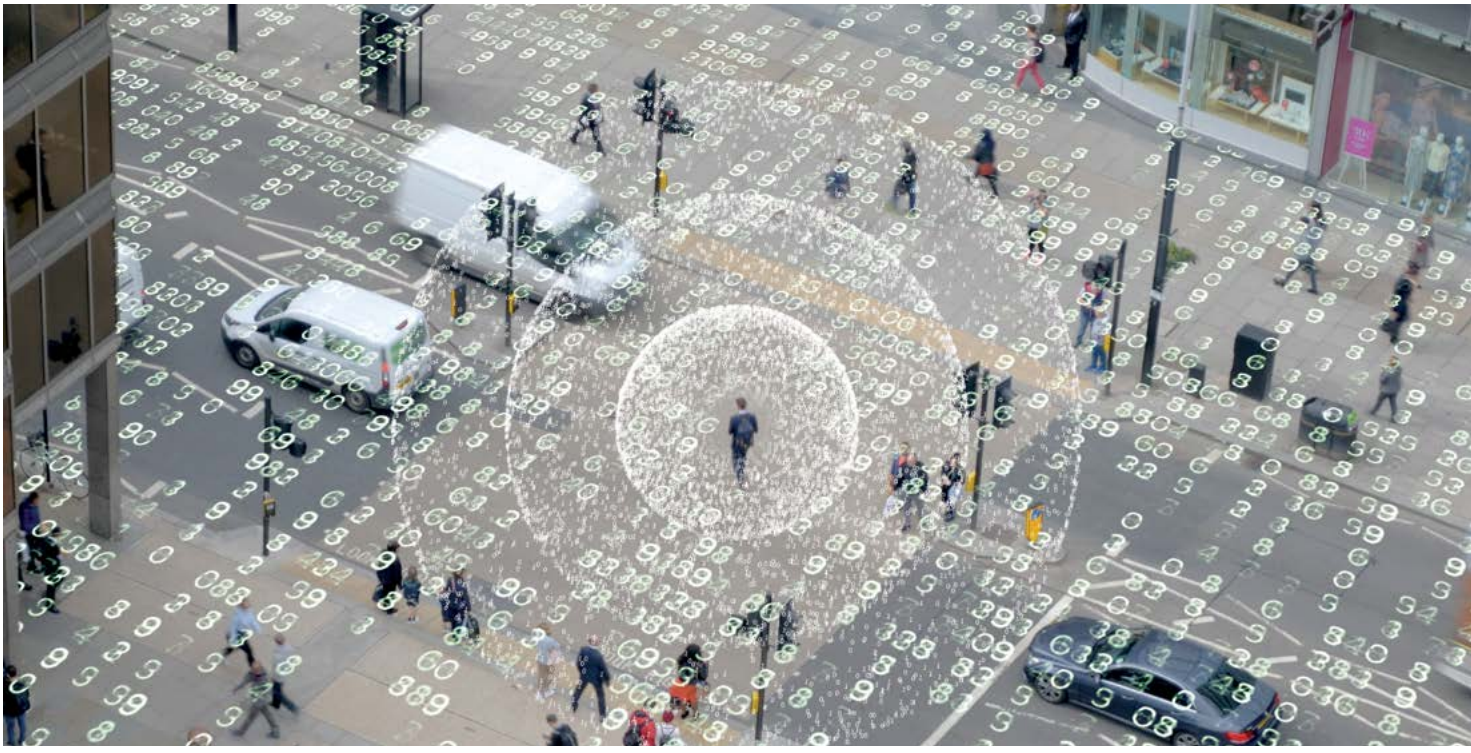
In the Boston bombing case, police used footage and images from state, public and private sources to identify the suspects. CCTV is also proving crucial in identifying the bombers who staged the recent co-ordinated attacks in Sri Lanka.

Two studies released by the Australian Institute of Criminology last month focused on the use of CCTV by police. The first showed that where police requested and used CCTV footage, there was an increase in the rate of matters being solved. The second study showed CCTV footage is highly valued by law enforcement personnel, with 90% of investigators using the footage when it was available. Two-thirds were able to use it for the reason they had requested it.

## NEW TOOLS, NEW CAPABILITIES

We are now seeing a move from reactive surveillance to proactive surveillance. Police body-worn cameras (BWCs) are an example of this. Every police service in Australia is now using BWCs. Rather than just

Surveillance is much more than just CCTV. It now includes things like private home or business security systems, police body-worn cameras and the use of helicopters and drones. And we all have the capacity to conduct surveillance and gather evidence using the technology contained in our mobile phones.



Surveillance is changing from being static, fixed and reactive to being flexible and proactive. The enhanced capabilities helps law enforcement fight crime, rather than just solve it.

recording a criminal event by chance, BWCs enable police to actively seek out those committing offences, and record the evidence against such offenders.

Queensland Police requires its officers to record whenever the officer is acting in the performance of his or her duties. The device must be recording prior to, and during, the exercising of a police power or applying a use of force.

This requirement can be problematic since the officer must physically start the recording. In the shooting matter of Justine Damond in the United States, officers were criticised for having their recording devices turned off during the shooting.

Some services have attempted to deal with this issue, such as Western Australia Police for instance, by having the BWC automatically begin recording when an officer draws their firearm.

Even traditional CCTV is becoming proactive with the introduction of mobile CCTV cameras that can be moved as required to areas of community concern.

Many police services are using drones for tasks such as crowd management, surveillance and target acquisition. Queensland and Victoria are just two states that are committed to the use of drones for policing purposes. In 2017, Queensland Police had a fleet of ten drones.

## FACIAL RECOGNITION ENABLES 'PREDICTIVE POLICING'

Facial recognition software was once the thing of Hollywood movies like *Mission Impossible*. It's now a reality, with the Council of Australian Governments (COAG) agreeing to share biometric data, such as drivers licence details and passport photos, between government agencies.

Facial recognition software was used by police during the 2018 Commonwealth games in Queensland. And the Queensland government has indicated police will continue to use facial recognition tools – although confusion surrounds when or how it will be deployed. The ABC has reported that the facial recognition system was so rushed that it lacked the data to operate effectively during the Commonwealth Games.

Facial recognition adds a predictive policing capability to traditional CCTV systems. In essence, predictive policing or pre-crime policing is an attempt by law enforcement to disrupt criminal activity by the early identification of criminal threats.

For example, Operation Nomad saw South Australian police visiting suspected and convicted arsonists when automated number plate recognition alerted them to suspects driving in fire danger zones. The operation was credited with the reduction of bushfire-related arson.

## KEEPING A WATCH ON BIG BROTHER

Surveillance is changing from being static, fixed and reactive to being flexible and proactive. The enhanced capabilities helps law enforcement fight crime, rather than just solve it.

The Coalition government promised A$20 million to increase the number of CCTV cameras across the country. Under the proposal, up to 2,600 cameras would be installed at 500 "crime hot spots".

While this is a largely positive move, we must ensure that there is accountability and transparency in the use of these technologies, and ensure they serve the purposes for which they were intended. An effective governance regime is essential to instill public confidence in the use of these technologies.

### DISCLOSURE STATEMENT

**Terry Goldsworthy does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond his academic appointment.**

**Terry Goldsworthy is Associate Professor in Criminology, Bond University.**

THE CONVERSATION

Goldsworthy, T (8 May 2019). *Big brother is watching: how new technologies are changing police surveillance.* Retrieved from http://theconversation.com on 19 June 2020.

# Facial recognition technology is expanding rapidly across Australia. Are our laws keeping pace?

**With the spread of this technology in Australia and other democratic countries, there are important questions about the legal implications of scanning, storing and sharing facial images, observes Rick Sarre**

Facial recognition technology is increasingly being trialled and deployed around Australia. Queensland and Western Australia are reportedly already using real-time facial recognition through CCTV cameras. 7-Eleven Australia is also deploying facial recognition technology in its 700 stores nationwide for what it says is customer feedback.

And Australian police are reportedly using a facial recognition system that allows them to identify members of the public from online photographs.

Facial recognition technology has a somewhat nefarious reputation in some police states and non-democratic countries. It has been used by the police in China to identify anti-Beijing protesters in Hong Kong and monitor members of the Uighur minority in Xinjiang.

With the spread of this technology in Australia and other democratic countries, there are important questions about the legal implications of scanning, storing and sharing facial images.

## Use of technology by public entities

The use of facial recognition technology by immigration authorities (for example, in the channels at airports for people with electronic passports) and police departments is authorised by law and therefore subject to public scrutiny through parliamentary processes.

In a positive sign, the government's proposed identity matching services laws are currently being scrutinised by a parliamentary committee, which will address concerns over data sharing and the potential for people to be incorrectly identified. Indeed, Australian Human Rights Commissioner Edward Santow recently sounded an alarm over the lack of regulation in this area.

At the moment, there are not strong and clear enough legal protections in place to prevent the misuse of facial recognition in high stakes areas like policing or law enforcement. Another specific concern with the legislation is that people's data could be shared between government agencies and private companies like telcos and banks.

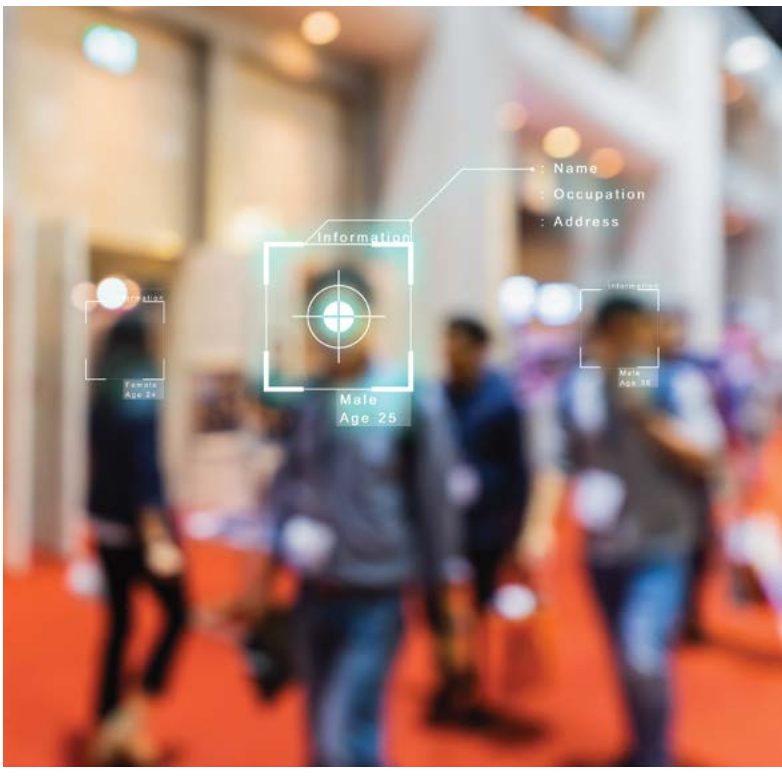
## How private operators work

Then there is the use of facial recognition technology by private companies, such as banks, telcos and even 7-Elevens. Here, the first thing to determine is if the technology is being used on public or private land. A private landowner can do whatever it likes to protect itself, its wares and its occupants so long as it doesn't break the law (for example, by unlawful restraint or a discriminatory practice). This would include allowing for the installation and monitoring of staff and visitors through facial recognition cameras.

*At the moment, there are not strong and clear enough legal protections in place to prevent the misuse of facial recognition in high stakes areas like policing or law enforcement.*

By contrast, on public land, any decision to deploy such tools must go through a more transparent decision-making process (say, a council meeting) where the public has an opportunity to respond. This isn't the case, however, for many "public" properties (such as sports fields, schools, universities, shopping centres and hospitals) that are privately owned or managed. As such, they can be privately secured through the use of guards monitoring CCTV cameras and other technologies.

Facial recognition is not the only surveillance tool available to these private operators. Others include iris and retina scanners, GIS profiling, internet data-mining (which includes "predictive analytics," that is, building a customer database on the strength of online behaviours), and "neuromarketing" (the use of surveillance tools to capture a consumer's attributes during purchases).



