|  |
| --- |
| Privacy and personal data  Emerging issues in media  and communications |
| Occasional paper 4 |
| June 2013 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Canberra**  Purple Building  Benjamin Offices  Chan Street  Belconnen ACT  PO Box 78  Belconnen ACT 2616  T +61 2 6219 5555  F +61 2 6219 5353 | **Melbourne**  Level 44  Melbourne Central Tower  360 Elizabeth Street Melbourne VIC  PO Box 13112  Law Courts  Melbourne VIC 8010  T +61 3 9963 6800  F +61 3 9963 6899 | **Sydney**  Level 5  The Bay Centre  65 Pirrama Road  Pyrmont NSW  PO Box Q500  Queen Victoria Building  NSW 1230  T +61 2 9334 7700  1800 226 667  F +61 2 9334 7799 |  |  | |
| © Commonwealth of Australia 2013  This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced  by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction  and rights should be addressed to the Manager, Editorial Services, Australian Communications and Media Authority,  PO Box 13112 Law Courts, Melbourne Vic 8010.  Published by the Australian Communications and Media Authority |

[Introduction 3](#_Toc359574745)

[Evolution of the personal data environment 5](#_Toc359574746)

[Sophisticated devices support rich data collection 6](#_Toc359574747)

[Software exploits device capabilities to capture a range of personal data 7](#_Toc359574748)

[Advances in network coverage and capacity aid personal data collection and storage 8](#_Toc359574749)

[Data collection and analytics processes 8](#_Toc359574750)

[Evolving for technical tools and privacy-enhancing services 10](#_Toc359574751)

[Personal data vaults 10](#_Toc359574752)

[Personal data monitors 11](#_Toc359574753)

[Anonymisers 11](#_Toc359574754)

[Changing definitions of personal information in the networked digital environment 11](#_Toc359574755)

[Citizens’ attitudes to digital data sharing and security 13](#_Toc359574756)

[Digital identity an enduring concept 13](#_Toc359574757)

[Citizens have concerns about electronic intrusions 15](#_Toc359574758)

[Citizens are concerned about financial loss 15](#_Toc359574759)

[Managing reputation 16](#_Toc359574760)

[Managing location activities 17](#_Toc359574761)

[Malicious activity risks to personal data 17](#_Toc359574762)

[Shared responsibilities 17](#_Toc359574763)

[Implications for regulatory settings 19](#_Toc359574764)

[Economy-wide and industry-specific regulation 19](#_Toc359574765)

[Communications-specific protections 20](#_Toc359574766)

[Identity of communications customers 21](#_Toc359574767)

[Location activity information 21](#_Toc359574768)

[Protections against electronic intrusions 21](#_Toc359574769)

[Reputation 22](#_Toc359574770)

[Emerging gaps in personal data protections 22](#_Toc359574771)

[Implications for informed consent 23](#_Toc359574772)

[Unattended and poorly attended risks 23](#_Toc359574773)

[Coherent frameworks for identification and authentication techniques 23](#_Toc359574774)

[Whole-of-economy governance and oversight 24](#_Toc359574775)

[A coherent strategy is required to manage personal data in the digital environment 24](#_Toc359574776)

[Enabling strategies for the personal information environment 27](#_Toc359574777)

[Communication strategies 27](#_Toc359574778)

[Facilitation of industry co- and self-regulation 27](#_Toc359574779)

[Direct regulation will continue to play an important role where it can be meaningfully applied 29](#_Toc359574780)

[Conclusion 31](#_Toc359574781)

[Appendix 1 32](#_Toc359574782)

[ACMA research relating to privacy and personal data protection 32](#_Toc359574783)

Executive summary

The evolution of the online environment from a medium for passive content consumption to one of constant connectivity and interaction is having a dramatic impact on the amount and types of personal information disclosed by citizens and consumers. According to veteran internet observer, Clay Shirky, of all recorded information created in human history, most of it has been created since 2010.[[1]](#footnote-1)

Developments in consumer and industrial devices and the networks that connect them have enabled this near-continuous collection of personal and behavioural data. A variety of software applications, including social networking sites, mobile device apps and online behaviour tracking ‘cookies’, are exploiting these device capabilities and generating substantial volumes of rich data about the social and economic activities of individuals—both online and offline. Organisations are increasingly looking to personal and behavioural data for insights that will drive more effective marketing practices and improve service delivery efficiency. In combination, these developments have created a personal data environment that is vastly different from that which characterised the pre-digital economy.