There's more. Our technological wizardry also allows the private sector to store and retrieve huge amounts of customer data, including every purchase we make and the price we paid. And the major political parties have compiled extensive private databanks on the makeup of households and likely electoral preferences of their occupants.

*Another specific concern with the legislation is that people's data could be shared between government agencies and private companies like telcos and banks.*

Is it any wonder we have started to become a little alarmed by the reach of surveillance and data retention tools in our lives?

## What's currently allowed under the law

The law in this area is new and struggling to keep up with the pace of change. One thing is clear: the law does not prohibit even highly intrusive levels of surveillance by the private sector on private land in the absence of illegal conduct.

The most useful way of reviewing the legal principles in this space is to pose specific questions:

### *Can visitors be legally photographed and scanned when entering businesses?*

The answer is yes where visitors have been warned of the presence of cameras and scanners by the use of signs. Remaining on the premises denotes implied consent to the conditions of entry.

### *Do people have any recourse if they don't want their image taken?*

No. The law does very little to protect those who may be upset by the obvious presence of a surveillance device on a door, ceiling or wall. The best option for anybody concerned about this is to leave the premises or not enter in the first place.

### *What about sharing images? Can private operators do whatever they like with them?*

No. The sharing of electronic data is limited by what are referred to as the "privacy principles", which govern the rights and obligations around the collection, use and sharing of personal information. These were extended to the private sector in 2001 by amendments to the *Commonwealth Privacy Act 1988.*

These privacy principles would certainly prohibit the sharing of images except, for example, if a store was requested by police to hand them over for investigation purposes.

### *Can private businesses legally store your image?*

Yes, private or commercial enterprises can store images of people captured on their cameras in their own databases. A person can ask for the image to be disclosed to them (that is, to confirm it is held by the store and to see it) under the "privacy principles". Few people would bother, though, since it's unlikely they would know it even exists.

The privacy principles do, however, require the business to take reasonable steps to destroy the data or image (or ensure there is de-identification) once it is no longer needed.

### *What if facial recognition technology is used without warnings like signs?*

If there is a demonstrable public interest in any type of covert surveillance (for example, to ensure patrons in casino gaming rooms are not cheating, or to ensure public safety in crowded walkways), and there is no evidence of, or potential for, misuse, then the law permits it.

However, it is not legal to film someone covertly unless there is a public interest in doing so.

## What does the future hold?

Any change to the laws in this area is a matter for our parliamentarians. They have been slow to respond given the difficulty of determining what is required.

It will not be easy to frame legislation that strikes the right balance between respecting individuals' rights to privacy and the desires of commercial entities to keep their stock, patrons and staff secure.

In the meantime, there are steps we can all take to safeguard our privacy. If you want to protect your image completely, don't select a phone that switches on when you look at it, and don't get a passport.

And if certain businesses want to scan your face when you enter their premises, give them a wide berth, and your feedback.

**DISCLOSURE STATEMENT**

**Rick Sarre is a member of the SA State Council of the ALP.**

**Rick Sarre is Adjunct Professor of Law and Criminal Justice, University of South Australia.**

THE CONVERSATION

Sarre, R (10 July 2020). *Facial recognition technology is expanding rapidly across Australia. Are our laws keeping pace?* Retrieved from http://theconversation.com on 25 August 2020.

# LARGE-SCALE FACIAL RECOGNITION IS INCOMPATIBLE WITH A FREE SOCIETY

**Should Australia be using this technology? Seth Lazar, Claire Benn and Mario Günther address fundamental questions about the kind of people, and the kind of society, we want to be**


In the US, tireless opposition to state use of facial recognition algorithms has recently won some victories. Some progressive cities have banned some uses of the technology. Three tech companies have pulled facial recognition products from the market. Democrats have advanced a bill for a moratorium on facial recognition. The Association for Computing Machinery (ACM), a leading computer science organisation, has also come out against the technology.

Outside the US, however, the tide is heading in the other direction. China is deploying facial recognition on a vast scale in its social credit experiments, policing, and suppressing the Uighur population. It is also exporting facial recognition technology (and norms) to partner countries in the Belt and Road Initiative. The UK High Court ruled its use by South Wales Police lawful last September (though the decision is being appealed).

Here in Australia, despite pushback from the Human Rights Commission, the trend is also towards greater use. The government proposed an ambitious plan for a national face database (including wacky trial balloons about age-verification on porn sites). Some local councils are adding facial recognition into their existing surveillance systems. Police officers have tried out the dystopian services of Clearview AI.

Should Australia be using this technology? To decide, we need to answer fundamental questions about the kind of people, and the kind of society, we want to be.

## FROM FACIAL RECOGNITION TO FACE SURVEILLANCE

Facial recognition has many uses. It can verify individual identity by comparing a target image with data held on file to confirm a match – this is "one-to-one" facial recognition. It can also compare a target image with a database of subjects of interest. That's "one-to-many". The most ambitious form is "all-to-all" matching. This would mean matching every image to a comprehensive database of every person in a given polity.

Each approach can be carried out asynchronously (on demand, after images are captured) or in real time. And they can be applied to separate (disaggregated) data streams, or used to bring together massive surveillance datasets.

Facial recognition occurring at one end of each of these scales – one-to-one, asynchronous, disaggregated – has well-documented benefits. One-to-one real-time facial recognition can be convenient and relatively safe, like unlocking your phone, or proving your identity at an automated passport barrier.

Asynchronous disaggregated one-to-many facial recognition can be useful for law enforcement – analysing CCTV footage to identify a suspect, for example, or finding victims and perpetrators in child abuse videos.

However, facial recognition at the other end of these scales – one-to-many or all-to-all, real-time, integrated – amounts to face surveillance, which has less obvious benefits. Several police forces in the UK have trialled real-time one-to-many facial recognition to seek persons of interest, with mixed results. The benefits of integrated real-time all-to-all face surveillance in China are yet to be seen.

And while the benefits of face surveillance are dubious, it risks fundamentally changing the kind of society we live in.

## FACE SURVEILLANCE OFTEN GOES WRONG, BUT IT'S BAD EVEN WHEN IT WORKS

Most facial recognition algorithms are accurate with head-on, well-lit portraits, but underperform with "faces in the wild". They are also worse at identifying black faces, and especially the faces of black women.

The errors tend to be false positives – making incorrect matches, rather than missing correct ones. If face surveillance were used to dole out cash prizes, this would be fine. But a match is almost always used to target interventions (such as arrests) that harm those identified.

More false positives for minority populations means they bear the costs of face surveillance, while any benefits are likely to accrue to majority populations. So using these systems will amplify the structural injustices of the societies that produce them.

Even when it works, face surveillance is still harmful. Knowing where people are and what they are doing enables you to predict and control their behaviour.

You might believe the Australian government wouldn't use this power against us, but the very fact they have it makes us less free. Freedom isn't only about making it unlikely others will interfere with you. It's about making it impossible for them to do so.

## FACE SURVEILLANCE IS INTRINSICALLY WRONG

Face surveillance relies on the idea that others are entitled to extract biometric data from you without your consent when you are in public. This is false. We have a right to control our own biometric data. This is what is called an underived right, like the right to control your own body.

Of course, rights have limits. You can lose the protection of a right – someone who robs a servo may lose their right to anonymity – or the right may be overridden, if necessary, for a good enough cause. But the great majority of us have committed no crime that would make us lose the right to control our biometric data. And the possible benefits of using face surveillance on any particular occasion must be discounted by their probability of occurring. Certain rights violations are unlikely to be overridden by hypothetical benefits.

Many prominent algorithms used for face surveillance were also developed in morally compromised ways. They used datasets containing images used without permission of the rightful owners, as well as harmful images and deeply objectionable labels.

## ARGUMENTS FOR FACE SURVEILLANCE DON'T HOLD UP

There will of course be counterarguments, but none of them hold up. You've already given up your privacy to Apple or Google – why begrudge police the same kind of information? Just because we have sleepwalked into a surveillance society doesn't mean we should refuse to wake up.

Human surveillance is more biased and error-prone than algorithmic surveillance. Human surveillance is indeed morally problematic. Vast networks of CCTV cameras already compromise our civil liberties. Weaponizing them with software that enables people to be tracked across multiple sites only makes them worse.

We can always keep a human in the loop. False positive rates can be reduced by human oversight, but human oversight of automated systems is itself flawed and biased, and this doesn't address the other objections against face surveillance.

Technology is neither good nor bad in itself; it's just a tool that can be used for good or bad ends. Every tool makes some things easier and some things harder. Facial recognition makes it easier to oppress vulnerable populations and violate everyone's basic rights.

## IT'S TIME FOR A MORATORIUM

Face surveillance is based on morally compromised research, violates our rights, is harmful, and exacerbates structural injustice, both when it works and when it fails. Its adoption harms individuals, and makes our society as a whole more unjust, and less free.

A moratorium on its use in Australia is the least we should demand.

**DISCLOSURE STATEMENT**

**The authors do not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and have disclosed no relevant affiliations beyond their academic appointment.**

**Seth Lazar is Professor, Australian National University.**

**Claire Benn is Research Fellow, Humanising Machine Intelligence Grand Challenge, Australian National University.**

**Mario Günther is Research Fellow, Humanising Machine Intelligence Grand Challenge, Australian National University.**

THE CONVERSATION

Lazar, S, Benn, C and Gunther, M (10 July 2020). *Large-scale facial recognition is incompatible with a free society.* Retrieved from http://theconversation.com on 25 August 2020.

# We don't own data like we own a car – which is why we find data harder to protect

**People find data difficult to own – and things we don't own, we tend not to protect, write Vincent Mitchell and Bernadette Kamleitner**

It's known as the "privacy paradox": people say they want to protect their data privacy online, but often do little to keep it safe.

Why?

We propose that it's because people find data difficult to own – and things we don't own, we tend not to protect. This is a question of psychological, not legal, ownership, which is more powerful in explaining why we care for things we call "mine".

Owning data is not like owning a car. If someone used your car, rented your car to others or stole it – you'd notice. And you'd care. But our data can be used, on-sold or stolen without our permission, without us ever really being aware, or worrying too much about it.

Data points are hard for us to claim and value. We find them difficult to own because we have less control, intimate knowledge and investment in them due to data being intangible, invisible and complex.

## HARD TO CLAIM

Data's intangibility means it's difficult for us to claim ownership. Unlike objects, data can be used by more than one person at a time. It is hard to know if you are the only person currently claiming the data and it is hard to exclude others from doing so. And unlike objects, repeated use doesn't degrade or imprint data. Because data can be easily copied, nothing is physically taken away from us. We cannot even feel if data are being harvested. This undermines our ability to claim it, and prevent it from being taken.

## HARD TO VALUE

Generally we own and protect only things that are valuable or meaningful. However, consumers don't know how valuable their personal data points actually are. This is partly because what comes in high volumes tends to be deemed low in value. And with the exceptions of things like your name or birth date, data points hold little value by themselves. It is only once they are combined with other data – of the same or other people – that they accrue value. This could happen through profiling.

This masking of value is accentuated by app permissions that often request bundles of data, such as "all contacts", rather than specific meaningful contacts, such as "your mother's phone number". Because consumers often assign a similar value to specific data points as to bundles of data, they don't see the value in giving away hundreds of contacts' details.

## HARD TO ATTRIBUTE OWNERSHIP

Attribution is key in the processes of ownership. The more we see someone as the person that brought the data into being through labour, the more we attribute ownership to them.

Even for well specified information, consumers are

It's known as the "privacy paradox": people say they want to protect their data privacy online, but often do little to keep it safe.

Owning data is not like owning a car. If someone used your car, rented your car to others or stole it – you'd notice. And you'd care. But our data can be used, on-sold or stolen without our permission, without us ever really being aware, or worrying too much about it.

uncertain about the extent to which data points are actually theirs. But most data are not well specified. Like any raw material, crude data points – such as your age – are inherently malleable. Without our knowing, they can be converted, combined and contrived to create valued things through another person's labour. This makes it hard to determine whose data it actually is.

And some personal data are jointly owned. For example, online purchase data are owned by you and the retailer.

The characteristics of data also undermine the processes we need to go through in order to feel that we own things, namely: control, intimate knowledge, and self-investment.

## LACK OF CONTROL

We find it difficult to control our data points because they are invisible, intangible, and increasingly diverse. For example, body parameters, location information, photos and contacts are all data points that come into being as a by-product of our lives. We cannot control these data points without altering the way we live.

Personal data is so complex and comes in such a massive scope, that it defies our ability to comprehend it. This is another fundamental barrier to the experience of control.

## LACK OF INTIMATE KNOWLEDGE

Since personal data are about us, it seems obvious that we should be knowledgeable about them. Not so.

Personal data comes from many unobtrusive sources, such as connected devices, which are collected passively. Data are largely invisible and do not noisily remind us of their existence. This precludes us from having intimate knowledge of them. Worse still, over 90% of us fail to fully understand permissions designed to explain the data collection and enhance our knowledge.

## LACK OF SELF-INVESTMENT

Another consequence of data being a by-product of our existence is we need to invest little effort into bringing them about. For example, we produce location data regardless of whether we want to or not. Only photos may require some investment from us, but they are a small proportion of our data.

The privacy paradox exists because personal data are possessions that are hard to own and protect.

Making data easier to claim through physical downloads, as Facebook have recently moved to do, or giving data value and attributing ownership through payment for data, can give us more control, knowledge and investment.

**DISCLOSURE STATEMENT**

**The authors do not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and have disclosed no relevant affiliations beyond their academic appointment.**

**Vincent Mitchell is Professor of Marketing, University of Sydney.**

**Bernadette Kamleitner is Professor of Marketing, Vienna University of Economics and Business.**

THE CONVERSATION

Mitchell, V, and Kamleitner, B (21 June 2018). *We don't own data like we own a car – which is why we find data harder to protect.* Retrieved from http://theconversation.com on 19 June 2020.

# AUSTRALIAN COMMUNITY ATTITUDES TO PRIVACY SURVEY

## Executive summary from the latest national privacy survey, prepared for the Office of the Australian Information Commissioner by Lonergan Research

The Australian Community Attitudes to Privacy Survey (ACAPS) 2020 was conducted between February and March 2020 with a nationally representative sample of 2,866 unique respondents aged 18 years and over. Additional research was conducted in early April 2020 to measure changing attitudes to privacy issues following the COVID-19 outbreak. For the first time since the survey's inception in 2001, all data was collected online.

The main objectives of the 2020 survey were to:

- Provide insight on Australian attitudes towards privacy
- Understand the change in Australian attitudes and behaviours over time through the construction of longitudinal trend models
- Identify awareness of and concern about emerging privacy issues, related to new technologies and to regulation, and
- Collect data to assist the OAIC as the national privacy regulator across policy, compliance, and communications initiatives.

### MAIN FINDINGS

Privacy is an important issue for most Australians. Seventy per cent consider the protection of their personal information to be a major concern in their life.

The biggest privacy risks identified by Australians in 2020 are:

- Identify theft and fraud (76%)
- Data security and data breaches (61%)
- Digital services, including social media sites (58%)
- Smartphone apps (49%), and
- Surveillance by foreign entities (35%) or Australian entities (26%).

Three in 5 Australians (59%) have experienced problems with how their personal information was handled in the past 12 months. The majority involved unwanted marketing communications or having their personal information collected (with or without consent) when this was not required to deliver the service.

The behaviours Australians are most likely to consider a misuse are when:

- An organisation uses their personal information in ways that cause harm, loss or distress (84%)
- Information supplied to an organisation for a specific purpose is used for another purpose (84%), and
- A personal device is listening to conversations and sharing this with other organisations without their knowledge (83%).

Concerns regarding data privacy are driven by a belief that many companies routinely use personal information for purposes that make Australians uncomfortable.

Levels of comfort with the data practices of online businesses including social media sites and other digital platforms are low. They vary according to the nature of the organisation involved, the purpose for collecting or using the data and the type of personal information collected:

- The Australian Government is generally more trusted than businesses with the protection of personal information. Certain purposes are considered more legitimate than others, such as public safety. Australians are slightly more comfortable with most instances of government use of personal information than they were in 2017.
- Australians are particularly uncomfortable with businesses tracking their location through their mobile or web browser (62% uncomfortable) and keeping databases of information on what they have said and done online (62% uncomfortable).
- Australians are increasingly questioning data practices where the purpose for collecting personal information is unclear, with 81% of Australians considering 'an organisation asking for information that doesn't seem relevant to the purpose of the transaction' as a misuse (up 7% since 2017).


Most Australians have a clear understanding of why they should protect their personal information (85% agree) but half say they don't know how (49%agree). Four in 10 rate their knowledge of privacy as fair to poor, while 23% say their knowledge is excellent or very good. One third (34%) feel they are in control of their privacy, however just as many (34%) do not. This is not through lack of desire, as 87% want more control and choice over the collection and use of their personal information.

In line with this, Australians are most likely to believe they should have:

- The right to ask a business to delete their personal information (84%)
- The right to ask a government agency to delete their personal information (64%)
- The right to seek compensation in the courts for a breach of privacy (78%)
- To know when their personal information is used in automated decision-making if it could affect them (77%), and
- The right to object to certain data practices while still being able to access and use the service (77%).

Compared to 2017, fewer Australians are taking measures to protect their privacy, in particular:

- Asking public or private sector organisations why they need personal information (down 16%)
- Choosing not to use an app on a mobile device because of concerns over handling personal information (down 13%)
- Shredding documents (down 11%), and
- Adjusting privacy settings on a social networking website (down 10%).

## PRIVACY REGULATION AND REFORM

Eighty-three per cent of Australians would like the government to do more to protect the privacy of their data. A quarter (24%) feel the privacy of their personal information is well protected, while 40% feel it is poorly protected.

On a prompted basis, half (48%) of Australians know about the Privacy Commissioner, an increase of 4% since 2017. Australians are just as likely to report a misuse of privacy to the police (37%) as the Privacy Commissioner (38%). Two-thirds (64%) of those surveyed are unaware that they can request access to their personal information from business and government agencies. This has not changed since 2017.

## PRIVACY POLICIES

Only 1 in 5 Australians (20%) read and are confident they understand privacy policies on internet sites. The main reasons why Australians do not read privacy

policies include the length and difficulty of the policies.

Those who read privacy policies are much more likely to actively take measures to ensure the protection of their privacy and personal information.

Australians strongly support measures to improve privacy policies to make them easier to read. They want to see standard, simple language (87% support) and a plain English summary at the start of every privacy policy (86% support). There is also support (73%) for the use of icons as indicators that certain activities are undertaken, for example, if data is stored overseas.

## CHILDREN'S PRIVACY

Australian parents provide their children access to connected devices and digital services early in life and are more likely to be concerned about their children's privacy (91%) than their own (82%). They are particularly uncomfortable with businesses tracking the location of a child without permission (70%) and businesses obtaining personal information about a child and selling it to third parties (69%).

Parents are very supportive of measures to increase the protection of their children's privacy and educate children on these issues. The most appealing idea is that a company must provide important data privacy information to children in clear language that is not misleading (85% support, 60% strongly support).

Half of parents (47%) believe that they are doing everything they can to protect their child's personal information. Thirteen per cent do not actively do anything to protect their child's privacy online. Lack of knowledge, time and difficulty are the main reasons given for not doing more.

On average, parents believe children should be able to consent to handing over their personal information in exchange for an online service from the age of 13, which generally coincides with the acquisition of a mobile phone and more widespread use of social media.

## YOUNG AUSTRALIANS

Young Australians (18-24) are more likely than older counterparts to know how to protect their personal information (54%; cf. 49% overall, 43% aged over 50). However, they are less likely to understand why they should protect their personal information (78%; cf. 85% overall).

Young Australians are the least likely age group to believe protecting personal information is a major concern in their life (63% cf. 70% overall) and the most likely to believe it is too much effort to protect the privacy of their data (39%; cf. average 30%).

Three in 10 (29%) believe the privacy of information and data when choosing a digital service is extremely important, compared with the Australian average of 54%.

Compared to the average Australian, those aged 18-24 are more likely to take control of their privacy in the digital realm, but less likely to take control outside this environment.

Young Australians are more likely to adjust settings on social media (51%; cf. average 46%), use adblockers, VPNs and privacy-focused web search engines (40%; cf. average 32%) and change smartphone settings for a higher level of privacy (43%; cf. average 35%). They are less likely to shred documents (26%; cf. average 41%) or to ask public or private sector organisations why they need their information (20%; cf. average 27%).

As with control, young Australians are also more likely to take action to protect their privacy. A quarter (26%) of young Australians have changed a service provider due to privacy concerns (cf. average 13%). They are more likely to have deleted an app (61% cf. average 57%) and request that personal information is deleted (27% cf. average 23%).

## PRIVACY AND COVID-19

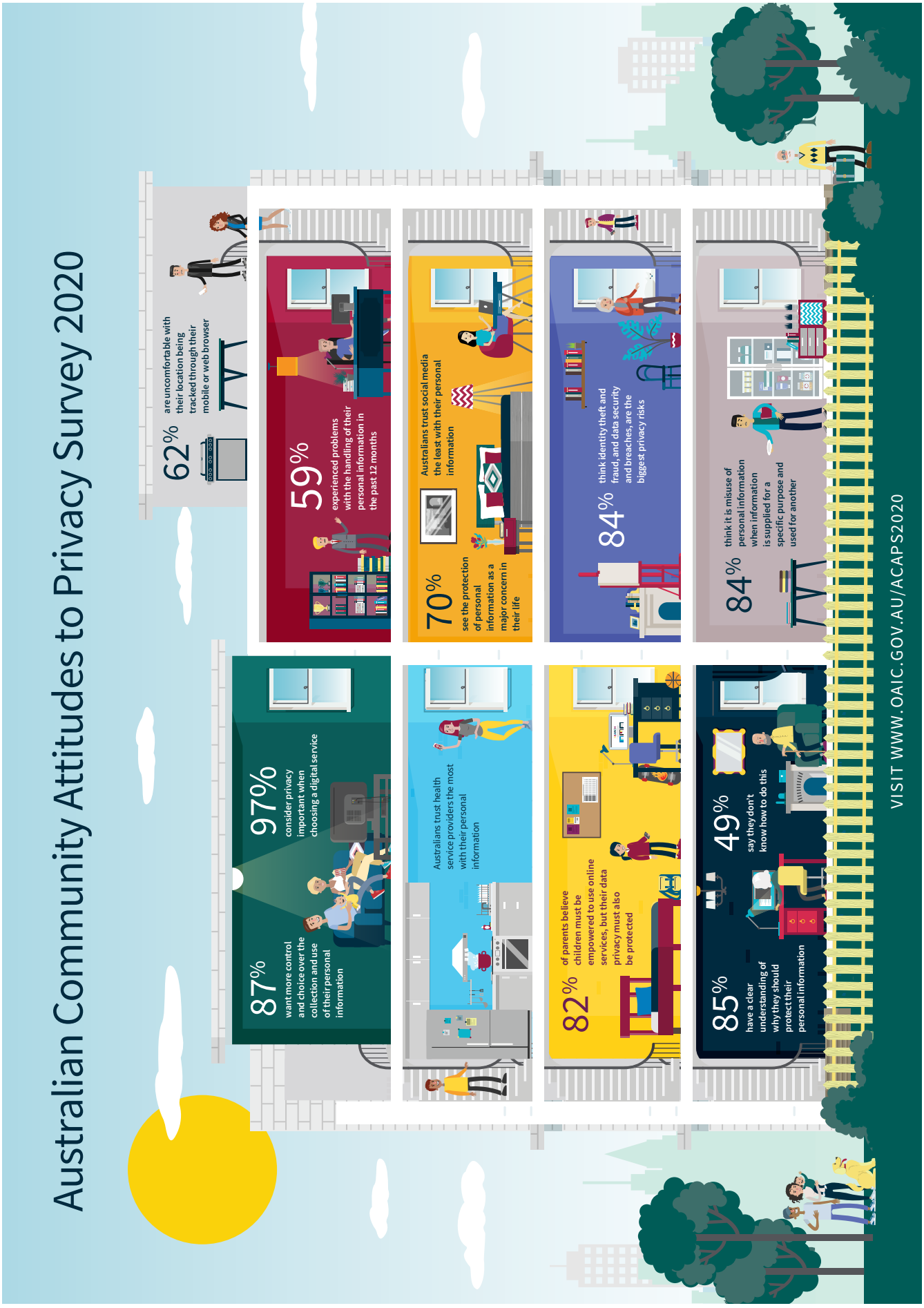
The main fieldwork for the 2020 ACAPS survey was conducted immediately prior to the COVID-19 outbreak in Australia. The outbreak had an impact on attitudes to privacy with half (50%) of Australians considering that their privacy is more at risk in a COVID-19 environment than usual and almost half (48%) being more concerned about the protection of their location information than they were before the outbreak. Overall, more Australians feel comfortable than uncomfortable with the protection of their personal information while using digital services at home during the COVID-19 outbreak, whether it is for work, studying or personal use.