Personal information has a particular meaning for privacy and communications data protection.[[2]](#footnote-2) A steady increase in the number and range of activities being undertaken in the digital environment is resulting in citizens disclosing increasing amounts of personal information. Much of this information is disclosed voluntarily. However, many popular e-commerce and social networking applications are coded to enable detailed records of online behaviour to be recorded and analysed. Many users are unaware of the scale of such practices.

This information also has a growing financial value. Personal data has been referred to as the ‘new oil’, with value moving towards organisations that automate and mine personal data.[[3]](#footnote-3) More than US$2 billion a year is spent on acquiring third-party personal data in the United States.[[4]](#footnote-4) The collection and analysis of anonymised location and behavioural information to develop user profiles and personalised marketing material is broadening the meaning attached to personal information.

Citizens have expressed particular concerns about how they manage risks to personal information in the digital data environment, particularly risks focusing on financial loss, reputation and managing their digital identities. Despite having particular concerns, citizens also consider the protection of personal information is a responsibility shared equally by users, service providers and governments. They are also looking for assistance in operating in a complex digital data environment.

The consequences of these developments are that issues previously confined to one sector may span a range of different services. Moreover, new issues are emerging that do not neatly fit within existing regulatory frameworks. A substantial amount of communications activity is occurring in environments that were not envisioned when the confidentiality safeguards in the privacy legislation and communications regulation were designed.

There are unique challenges in considering whether:

* the suite of existing regulatory safeguards translate into the digital environment
* other approaches are needed for safeguarding the privacy and personal data of citizens and consumers in a networked society and information economy.

While it is likely that a mix of interventions will continue to be required, the nature and scope of these may need to change to address the specific and changing circumstances of a networked information economy.

It will also be important to provide a single coherent framework within which different interventions might operate. Among other things, such a framework could incorporate a broadened definition of personal information, as well as addressing changing citizens’ concerns about the handling of their personal information in the modern information economy.

The ACMA undertakes research to identify the dimensions of digital technology change and shifts in the behaviour and expectations of digital citizens. The evolving personal information and digital data environment is a key development having a significant impact on current regulatory settings. Consequently, it offers insights into how any future arrangements should be designed.

# Introduction

Citizens and consumers are undertaking an increasing range of social and economic activities online, including the creation of significant amounts of digital content. Contemporary devices, networks and apps allow citizens to interact with each other and organisations in highly personalised ways. Early use of the internet offered individuals the opportunity to seek information and interact with other users without having to reveal their true identities. This gave rise to the popular saying: ‘On the internet, nobody knows you’re a dog’. The ability to engage online anonymously or pseudonymously has remained a cornerstone of the internet. Citizens and consumers are now establishing digital identities comprised of the credentials they use to identify themselves to service providers and may maintain several digital identities, each to be used in specific transactional, professional or social contexts.

Communications data and privacy-related safeguards designed to protect personal information have been delivered via a mix of national and sector-specific measures. Varying protections, obligations and information disclosure requirements and responsibilities are shared among a range of Commonwealth and state regulatory bodies, including the ACMA’s role in communications and media privacy regulation.   
At the federal level, other agencies with interests in privacy and personal data include the Office of the Australian Information Commissioner (OIAC), Department of Broadband, Communications and the Digital Economy (DBCDE), Attorney-General’s Department (AGD), Australian Competition and Consumer Commission (ACCC), Australian Securities and Investments Commission (ASIC), Department of Health and Ageing (DHA), National E-Health Transition Authority (NEHTA), Australia Post and the Australian Press Council. Each state also has its own counterpart agencies dealing with privacy-related matters.