The majority (60%) agree that some privacy concessions must be made to combat COVID-19 for the greater good. The same proportion agree that concessions should not be permanent. Consent is still important: more than half (54%) are comfortable with the government using phone data to help stop the spread of COVID-19 with consent, whereas 29% are comfortable with phone data being used without consent.

**Prepared for the Office of the Australian Information Commissioner by Lonergan Research (September 2020).**

---

Office of the Australian Information Commissioner. *Australian Community Attitudes to Privacy Survey 2020*, Executive summary pp. 6-9. Retrieved from www.oaic.gov.au on 22 October 2020.




Office of the Australian Information Commissioner. *Australian Community Attitudes to Privacy Survey 2020*, Infographic. Retrieved from www.oaic.gov.au on 22 October 2020.

# REBOOT YOUR PRIVACY AND PROTECT YOUR PERSONAL INFORMATION ONLINE

***Protecting your personal information online is increasingly important as even more of our day-to-day activity takes place in the digital environment: from work, study and socialising to shopping online or using connected devices like home assistants. This guide is courtesy of OAIC***

## 1. Protect your accounts

Multi-factor authentication, strong and unique passphrases and automatic device updates are some of the best tactics you can use to keep your accounts secure and protect your personal information online. Reduce the risk of someone gaining unauthorised access to your accounts and stealing your digital identity by:

- Enabling two-factor authentication/multi-factor authentication for accounts and devices whenever possible, for an extra layer of security and to prevent your logins being compromised.
- Setting strong and unique passphrases for your important online accounts. Like a password, a passphrase can be used to verify access to a computer system, program or service, and is most effective when it is:
  - Unique – not a famous phrase or lyric, and not re-used
  - Longer – phrases are generally longer than words
  - Complex – naturally occurring in a sentence with uppercase, symbols and punctuation
  - Easy to remember – saves you being locked out.
- Storing your login credentials in a reputable password manager which can also generate new passphrases for you to use across different platforms.
- Turning on automatic software updates for your devices to keep your security up to date. The Australian Cyber Security Centre has step-by-step guides for turning on automatic updates for Windows 10 as well as iOS devices.
- Checking whether your passwords/passphrases have been compromised on Have I Been Pwned, a searchable database of email addresses that have been caught up in data breaches. If your password is listed you should update it immediately.

Get more tips on how to protect your information at cyber.gov.au and the Australian Cyber Security Centre (www.cyber.gov.au/acsc/individuals-and-families/do-things-safely).

## 2. Detox your digital profile

Social media is a great way to stay in touch, but are you aware of how much personal information you share? Posts and status updates, polls and quizzes, photos and videos can all reveal a lot about you. The information you share may be given to other organisations without your explicit consent. It can also be used to steal your identity or cause you harm in other ways.

Adjust your privacy settings to help protect your personal information – use the 'privacy check-up tools' on Facebook and Google or edit your privacy settings on other networks. Depending on the site, you may be able to:

- Set your page or online profile to 'private'
- Limit who can see your contact details or find your profile via your phone or email
- Limit the audience for your posts or stories, including old posts
- Control who can send you friend requests or connect with you
- Review and reduce the number of apps that can access your social media profile

You should also be aware of what you share: think before you tag yourself at a location, and consider their privacy before you tag a friend. For more tips check the Data Detox Kit (www.datadetoxkit.org).

## 3. Be smart about connected devices

Smart connected devices are everywhere in our lives: from home assistants to connected toys, fitness trackers and sensors in our cars. While they can be helpful, they can also collect and share your personal information.

Before you buy, take some time to research a product's security and privacy credentials. Look for trusted reviews or guides like Mozilla's **privacy not included* to help you decide which device is right for you.

Reading the privacy policy will help you understand how a device operates and whether you are comfortable with its data practices. Does it share your information with any third parties? How long is your personal information retained? If you're unsure, ask questions of the manufacturer or the retailer.

Adjust the privacy settings to reduce the amount of personal information that is collected. You may also be able to limit or stop the sharing of your personal information with any third parties.

While you may be comfortable with a car accessing your address book to help you safely take calls when driving, a smart fridge probably does not need to sync with your calendar in order to work. If the device has voice recognition, check whether it's listening all the time and how you can control the settings or delete the information.

Does your device always need to be switched on or connected to the internet? Limiting internet access or switching the device off when it is not in use will help protect your privacy. Remember to use a strong password and turn on automatic updates to keep the device secure.

## 4. Tracking your location

Your devices and apps may track your location by default unless you adjust your settings. This may be a necessary

part of the service if it is a navigation or ridesharing app, but you should think about whether the app you are installing needs location data or permissions to be turned on to work.

Your location data can be combined with other information about you to create a rich picture about who you are, where you go and what you like. For example, your location data might reveal how you travel to work, where you live, or how long you spend exercising each day.

An app's privacy notice should explain why it collects location data and how it is used, including whether it is shared with any third parties. If it's not clear who you're dealing with and what information they are collecting about you, then reconsider whether you really need the app at all.

You can also adjust the settings on your phone and other devices to limit or stop location tracking altogether. This might stop some apps working properly. You can also control each app's ability to access your location information. Your location can also be tracked when you browse the internet, so to limit this you can:

- Use a browser with an alternative privacy approach like Firefox or DuckDuckGo
- Use 'add-ons' or extensions that make it more difficult to track you online
- Regularly clear your cookies and cache
- Switch to a virtual private network (VPN).

## 5. Where's your data going?

When you visit a website or use an app, your device may be tracked using cookies and online identifiers. Cookies are small data files that are sent from a website to your device to record information such as settings or your browsing activity. An online identifier may be used to distinguish one person from another according to patterns of information generated by a device. They include internet protocol (IP) address, advertising ID, MAC address, pixel tag, account credentials and device fingerprints.

Cookies and online identifiers help websites and services to work more efficiently by remembering your preferences and settings. However, they can also be used to record your behaviour online and share information about you with third parties. For example, online tracking may enable ads to be shown to your device based on your browsing habits.

Your activity may also be tracked and recorded by social media sites and digital platforms like Facebook and Google. Depending on your privacy settings, and whether you log out of your profile, they can continue to track your activity when you leave the service or platform and visit other websites. You can adjust your habits and change your settings to limit activity tracking and help control your privacy by:

- Not browsing other websites or shopping online while logged into social media or a digital platform
- Deleting cookies in your browser settings or not accepting cookies when you navigate to a website
- Choosing your advertising preferences to limit ad tracking and resetting your advertising ID (see Apple and Google for more information).

## 6. The side effects of screen scraping

Screen scraping is a process where information from your screen is collected (or 'scraped') and made available to another application or website. It is sometimes referred to as Digital Data Capture and can be useful for consumers, such as when data from an old application is made available to a new application. It is sometimes used in the financial sector when a consumer directs a third-party service provider to access and recover their data from a web application.

However, when you agree to let a third party access your information via screen scraping you are also required to provide your log-in details, such as your username and password. This may not only breach security requirements or terms and conditions, it is also a significant privacy risk.

The new Consumer Data Right will provide a safe alternative to screen scraping. It allows you to access certain data about you held by businesses, and direct that your data is securely transferred to an accredited third party of your choice. The Consumer Data Right will be introduced in the banking sector in 2020 and will then be rolled out to other parts of the economy, including energy and telecommunications.

Personal information can also be 'scraped' from websites and digital platforms without permission, in a process known as web scraping. To help protect your personal data, check your privacy settings on social media and other online platforms, and consider limiting the amount of personal information like photos that you share online.

## 7. Shopping up a storm?

Almost three quarters of Australian households are now shopping online, so it's more important than ever to take practical steps to keep personal information safe. Breaches of your personal data including financial information can have serious consequences, like identity theft.

If you are signing up for a loyalty program or creating an online shopping account, remember that your personal information is valuable and should be protected. Consider checking out your shopping as a guest or leaving data fields blank to limit the amount of personal information the site collects and stores.

Know who you're buying from. Where possible, shop from reputable brands and cross-check information. This could include searching for reviews from other customers or reading information on warranty, refunds and complaints handling before making a purchase. If anything looks suspicious, don't risk it.

Only shop from secure websites – look for a URL starting with 'https' and a closed padlock symbol. When you are ready to buy, make sure you pay using a secure method like PayPal, BPay or your credit card. These offer dispute resolution processes if things don't go to plan.

If paying by PayPal, select the 'payment for goods/

services' option. If a seller instructs you to make the payment 'to friends and family' rather than 'payment for goods' this violates PayPal's policies and voids the buyer protections.

Fake ads are an increasing source of online scams, so watch out for offers that seem too good to be true. Fake retailer websites or online stores that offer luxury and other goods at a steep discount can appear legitimate. Payment methods like money order, pre-loaded money cards or wire transfer are another warning sign. Search for reviews from real users and don't trust a site just because it's been advertised on social media.

The ACSC (www.cyber.gov.au/acsc/view-all-content/advice/shopping-or-buying-online) offers more advice on how to shop safely online. For information on the latest scams and how to report them, visit the ACCC's Scamwatch (www.scamwatch.gov.au/report-a-scam).

## 8. Phishing for information

Malicious and criminal attacks are the leading cause of data breaches involving personal information, which can result in serious harm. Common cyber incidents include phishing and brute-force attacks, which use technology to generate millions of character combinations per second to try and crack passwords. These incidents can compromise your log-in details and potentially give people unauthorised access to your email and other online accounts.

Scammers can also use a range of sneaky tactics to extract your personal information and use it to steal your identity or commit fraud. For example, remote access scams try to convince you that you need to give an IT expert access to your computer, or buy and install new software to fix a problem.

Be alert for unexpected messages and requests for your personal details. Phishing messages can often feature branding and logos, or use similar language to well-known organisations, to appear 'real' and try to trick you into clicking on a link or attachment. Look out for requests to check or confirm login details, suspicious looking attachments, requests for money (especially with a sense of urgency), or where contact or bank details may have changed from previous, legitimate correspondence you received from the business.

If you're still in doubt, contact the organisation that the message claims to be from, using the contact details on their website or other official sources, not the contact details in the message you received.

Find out more about how to avoid phishing attacks from Scamwatch (www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing) and cyber.gov.au (www.cyber.gov.au/acsc/view-all-content/threats/phishing).

## 9. Protect kids' privacy online

Just like adults, many children are also spending more time online and are using a wide range of devices. Smart toys and fitness trackers, apps and social media accounts, phones and other devices can all capture your child's personal information, track their activity and create a lasting digital footprint. By keeping up with the latest apps, platforms and other technology you will be better placed to guide your child through the online environment and help protect their privacy.

At any stage, it's a good idea to talk about online safety and privacy issues and keep the lines of communication open. Encourage your child to safeguard their personal information, like their real name, address telephone number, school, and date of birth, and report any unexpected contact or notices.

Depending on your child's age, other strategies may include supervising screen time, limiting access to devices or setting parental controls. Adjusting privacy settings together can help your family control the information collected through webcams, microphones and cookies, as well as websites, apps, games and software. This is particularly important for social media and other digital profiles, to limit who can see your child's personal information. Other steps to protect your child's privacy include:

- Setting strong and unique passwords and not sharing them at school or online
- Securing mobile devices with a pin lock, or passcode
- Disabling geo-location services when they are not needed
- Only downloading apps from reputable sources
- Controlling cookies and the use of add-ons and ad-blockers

Visit the eSafety website (www.esafety.gov.au) for more advice about online technology and safety for parents, carers and children.

## 10. Clean up your email trail

In both our personal and professional lives, we frequently use email to send important information to others. This can include personal information about ourselves, such as financial and identity information. It can also include information about our family members or friends. Emails can remain in our accounts for extended periods of time if we don't actively delete them.

Our Notifiable Data Breaches report for July-December 2019 found that many cyber data breaches involved malicious actors gaining access to personal information stored in email accounts. The report also found that people often email personal information to the wrong recipient by mistake. To help you limit the risks with using emails:

- Use strong and unique passphrases for your email accounts to reduce the risk of your login details being compromised or stolen
- Regularly review and move your emails to a secure document management system or device
- Delete any emails from your inbox and sent box once they have been moved or are no longer needed
- If you are sending important information to another recipient, consider protecting your information using passwords or encryption.

---

Office of the Australian Information Commissioner. *Reboot your privacy and protect your personal information online.* Retrieved from www.oaic.gov.au on 22 June 2020.

# Your credit report is a key part of your privacy – here's how to find and check it

**The Privacy Act gives you the right to find out what's in your credit report and change any incorrect information in your report, advises Harjinder Singh, Nigar Sultana and Yeut Hong Tham**

The Australian government encourages citizens to protect their privacy and personal information. Most of the tips provided by the Office of the Information Commissioner are pretty intuitive – know your rights, read privacy policies, use security software and more. But you might be surprised to know "check your credit report" is also on the list of recommended actions.

Checking your credit report, preferably annually, is a good way to ensure incorrect information is not listed against you. Having the right information in place can protect you against identity theft, so is an important component of privacy in this sense.

The *Privacy Act 1988* is an Australian law which regulates the handling of personal information about individuals. The *Privacy Act* has very strict rules, reflected in 13 Australian Privacy Principles, that control the way information about you is accessed, used and corrected.

*Checking your credit report, preferably annually, is a good way to ensure incorrect information is not listed against you. Having the right information in place can protect you against identity theft, so is an important component of privacy in this sense.*

The *Privacy Act* gives you the right to find out what's in your credit report and change any incorrect information in your report.

As well as stopping others from stealing your identity, having an accurate credit report is also crucial if you want to borrow money. For example, when applying for credit such as a home loan, the lender will obtain your credit report to assess your credit worthiness and also your ability to repay the loan. You really don't

## WHAT STAYS ON A CREDIT REPORT?

| THIS TYPE OF INFORMATION | STAYS ON YOUR CREDIT REPORT FOR |
|---|---|
| **Bankruptcy** | The later of:<br>➤ 5 years starting on the day you became bankrupt, or<br>➤ 2 years starting on the day you were no longer bankrupt |
| **Court judgement** | 5 years |
| **Credit enquiry** | 5 years |
| **Current consumer credit obligations** | 2 years (from the end of the consumer credit) |
| **Debt agreement** | The later of:<br>➤ 5 years from the day the agreement was made.<br>➤ 2 years from the day the agreement was:<br>– Terminated<br>– Ends when the agreement ends under s 185N of the *Bankruptcy Act 1966*<br>– An order was made declaring the agreement void |
| **Default** | 5 years |
| **Repayment history** | 2 years |
| **Serious credit infringement** | 7 years |

Office of the Australian Information Commissioner. *What stays on a credit report?* Retrieved from www.oaic.gov.au on 19 June 2020.


want your application for a home loan to be knocked back because of errors in your credit report, do you?

## HOW TO CHECK YOUR CREDIT REPORT

The first step is getting a copy of your credit report. This can be obtained free from credit reporting agencies such as Equifax, illion and Experian. Tasmanians can also refer to the Tasmanian Collection Service. Make sure you spend a bit of time looking carefully for this free option – it is there, but can sometimes be a little buried.

The report will be sent to you in about ten days. If you are in a hurry and need it faster, you can pay between A$30 to A$50 dollars and the credit report will arrive in a day or two.

## LOOK AT THE DETAILS

Once you have your credit report, there are certain things that you must check. First, as a minimum, check that your personal details such as name, date of birth, employment and driver's license or other identifying documents are correct.

*As well as stopping others from stealing your identity, having an accurate credit report is also crucial if you want to borrow money.*

Second, have a look at your credit history in the report. This will include details of all credit or loans that you applied for, any overdue payments more than 60 days for which default actions have been initiated, and any other credit infringements. Such credit infringements can be listed on your credit report for between five to seven years, depending on their severity.

Third, examine your repayment history to determine whether you missed any payments on due dates.

Last, check whether any recorded serious adverse credit activities such as bankruptcies, court judgements and debt agreements are correct and accurately reflect your circumstances.

## WHAT HAPPENS IF IT'S WRONG?

You are entitled to request changes to any incorrect listing and this should be done free for you. In the first instance, you can contact the credit reporting agency directly and they will be able to fix small errors immediately. For other errors originating from a credit provider such as a bank, they will sometimes even contact the bank on your behalf.

However, if you have to contact the credit provider yourself, do so and explain why the listing is incorrect. Most often, they will fix the mistake. If they refuse, you can then go to an independent dispute resolution scheme, such as the Australian Financial Complaints Authority.

If all else fails, you can also contact the Office of the Australian Information Commissioner who will deal with your complaint if it is not older than a year.

So, what are you waiting for? It really is in your best interest to check your credit report, and no one else can do it for you.

**DISCLOSURE STATEMENT**

**The authors do not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and have disclosed no relevant affiliations beyond their academic appointment.**

**Harjinder Singh is Senior lecturer, Curtin University.**

**Nigar Sultana is Senior Lecturer, Faculty of Business and Law, Curtin University.**

**Yeut Hong Tham is Lecturer, Curtin University.**

THE CONVERSATION

Singh, H, Sultana, N and Tham, Y (17 May 2019). *Your credit report is a key part of your privacy – here's how to find and check it.* Retrieved from http://theconversation.com on 19 June 2020.

# DIY GENETIC TESTING CAN UNVEIL THE MYSTERY OF YOUR ANCESTRY – BUT WHAT HAPPENS TO YOUR DATA?

***As genetic testing becomes cheaper and easier, there's been a boom in companies offering do-it-yourself kits – but do you know what happens to your genetic data after sending it off for testing? Stephanie Smail reports for ABC Radio RN Breakfast***

Scientists, public health experts and lawyers are warning that while most of the tests are not for complex health analysis, there is a worrying lack of regulation around what happens to that data.

With the rise of companies like ancestry.com, there has been a surge in interest among the general public to uncover the information in their genes.

And now as well as ancestry, companies such as 23andMe are offering clients disease-based testing to look at whether their genes are predisposed to disease such as Alzheimer's. Amazon announced that in the last black Friday sales, 23andMe was one of their top five products, with sales going through the roof.

But in some countries like Germany, direct to consumer testing has been completely banned.

## HOW DOES IT WORK, AND WHAT ARE THE ETHICS?

Dr Nic Waddell from QIMR Berghofer Medical Research Institute said it could be as simple as a company sending you a small DIY kit to your house.

"You put saliva into a tube, you send that away and then they do a small DNA test," she said.

Dr Waddell has been leading a study looking into the ethical and legal implications of genetic testing.


She pointed out there were risks to consumers sending their DNA away without reading the fine print.

"You get people buying them for people as gifts for birthday presents and things – but in those sort of things it's always important to actually read the fine details," she said.

"Because in some instances the data that's generated by the companies, they may be keeping that data for a period of time, they may be sharing that data to different companies.

"It's always important just to be aware of what is happening to your samples and your data that's being generated."

## HOW MUCH INFORMATION DO YOU REALLY WANT?

Questions have also been raised around clinical testing. Scientists and doctors say whole genome testing delivers a raft of benefits, including driving the emerging field of so-called precision medicine that can tailor treatment to the genetic causes of cancer.

But Dr Waddell said it could also deliver more information than a patient might be prepared for. She has been investigating whether the right consent processes are in place to protect patients from getting unwanted information about other potential health problems.

"It all starts from when a patient first either consents to a research study or they consent to have routine genetic testing to find out a condition within them," Dr Waddell said.

"In that consent process they need to understand what the testing involves, they need to understand the benefits, the potential risks and disadvantages.

"But also have an understanding that other information about different diseases than the one they're undergoing testing or research for may crop up."

## WHO OWNS YOUR GENETIC DATA?

Then there are questions about who owns, manages and protects the data from genetic testing results. Dr Matthew Rimmer, a professor of intellectual property and innovation law at the Queensland University of Technology, said Australia has not had much success in developing human rights protections.

"Let alone specifically in terms of efforts to try and deal with new technologies," he said.

"So that has been problematic as genetic testing becomes much more widespread.

"It's kind of raised a whole host of *Gattaca*-style questions abut law and ethics and genetics."

But this is not a recent problem to crop up; Dr Rimmer said Australian policy makers have just taken too long to respond.

"It's a great tragedy in Australia that we've been very slow to mint laws to provide for adequate protection for individuals and consumers in respect of genetic privacy and genetic discrimination," he said.

During the 1990s, Australian Democrats senator Natasha Stott Despoja put forward a number of bills to try to provide greater protection. They included laws about genetic privacy to try and stop discrimination.

Dr Rimmer said the Australian Law Reform Commission handed down a "significant series of reports" on genetic privacy and genetic discrimination.

But he pointed out that there has been a lack of legislative action on the subject in Australia so far.

"So my concern is that as the genetic revolution moves on pace, Australia has been very slow to respond," he said.

## CAN YOU REQUEST TO HAVE IT DESTROYED?

Jane Tiller, a public health genomics adviser at Monash University, said while she supported people being able to access their genetic information, there was a general lack of regulation in place to protect consumers.

"The general guy off the street who's going online and getting a genetic test has difficulty knowing where that test is coming from," she said.

"Generally they're based overseas – there aren't a lot of tests offered in Australia as yet."

So when someone signs up, it is unlikely they will know where the company is based or where their data is being sent – or how much privacy their data will have.

"It's a great tragedy in Australia that we've been very slow to mint laws to provide for adequate protection for individuals and consumers in respect of genetic privacy and genetic discrimination."

Ms Tiller said though most genetic testing companies would destroy data upon request, many people have no idea that they have to request that.

She said the Federal Government needed to step up and start protecting consumers. Ms Tiller suggested the Australian Government should see the issue in a regulatory sense and collaborate with other regulators in other countries that are all facing similar issues.

"[And] talk about how they can do cross-regulation and how we can look at that in a more collaborative way," she said.

She said there was little information available to consumers, and what was available was often conflicting.

"So a system of accreditation or recognition where they could be kind of like a Heart Foundation tick," she said.

"Consumers could access [that] to know this is one that's meeting international accreditation standard – [that] would be a start."



Smail, S (28 February 2018). 'DIY genetic testing can unveil the mystery of your ancestry – but what happens to your data?', *ABC News*. Retrieved from www.abc.net.au/news on 22 June 2020.

# My Health Record: the case for opting out

**Katharine Kemp, Bruce Baer Arnold and David Vaile present the negative case for opting out of the government's My Health Record scheme**

Unless you take action to remove yourself from the My Health Record (MHR) system, the federal government will make a digital copy of your medical record, store it centrally, and, as the default, provide numerous people with access to it.

If you don't opt out during this period* and later choose to cancel your record, you will no longer be able to access that record but the government will continue to store it until 30 years after your death. You will need to trust that it will not be breached. There are three main problems with the MHR scheme.