The establishment of these measures predates the arrival of the digital services that now underpin many citizens’ social and economic interactions. The *Privacy Act 1988* (Privacy Act)has been the subject of a recent review by the Australian Law Reform Commission (ALRC) and a number of useful reforms are due to take effect from March 2014. The Attorney-General has recently announced that the ALRC will undertake a further review of privacy safeguards.

This paper is the fourth in a series of occasional papers examining emerging issues in contemporary media and communications. Previous papers examined the mobile apps market, near-field communications and cloud computing.

While some digital data is aggregated and anonymised, the capacity for data to be traded and combined means that citizens will not be aware of where their data is going, and what it might be used for at the time of collection. These practices challenge the ongoing viability of traditional data collection processes based on obtaining a citizen’s informed consent. This paper covers:

* developments in network and device capabilities, data analytics, the apps and service environment that are transforming the nature of personal and private communications in a networked society and information economy
* consumer and citizen concerns in dealing with digital data creation and use
* the integration of digital data into social and economic transactions and the implications for existing communications privacy protections and obligations
* strategies and tools to address emerging privacy and personal data concerns in a networked society and information economy.

The ACMA would welcome further discussion from interested parties on the following questions:

1. Which privacy and personal data issues are of most concern to citizens?
2. What tools, skills, knowledge and behaviour would equip citizens to better manage their own personal data?
3. What role can the ACMA and other agencies play in fostering citizen-friendly personal data practices on the part of organisations?
4. How can industry participants promote awareness of and compliance with self-regulatory schemes that address citizens’ privacy and personal data concerns?

Feedback on this paper can be directed to [regframe@acma.gov.au](mailto:regframe@acma.gov.au).

# Evolution of the personal data environment

In the pre-digital economy, a relatively small number of organisations held and had access to individuals’ personal information. Personal information tended to be collected sporadically, often in hard copy, for a single specific use.

In contrast, in the networked society and information economy, digital data is the currency of social and economic transactions, where those transactions are increasingly mobile and global. Data about citizens’ online and offline behaviour is being analysed to improve delivery of services and target marketing activities. The increased capacity to create, store, analyse and reuse digital data about citizens’ activities and behaviour is transforming the personal data environment (see Figure 1).

|  |
| --- |
| Figure 1 Personal data environment |
|  |
|  |

This chapter examines developments in communications and computer processing power that are transforming the personal data environment. Key developments covered include:

* device capabilities
* software and apps
* increasing network capacity for data traffic
* increases in search and data analytics spawned by advances in computer processing
* the changing forms of personal information.

## Sophisticated devices support rich data collection

Vendors are designing devices with increasing data storage capacity and functions, many of which have implications for the creation, storage and use of personal data. The most significant developments in consumer devices have been the range of smartphones and tablets with audiovisual recording capabilities, sensors for location data and near-field communications, and new wireless networking capabilities.

An important characteristic of these devices is that they are personal and portable. They allow data about individuals’ behaviour and preferences to be recorded and related to other data stored on the devices and data to be exchanged on a near-continuous basis.

|  |
| --- |
| Figure 2 Connected devices enable collection of personal data |
| cloud graphic |
|  |

Take-up of these devices has been rapid, with adult ownership of smartphones roughly doubling between June 2011 and June 2012.[[5]](#footnote-5) It is estimated that by the end of 2013, around 50 per cent of Australian homes will have at least one tablet and 70 per cent of Australians will own a smartphone.[[6]](#footnote-6)

Interest in location data is rapidly increasing as a result of the rapid take-up of smartphones and other devices with Global Positioning System location capabilities. An increasing range of applications are incorporating location information in their functions to deliver information that is geographically relevant to users.

Near-field communications (NFC) technology is another example of device technology with the potential to have an impact on personal data collection. Mobile devices are increasingly incorporating NFC capabilities. To date, NFC use is largely limited to payment mechanisms. However, its possible application to customer loyalty, ticketing and a range of other proximity-related applications would potentially enable the collection of new types of behavioural data.