## 1. IT CAN'T BE RELIED UPON AS A CLINICAL RECORD

Contrary to what many Australians may believe, MHR is *not* a clinically-reliable medical record, and was not designed to be. It is not up-to-date and comprehensive. As the Office of the Australian Information Commissioner (OAIC) points out:

*The My Health Record system contains an online summary of a patient's key health information; not a complete record of their clinical history.*

If, for example, a doctor were treating a child in an emergency, the doctor could *not* rely on an MHR to know what medications the child has been prescribed up to that date. In an emergency, an unreliable record is a distraction, not a help.

Many doctors have in fact objected to the incompleteness and lack of utility of the MHR. A recent poll on the AMA's doctors portal suggests 76% of respondents think the MHR will not improve patient outcomes while 12% think it will.

Notwithstanding this fundamental deficiency, the government is pushing ahead with an inherently risky scheme.

## 2. IT CREATES A SECURITY RISK

If you read the very long (7,800 words) privacy policy for MHR, you'll see that the Australian Digital Health Agency (ADHA) itself states there are risks from the online transmission and storage of our personal information in this system.

### *Health data is prized by hackers*

We have witnessed a stream of health data breaches in Australia and overseas, and the incentives for these breaches are only increasing.

Storing records digitally with online access greatly increases their accessibility for criminals, hackers and snoopers. Health records are valuable as a means of identity theft due to the wealth of personal information they contain. They are a huge prize for hackers, fetching a high price on the Dark Web.

### *You won't know who has seen it*

It won't just be your doctor who has access to this centralised digital record of your personal health information. The default position is that numerous people will have access – doctors, pharmacists, physiotherapists, nurses, and unidentified staff of various organisations.

MHR's access-logging system does not track which individuals are accessing records, only institutions, which means you won't be able to tell who has seen it. Even without a technical hack, that will make it almost impossible to keep your information secure in this system.

### *De-identification is risky*

The government is also planning to allow access to your health information for research purposes by "de-identifying" your information. That means the data should not be able to be linked to a particular individual.

But the national government has a bad record for successfully de-identifying health information.

In 2016, the government released a data set that included information on a large number of patients spanning 30 years. It was meant to be de-identified.

IT researchers at Melbourne University quickly demonstrated it could be re-identified and linked to the individuals concerned. Such re-identification risk will only grow, as data sets proliferate and tools get smarter.

### *Third-party access jeopardises security*

MHR also permits external health apps to access your records. According to the legislation, this should only be done with your consent.

Unfortunately, and predictably, health apps are already securing "consent" through obscure, standard form contracts so you might not be aware the app owner could sell your sensitive medical information to others.

Last month, the ABC revealed one such health app (HealthEngine) was selling patient information to law firms, so patients with serious conditions and injuries were contacted repeatedly by strangers pushing them to pursue legal claims. Many didn't know how their sensitive medical information was revealed.

The ADHA's website has published a report on the woefully inadequate privacy policies of mental health apps, and yet these apps might be authorised to access your MHR data with your supposed consent.

## 3. AN 'OPT-OUT' SCHEME GOES AGAINST BEST PRACTICE

Critically, the opt-out consent mechanism for MHR flies in the face of global best practice for informed consent – and our own federal privacy regulator's guidelines on the sort of consent necessary for use of health information.

Consent for use of personal information should be express, fully informed, easy to understand, and should require action on the part of the individual. MHR disregards all of those principles.

MHR does not seek your express consent. Instead, if you do not take the necessary steps before 15 October, your health records will automatically be copied, stored and shared.

You will also not be *fully informed*. There will be no national television, radio or print media campaign to advertise the MHR scheme, which many Australians have misunderstood in the past. The government will not even send you a letter to tell you about this scheme, let alone its very serious risks.

By contrast, the OAIC says organisations seeking individual consent to use personal information should generally:

*... ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent.*

and:

*... seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.*

Even if implied consent were acceptable (and it is not), the OAIC states further that an organisation:

*... should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.*

## THE TIME TO OPT-OUT IS NOW

MHR is likely to create very limited benefits for many, if not most, Australians. It creates unacceptable security risks for our most sensitive personal information. And the government's method of obtaining "consent" goes against international best practice.

If the MHR scheme were properly advertised, fully explained and Australians given a choice whether to opt-in, Australians could make an informed choice about whether the limited benefits justify the substantial risks to their sensitive information.

Those concerned about the security of their health information will need to take steps now to remove themselves from the MHR system.

*** Editor's note: The My Health Record opt-out period began on 16 July 2018 for an initial period of three months, however after broad community privacy concerns were raised, a Senate vote subsequently extended the period until 31 January 2019.**

**For people who did not opt out, their My Health Record was created after 31 January 2019. People can also choose to register for a My Health Record or cancel at any time.**

**This article has been updated to reflect that the ADHA report on the privacy policies of health apps focused on mental health apps.**

**DISCLOSURE STATEMENT**

**Katharine Kemp receives funding from The Allens Hub for Technology, Law and Innovation. She is a Member of the Advisory Board of the Future of Finance Initiative in India, the Centre for Law, Markets & Regulation and the Australian Privacy Foundation. Bruce Baer Arnold teaches health, consumer protection and privacy law. He has been the Australian representative on high-level OECD Health Data working parties. Dr Arnold is a Vice-Chair of the Australian Privacy Foundation. David Vaile is affiliated with the Australian Privacy Foundation (chair), Internet Australia (policy committee), NSW Law Society (privacy and data committee), Association of Market and Social Research Organisations (privacy code compliance committee) and AUSTRAC (privacy consultative committee), none of which stands to benefit from this article.**

**Katharine Kemp is Lecturer, Faculty of Law, UNSW, and Co-Leader, 'Data as a Source of Market Power' Research Stream of The Allens Hub for Technology, Law and Innovation, UNSW.**

**Bruce Baer Arnold is Assistant Professor, School of Law, University of Canberra.**

**David Vaile is Teacher of cyberspace law, and leader of the Data Protection and Surveillance stream of the Allens Hub for Technology Law and Innovation, UNSW Faculty of Law, UNSW.**

THE CONVERSATION

Kemp, K, Arnold, B.B, and Vaile, D (16 July 2018). *My Health Record: the case for opting out.* Retrieved from http://theconversation.com on 19 June 2020.

# My Health Record: the case for opting in

## JIM GILLESPIE PRESENTS THE AFFIRMATIVE CASE FOR OPTING IN TO THE GOVERNMENT'S MY HEALTH RECORD SCHEME

**Editor's note: The My Health Record opt-out period began on 16 July 2018 for an initial period of three months, however after broad community privacy concerns were raised, a Senate vote subsequently extended the period until 31 January 2019.**

**For people who did not opt out, their My Health Record was created after 31 January 2019. People can also choose to register for a My Health Record or cancel at any time.**

The My Health Record (MHR) system promises to make Australia a leader in providing citizens with access to their own health records.

The scheme gives health care professionals access to information on your medications and allergies, immunisation records, summaries of hospital and GP care, investigation reports, and advance care plans.

This information could save lives in emergencies by providing health workers with information about drug allergies, medications, and medical history. Better continuity in the management of this information would help reduce the 27% of clinical incidents in Australian hospitals currently caused by medication (mis)management.

### The system had a rocky start

Launched in 2012 as the Personally Controlled Electronic Health Record (PCEHR), the system was plagued by technical failures and cost overruns. Take-up was low.

After five years, only 20% of consumers had opted in. Even more seriously, there was limited interest from health professionals – particularly GPs and pharmacists who deal with patients most often.

Faced with the low patient take-up and limited training or information, health professionals saw little reason to waste time on an unwieldy system. This mirrored international experience. Many countries suffered expensive disasters in building e-health systems from the top down. E-health appeared to serve the interests of administrators, not clinicians and patients.

Not surprisingly, patients showed little interest. British critics of a similar expensive failure warned:

*We need fewer grand plans and more learning communities.*

The Australian experience has run the full gamut from failed top-down "grand plan" to a version that is more responsive to consumers and health professionals.

### Linking up the fragmented health system

Large trials in the Nepean-Blue Mountains and North Queensland Primary Health Networks tested a more user-friendly system. In both trials, the opt-out rate was low: less than 2%. The engagement of clinicians also increased.

In the Blue Mountains fewer than 15% of GPs had registered with the PCEHR. By the end of the trial, with extensive education and training, this figure has risen to 70%.

MHR offers new possibilities for linking up the fragmented health system, making it easier to navigate. Just as importantly, it can help you to become more informed and engaged with your own health care. And better health literacy is a necessary step in shifting the balance of the system towards patients.

The Consumers' Health Forum – a supporter of MHR – has stated that patients are:

*... more likely to give permission to share their data if they understand how their data will be used and any benefits that will come from its use.*

However, active participation in MHR will remain a challenge for many people, especially those who struggle with digital literacy.

### Addressing security concerns

Any system that contains health information must be built on trust. Most of the criticisms of MHR rest on fears of inappropriate use or hacking of data. However, critics have not pointed to any breach of the PCHR


in its five years of operation. Rather, examples are often drawn from commercial operations which have succumbed to the temptation to commercialise data – an offence that could lead to prison under MHR.

Uncertainty is inherent in many facets of modern life, such as the use of credit card information for online purchases. Most surveys of popular attitudes towards the use of digital health information has shown a consistent, but nuanced concern.

Concerns identified in the two major trials were mainly focused on individuals' lack of computer skills. But almost all consumers thought the benefits greatly outweighed any potential privacy risks.

The system will only succeed if concerns about protection of confidentiality are respected. A weak link is the digital skills and awareness of health practitioners, particularly GPs.

A large amount of health data is already out there in Medicare Benefits Schedule (MBS) and Pharmaceutical Benefits Scheme (PBS) data, the Australian Immunisation Register, and the Australian Organ Donor Register. These data are increasingly linked together, with great potential benefits. Data from Medicare, hospital records and other sources can be linked to improve our knowledge of causes of diseases and risk factors, and the best forms of intervention.

## MHR is a step toward empowering patients

Our health system suffers from a deficit of transparency. Patients are locked out of knowledge of how the system works – from the confusion around private health insurance plans to undisclosed out-of-pocket costs for medical procedures.

Rather than protesting about a horse that has long since bolted, we need more scrutiny and improvement of current systems.

MHR is a small step towards empowering patients with greater knowledge about their health. Pressures to present records in terms that are comprehensible to consumers may even take us towards interactive "learning communities" – the basis of a more people-centred health system. Better-informed patients can enable more effective communication and mutual learning from health professionals.

If you choose not to opt out of MHR, a record will be created for you automatically. You can log into the system at www.myhealthrecord.gov.au to set controls on who has access to your data and set restrictions on the types of data that will be included. You can change your mind at any time and close access to your data.

**DISCLOSURE STATEMENT**

**Jim Gillespie has received funding from the National Health and Medical Research Council and WentWest/ Western Sydney Primary Health Network.**

**Jim Gillespie is Deputy Director, Menzies Centre for Health Policy & Associate Professor in Health Policy, University of Sydney.**

THE CONVERSATION

Gillespie, J (16 July 2018). *My Health Record: the case for opting in.* Retrieved from http://theconversation.com on 19 June 2020.

# COVIDSAFE APP AND MY PRIVACY RIGHTS

**The information in this article from the OAIC describes how the Privacy Act applies to the Australian Government's controversial COVIDSafe app**

### *What is the COVIDSafe app?*

The COVIDSafe app is part of the Australian Government's response to the COVID-19 pandemic and assists with contacting people who may have been exposed to the virus. Please visit the Department of Health website (www.health.gov.au/resources/apps-and-tools/covidsafe-app#about-the-app) for more information about the app.

### *Can someone make me use the COVIDSafe app?*

No. The app is voluntary. Whether or not you choose to download and use the app is entirely your choice. You cannot be required to download or use the app. If the app has been installed on a device you use at your workplace, your employer should delete the app upon your request.

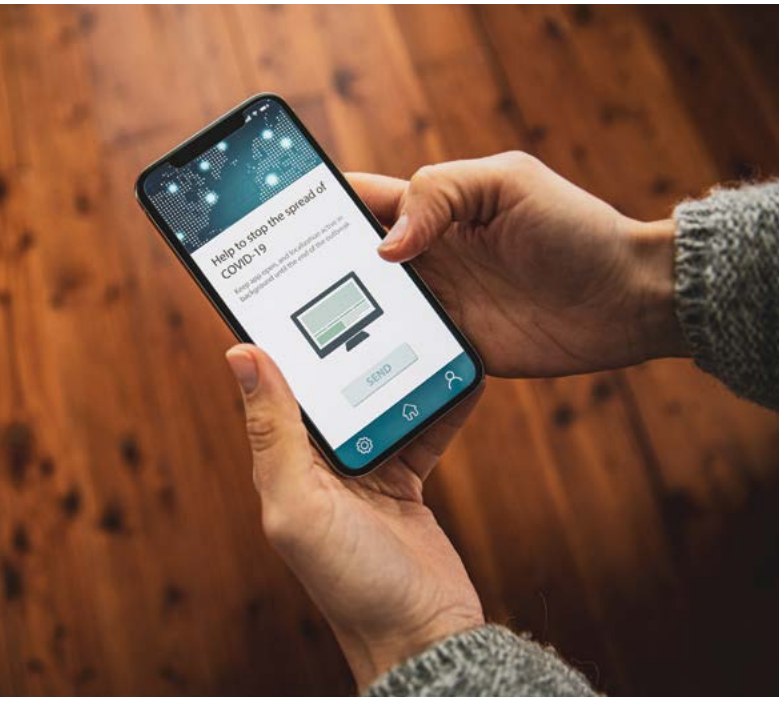
It is an offence under the *Privacy Act* for any individual, organisation or government agency to require you to download or use the app. However, this does not apply to private citizens in their personal lives. For example, it is not an offence if a relative or friend asks you to download the app before visiting their home.

### *What if someone tells me that I am required to download the app?*

You cannot be required to download or use the COVIDSafe app to take part in an activity or provide or receive a good or service.

This means that:

- A business cannot charge you more for a product or service just because you are not using the app
- A school cannot require students to use the app to attend on-site lessons
- A restaurant cannot refuse you service just because you don't have the app
- A landlord cannot require a tenant to download the app
- An airline cannot refuse to let you fly just because you don't have the app
- Your employer cannot dismiss you, alter your position to your detriment, stop you entering your workplace, or pay you less just because you don't have the app (even if you are using a work-issued phone)
- Your sporting club cannot stop you from playing just because you don't have the app.




If you have been told that you need to download or use the COVIDSafe app, you can lodge a complaint with us (www.oaic.gov.au/privacy/privacy-complaints/).

### *If I get the COVIDSafe app, what information will be collected about me?*

If you download and register to use the COVIDSafe app, you will be asked to supply some registration information.

You will need to provide your:

- Name (or a pseudonym)
- Mobile phone number
- Age range
- Postcode.

This information will ensure your state or territory health authority has your details if you have been in contact with someone with the virus, and that people who are vulnerable are contacted first. Contact tracers will determine your risk category according to your age and proximity to a known cluster.

The National COVIDSafe Data Store, which is administered by the Digital Transformation Agency, will send your phone a new user ID every two hours. The user ID will be automatically encrypted and stored in the app on your phone. The user ID will also be stored in the National COVIDSafe Data Store.

The app will use Bluetooth signals every minute to detect and record details of phones nearby which are also using the COVIDSafe app. This process is called a 'digital handshake'. The app does not use GPS or any other location-tracking system and does not record your (or anybody else's) location.

The app will collect the following information about all digital handshakes it has made with other phones:

- Make and model of the phone
- Date and time of contact
- Bluetooth signal strength
- The phone's encrypted user ID.

The app stores this data on your phone for 21 days, then automatically deletes it. However, if you test positive to COVID-19 and agree to upload the data on your phone to the National Data Store, this data will remain in the Data Store to assist contact tracers until it is no longer required by the contact tracers, and will be deleted once the Health Minister determines that the COVIDSafe app is no longer needed.

The app will not collect the name, phone number, age or postcode of other people, or any location information.

While you have the app on your phone, your digital handshake information will be sent to the phone of other COVIDSafe users, if you are close enough. If you delete the app, it will stop exchanging digital handshakes with other COVIDSafe users and delete any digital handshakes collected by the phone and not uploaded to the Data Store.

You can read more about what information is collected in the COVIDSafe App Privacy Policy (https://covidsafe.gov.au/privacy-policy.html).

### *How will the COVIDSafe app protect people?*

The COVIDSafe app is a tool to help speed up the process of tracing and contacting people who have potentially been exposed to the virus.

Contact tracing will occur whether or not you have the app. However, the app can make this process easier and more reliable because it does not rely on your memory of who you have been in contact with and will collect contacts from people you may not know.

The app will not protect you from catching the virus and it will not alert you in real time if you come close to someone who has the virus. You must practise appropriate physical distancing and good hygiene, whether or not you have the COVIDSafe app.

# Using mobile apps: the ABCs of privacy protection

## Fact sheet courtesy of the Information and Privacy Commission NSW

**The ABCs of privacy protection provides a few simple steps to follow to help you protect your privacy when you download and use mobile apps on smartphones and tablets.**

Mobile apps are becoming a huge part of our everyday lives. From checking the weather and getting real-time news and transport updates, to shopping and playing games, there seems to be an app for almost everything!

Keeping your personal details private should always be a top priority when using apps on your smartphones and tablets. The good news is there are things you can do to help protect your privacy. Just remember the ABCs next time you download an app to ensure your information is protected.

### KNOW YOUR ABCS

1. ALWAYS check what information the app is collecting, and what it will do with it. If it seems excessive, reconsider whether you really need the app.
2. BE AWARE of apps that share information online. For example, some apps might post your exact location, or publish photos you've taken online without you knowing about it.
3. CHECK the reviews before you download an app. No reviews or only positive reviews all sounding the same may mean you should take extra care with any information you are asked to provide.
4. NSW privacy law requires public sector agencies, including councils and universities, health service providers and certain businesses to be upfront about what they are doing with any personal information they collect in their privacy statement. This includes any personal information collected through a mobile app.

We always encourage you to read the privacy policy or statement whenever you are asked to provide personal information, and make sure you are able to refuse particular sharing services if you wish to. These services may include the sharing of posts between social media sites.

You should also be able to easily delete or deactivate an app at any time. We suggest you consider regularly deleting any apps you don't use.

If you're thinking of developing an app, or you are interested in finding out more about the obligations of organisations in relation to the protection of users' personal information, please view the IPC's fact sheet on *Developing Mobile Apps: know the risks* agency checklist, available to download at www.ipc.nsw.gov.au.

### *For more information*

Contact the Information and
Privacy Commission NSW (IPC):
Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

**NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.**

Information and Privacy Commission NSW. *Using mobile apps: the ABCs of privacy protection* (Updated August 2019). Retrieved from www.ipc.nsw.gov.au on 22 June 2020.

### How does the Privacy Act protect the information collected through the COVIDSafe app?

The *Privacy Act* was amended on 14 May 2020 to protect data in the COVIDSafe app and the National COVID Safe Data Store. The *Privacy Act*:

- Prohibits anyone being required to download or use the app
- Strictly limits the purposes for which data from the app can be collected, used or disclosed
- Requires data to be deleted when it is no longer needed.

Information that has been collected or generated through the COVIDSafe app can only be collected, used or disclosed by:

- State or territory health officials who are contact tracing individuals possibly exposed to COVID-19
- The administrators of the COVIDSafe app and the National COVIDSafe Data Store, to enable the app, the Data Store and contact tracing to work properly and to ensure the integrity of the app and Data Store
- The Office of the Australian Information Commissioner and police enforcing these privacy protections.

Information that has been collected or generated through the COVIDSafe app cannot be accessed by police, or used in court proceedings, except where the suspected crime is a breach of Part VIIIA of the *Privacy Act*. The National COVIDSafe Data Store is held in Australia, and it is an offence for the data to be retained or sent overseas.

### What happens if my information is sent to a state or territory health department?

Information about you that is sent from the National COVIDSafe Data Store to a state or territory health department is still protected by the *Privacy Act*.

Information that a state or territory health department collects about you by any other method is not subject to the *Privacy Act*. For example, if someone you work with is diagnosed with COVID-19, they may tell a state or territory contact tracing team about any colleagues they have been in close contact with. This would happen whether or not you have the app.

Any information that has not come from the National COVIDSafe Data Store must be handled in line with the privacy law that applies in that state or territory. For example, if a contact tracing team calls you to ask for more information, the information you provide directly to them will be covered by the privacy law that usually applies to that state or territory health department.

### When will my data be deleted?

The data held in your app about your close contacts (its record of 'digital handshakes') is automatically deleted once it is more than 21 days old.

You can delete the app from your phone at any time. This will delete all digital handshakes from your phone and will stop your phone creating any new digital handshakes.

You can also request the deletion of your registration data (your name, mobile phone number, age range and postcode) and your record of close contacts from the National COVIDSafe Data Store, using this online form (https://covidsafe-form.service.gov.au).

You cannot ask for your 'digital handshake' data, which may be held in the National COVIDSafe Data Store as a result of other users uploading their close contacts, to be deleted. However, if your registration information is deleted this means that any digital handshakes that are uploaded to the National COVIDSafe Data Store by others who you have come into close contact with will not be able to be linked back to you.

Once the Health Minister has determined that the COVIDSafe app is no longer needed to prevent or control the spread of the virus, all data in the National COVIDSafe Data Store will be deleted as soon as is reasonably practicable, and users will be informed.

### Who is enforcing the privacy protections for the COVIDSafe app?

The OAIC has an independent oversight function under the *Privacy Act*, and is actively monitoring and regulating compliance with the *Privacy Act* which governs the COVIDSafe app.

We have powers to:

- Conduct audits
- Investigate complaints
- Order compensation to be paid to individuals who suffer from an interference with their privacy
- Seek civil penalties against individuals and organisations which breach the law
- Refer matters to the police if we think a crime has been committed
- Refer matters to state and territory privacy regulators if appropriate.

### How can I make a privacy complaint?

If you believe that any individual or organisation has breached the new COVIDSafe app law, you can:

- Make a complaint to the OAIC and/or
- Make a complaint to the Australian Federal Police (www.afp.gov.au/contact-us/report-commonwealth-crime).

For more information about how to make a complaint to the OAIC, see www.oaic.gov.au/privacy/privacy-complaints.

### Where can I find out more?

- For more information about how the COVIDSafe app works, visit the Department of Health's COVIDSafe app website at www.health.gov.au/resources/apps-and-tools/covidsafe-app.
- For more information about how the *Privacy Act* applies to the COVIDSafe app, please contact us through our online enquiries form or phone 1300 363 992.

---

Office of the Australian Information Commissioner. *The COVIDSafe app and my privacy rights.* Retrieved from www.oaic.gov.au on 22 June 2020.

# EXPLORING ISSUES

## WORKSHEETS AND ACTIVITIES

The Exploring Issues section comprises a range of ready-to-use worksheets featuring activities which relate to facts and views raised in this book.

The exercises presented in these worksheets are suitable for use by students at middle secondary school level and beyond. Some of the activities may be explored either individually or as a group.

As the information in this book is compiled from a number of different sources, readers are prompted to consider the origin of the text and to critically evaluate the questions presented.

Is the information cited from a primary or secondary source? Are you being presented with facts or opinions?

Is there any evidence of a particular bias or agenda? What are your own views after having explored the issues?

## CONTENTS

**Brainstorm, individually or as a group, to find out what you know about protecting your privacy.**

1. **What is privacy, and why is it important?**

2. **What are the Australian Privacy Principles, and how many are there? Provide some examples.**

3. **What is CCTV, and how can it be used for surveillance?**

4. **Explain the term 'biometric scanning'. Provide some examples.**

5. **What is 'web scraping'? Provide some examples.**

**Complete the following activities on separate sheets of paper if more space is required.**

*"Facial recognition technology is increasingly being trialled and deployed around Australia."*

Sarre, R, *Facial recognition technology is expanding rapidly across Australia. Are our laws keeping pace?*

**Write one to two paragraphs discussing facial recognition technology. Describe what it is and how it can be applied, and outline your thoughts on its uses. Include whether you feel it could be seen as an invasion of privacy and whether there are any positives and/or harms associated with it.**

*"Privacy is an important issue for most Australians. Seventy per cent consider the protection of their personal information to be a major concern in their life."*

OAIC, *Australian Attitudes to Privacy Survey 2020.*

**Refer to the report findings for the Australian Community Attitudes to Privacy Survey 2020. In one to two paragraphs, explain respondents' concerns relating to the five (5) biggest privacy risks identified:**

**Identity theft and fraud:**

**Data security and data breaches**

**Digital services, including social media sites**

**Smartphone apps**

**Surveillance by foreign or Australian entities**

*"Known as the 'privacy paradox': people say they want to protect their data privacy online, but often do little to keep it safe."*

Mitchell, V, and Kamleitner, B, *We don't own data like we own a car – which is why we find data harder to protect.*

**Write one to two paragraphs expressing your understanding of the concept of the 'privacy paradox'. Describe what it is, who it affects, and why you believe it exists. Illustrate your response with some examples of the privacy paradox in action.**

**Complete the following multiple choice questionnaire by circling or matching your preferred responses. The answers are at the end of this page.**

1. **Which of the following is information that stays on a credit report? Select any that apply.**

a. Social Security payments
b. Repayment history
c. Bank account details
d. Credit enquiries
e. Credit infringements
f. Current credit obligations
g. Court judgements
h. Bankruptcy

2. **Which of the following are some of the best ways to keep your online accounts secure? Select any that apply.**

a. Enable two-factor authentication
b. Keep your passwords stored on your device
c. Use strong and unique passwords
d. Use a reputable password manager
e. Use your date of birth as a password
f. Keep a copy of your passwords on someone else's device
g. Enable automatic software updates

3. **What purpose was the COVIDSafe app developed for in Australia?**

a. To be used as a tool to test people for COVID-19
b. To track the movements of all Australians at all times
c. To assist in tracing and contacting people potentially exposed to COVID-19
d. To be used to record all medical information for people who test positive for COVID-19
e. To enable people with COVID-19 to communicate with each other
f. To be used as an 'information only' resource for COVID-19 safety

4. **Pilots of commercial drones need to be registered with the Civil Aviation Safety Authority once their drone exceeds what weight?**

a. 100g
b. 250g
c. 500g
d. 1kg
e. 2kg
f. 5kg

5. **Which of the following are examples of personal information? Select any that apply.**

a. Name and address
b. IP address
c. Mobile phone location
d. Computer model
e. Photographs
f. Credit card information

## MULTIPLE CHOICE ANSWERS

1 = b, d, e, f, g, h ; 2 = a, c, d, g ; 3 = c ; 4 = e ; 5 = a, b, c, e, f.

- The *Privacy Act 1988* (Privacy Act) covers how your personal information is handled by Australian Government agencies and any organisation with an annual turnover of more than $3 million, and some other organisations (OAIC, *Privacy and personal information*). (p.1)
- There are 13 Australian Privacy Principles and they govern standards, rights and obligations around: the collection, use and disclosure of personal information, an organisation or agency's governance and accountability, integrity and correction of personal information, and the rights of individuals to access their personal information (OAIC, *Australian Privacy Principles*). (p.4)
- Australian data privacy laws are generally weak when compared with those in the United States, United Kingdom and the European Union. They fall short in both specific exemptions for politicians, and because individuals cannot enforce laws even where they do exist (Vaile, D, *Australia should strengthen its privacy laws and remove exemptions for politicians*). (p.5)
- All political parties use databases to engage with voters, but they're exempt from privacy laws so there's no transparency about what anybody's doing (*ibid*). (p.5)
- Even if you have your number listed on the Do Not Call Register, a political party or candidate can authorise a call to you, at home or at work, if one purpose is fundraising (*ibid*). (p.6)
- A recent report explained how companies most of us have never heard of – data aggregators, data brokers, data analysts, and so on – are trading in our personal information (Kemp, K, *Here's how tech giants profit from invading our privacy, and how we can start taking it back*). (p.8)
- Google uses location data to work out demographic information, target advertising, and offer advertising services to other businesses (Kemp, K, *The ACCC is suing Google over tracking users. Here's why it matters*). (p.9)
- In July 2019, the US Federal Trade Commission settled with Facebook on a US$5 billion fine for repeatedly misleading users about the fact personal information could be accessed by third-party apps without the user's consent, if a user's Facebook 'friend' gave consent. Facebook's share price went up after the FTC approved the settlement (*ibid*). (p.10)
- In 2014, Facebook users were offered an app called "This is Your Digital Life", which paid users to take a personality quiz. The app harvested the data not only of the person taking the quiz but also of their Facebook friends, who had no knowledge of the app or the data collection. The app developer then sold that information to a political lobbying company, Cambridge Analytica, which used the personal data for political profiling (Manwaring, K and Kemp, K, *Australia's privacy watchdog is taking Facebook to court. It's a good start*). (p.11)
- An organisation or agency may only scan your identity documents (ID) if it's reasonably necessary for their business activities. If your ID contains sensitive information you must also consent to the scanning (OAIC, *Surveillance and monitoring*). (p.16)
- Artificial intelligence can analyse CCTV video footage without human input (Bunn, A and Thompson, N, *Australians accept government surveillance, for now*). (p.19)
- When face recognition is used to identify suspects, there are often multiple records of images of people who are a close match to the suspect. This can result in a high error rate, posing a risk that innocent people are accused of criminality and wrongdoing (*ibid*). (p.19)
- Pilots of commercial drones weighing 2 kilograms or more need to be registered with the Civil Aviation Safety Authority and have an operator's certificate before their remotely piloted aircraft goes zipping through the public airspace (CHOICE, *Drones and Australian law*). (p.24)
- Surveillance is much more than just CCTV. It now includes things like private home or business security systems, police body-worn cameras and the use of helicopters and drones. And we all have the capacity to conduct surveillance and gather evidence using the technology contained in our mobile phones (Goldsworthy, T, *Big brother is watching: how new technologies are changing police surveillance*). (p.27)
- CCTV footage is highly valued by law enforcement personnel, with 90% of investigators using the footage when it was available (*ibid*). (p.27)
- Many police services are using drones for tasks such as crowd management, surveillance and target acquisition. Queensland and Victoria are just 2 states that are committed to the use of drones for policing purposes (*ibid*). (p.28)
- Privacy is an important issue for most Australians. 70% consider the protection of their personal information to be a major concern in their life (OAIC, *Australian Community Attitudes to Privacy Survey*). (p.35)
- The biggest privacy risks identified by Australians in 2020 are: identify theft and fraud (76%); data security and data breaches (61%); digital services, including social media sites (58%); smartphone apps (49%); and surveillance by foreign entities (35%) or Australian entities (26%) (*ibid*). (p.35)
- 3 in 5 Australians (59%) have experienced problems with how their personal information was handled in the past 12 months. The majority involved unwanted marketing communications or having their personal information collected (with or without consent) when this was not required to deliver the service (*ibid*). (p.35)
- Cookies and online identifiers help websites and services to work more efficiently by remembering your preferences and settings. However, they can also be used to record your behaviour online and share information about you with third parties (OAIC, *Reboot your privacy and protect your personal information online*). (p.40)
- Health records are valuable as a means of identity theft due to the wealth of personal information they contain. They are a huge prize for hackers, fetching a high price on the Dark Web (Kemp, K, Arnold, B.B, and Vaile, D, *My Health Record: the case for opting out*). (p.46)

# GLOSSARY

**Australian Privacy Principles**
The APPs are the cornerstone of the privacy protection framework in the *Privacy Act 1988*. There are 13 Australian Privacy Principles and they govern standards, rights and obligations around: the collection, use and disclosure of personal information; an organisation or agency's governance and accountability; integrity and correction of personal information; and the rights of individuals to access their personal information.

**Biometric scanning**
Biometric information scanning is when an organisation or agency takes an electronic copy of your biometric information, which includes any features of your: face, fingerprints, iris, palm, signature, or voice.

**Closed-circuit television (CCTV)**
CCTV is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.

**Do Not Call Register**
Even if you have your number listed on the Do Not Call Register, a political party or candidate can authorise a call to you, at home or at work, if one purpose is fundraising. It also permits other uses.

**Drone**
An unmanned aerial vehicle which can be fully or partially autonomous, but which is more often controlled remotely by a human pilot, and often carrying a camera. Several laws cover the use of drones in Australia.

**Hacking**
Occurs when a scammer gains access to your personal information by using technology to break into your computer, mobile device or network.

**ID scanning**
When an organisation or agency takes an electronic copy of a document that proves your identity, such as your driver licence.

**Information privacy**
Relationship between the collection and dissemination of data, technology, the public expectation of privacy, legal and political issues surrounding them. Also known as data privacy or data protection.

**Personal information**
The *Privacy Act* defines personal information as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'

**Phone hacking**
Practice of intercepting telephone calls or voicemail messages, often by accessing the voicemail messages of a mobile phone without the consent of the phone's owner.

**Privacy**
The interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations. Privacy has several dimensions: privacy of the person (sometimes referred to as 'bodily privacy'), privacy of personal behaviour, privacy of personal communications, and privacy of personal data (sometimes referred to as 'data privacy' and 'information privacy').

**Privacy Act**
The *Privacy Act 1988* regulates how your personal information is handled. For example, it covers how your personal information is collected, how it is then used and disclosed, its accuracy, how securely it is kept, and your general right to access that information.

**Privacy paradox**
The discrepancy between an individual's intentions to protect their privacy and how they actually behave in the online marketplace.

**Privacy protection**
Process of finding appropriate balances between privacy and multiple competing interests.

**Right to privacy**
An element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals.

**Spam Act**
Under the *Spam Act 2003*, organisations cannot email you advertisements without your request or consent. They must also include an unsubscribe notice at the end of a spam message, which allows you to opt out of unwanted repeat messaging. However, the Act says that it has no effect on "implied freedom of political communication".

**Surveillance**
Monitoring of behaviour, activities, or information for the purpose of information gathering, influencing, managing or directing. This can include observation from a distance by means of electronic equipment, such as closed-circuit television, or interception of electronically transmitted information, such as internet traffic.

**Surveillance capitalism**
Refers to an economic system centred around the commodification of personal data with the core purpose of profit-making.

**Web scraping**
Process of automatically mining data or collecting information from the World Wide Web.

## Websites with further information on the topic

Access Now www.accessnow.org/issue/privacy
Australian Cyber Security Centre www.cyber.gov.au
Australian Human Rights Commission www.humanrights.gov.au
Australian Privacy Foundation www.privacy.org.au
Civil Liberties Australia www.cla.asn.au
Digital Rights Watch www.digitalrightswatch.org.au
Information and Privacy Commission New South Wales www.ipc.nsw.gov.au
Liberty Victoria https://libertyvictoria.org.au
Office of the Australian Information Commissioner www.oaic.gov.au
Office of the Information Commissioner Northern Territory https://infocomm.nt.gov.au
Office of the Information Commissioner (WA) www.oic.wa.gov.au
Office of the Victorian Information Commissioner https://ovic.vic.gov.au
Privacy International www.privacyinternational.org
Queensland Council for Civil Liberties www.qccl.org.au
The Conversation Australia https://theconversation.com/au

### ACKNOWLEDGEMENTS

The publisher is grateful to all the contributors to this book for granting permission to reproduce their works.



### ILLUSTRATIONS AND PHOTOGRAPHS

Photographs and illustrations courtesy of iStock, except cartoon on page 7 by Helen J. Robinson/The Conversation, cartoons on pages 11 and 33 by Angelo Madrid, cartoon on page 18 by Simon Kneebone, infographic on page 38 © Office of the Australian Information Commissioner, and cartoon on page 44 by Don Hatcher.

### THANK YOU

- The Conversation Australia
- Office of the Australian Information Commissioner.

# INDEX