## Software exploits device capabilities to capture a range of personal data

Software, including device operating systems and applications, is at the heart of personal data collection practices. Significant amounts of personal information are collected as a result of citizens’ online interactions with applications. These a range from social networking sites, and other applications which run in browser interfaces, to the many ‘apps’ available for smartphones, tablets and other devices.

Online behaviour-tracking and analysis are also underpinned by software. Use of website ‘cookies’ to track consumers’ online activities—and the use of this information to inform marketing activities—are giving rise to demands from citizens for ‘do not track’ tools and measures.

Growth in the take-up of mobile apps is having a significant impact on the amount of personal data created and captured. Video content accounts for the majority of mobile data traffic. However, social networking and picture messaging via mobile device apps are expected to be significant contributors to the doubling of mobile data traffic each year over the next five years.[[7]](#footnote-7) Whereas consumption of media on traditional platforms is largely anonymous, online content consumption is associated with the collection of a range of personal and behavioural data.

Data collection and usage practices are evolving, with apps used in a number of these practices. For example:

* citizens are voluntarily sharing significant amounts of information about themselves and their activities through social networking apps
* many apps facilitate storage of personal data on cloud computing services
* behavioural data recorded by browser, social networking and multimedia apps, is being commercially exploited and traded for marketing purposes
* a number of apps have been found to be vectors for malware that targets personal information for use in cybercrime and other malicious activity.

|  |
| --- |
| Figure 3 Apps and privacy issues |
|  |
| *Source: Juniper Networks.[[8]](#footnote-8)* |

The impact of mobile device apps on privacy and personal data is discussed in further detail in the separate paper, [*Mobile applications—Emerging issues in media and communications*, *Occasional paper 1*](http://www.acma.gov.au/theACMA/Library/researchacma/Services-and-emerging-technologies-research/emerging-issues-in-media-and-communications-occasional-papers)*.*

## Advances in network coverage and capacity aid personal data collection and storage

High-capacity fixed and mobile networks enable near continuous collection and transmission of data from connected devices. They also facilitate remote access to data and applications provided by cloud computing services.

The capacity for remote storage and access to data is a fundamental characteristic of the online environment. Advances in storage and networking technologies now allow management of a broader range of data, including the outsourcing of data management. Organisations can potentially achieve significant efficiencies by using data management services, such as cloud computing. However, the outsourcing of personal data management activities gives rise to questions about how responsibilities for protection of data are assigned, including applicable personal information protections, when cloud services are located in other jurisdictions.[[9]](#footnote-9)

## Data collection and analytics processes

A growing demand for information about citizen and consumer behaviour is driving the development of new approaches to the collection and analysis of personal information, using, for example, web analytics, record exchanges and business intelligence systems (see Figure 4).

|  |
| --- |
| Figure 4 Data analytics processes analyse consumers’ preferences and behaviour |
| [http://www.neustar.biz/information/img/ian/ianlifecycle460px.png](http://www.neustar.biz/information/img/ian/ianlifecyclensr-800px.png) |
| *Source: Neustar.[[10]](#footnote-10)* |

Organisations that collect and hold personal information are recognising its potential value to third parties and developing new business models, which aim to generate new revenue.

Telecommunications companies Telefonica and Verizon Wireless have established specialist data analytics units within their operations to extract commercial value from data collected regarding their customers’ online and telecommunications activities. Examples of the types of information products that can be produced from this data include:

* analyses of customers’ physical movements in clear and simple graphs and figures
* searches of an area by footfall, demographic, or address
* customer visits to an area identified by time, gender, or age
* reports on the movements of crowds at any given place by hour, day, week, or month.[[11]](#footnote-11)

With increases in computing power, and the availability of personal information from social networking activity, information aggregators have the capacity to combine distinct pieces of digital information, such as an individual’s online activity, behavioural preferences and location data. And many consumers will not be aware of the extent to which information they have voluntarily shared on social networking sites—such as location data and ‘likes’—is being used to inform marketing practices. It has been reported that an individual’s personality type can be deduced by analysing the content of their ‘tweets’. The resulting personality profile information may then be used to design and target marketing activity.[[12]](#footnote-12)

While some data is aggregated and anonymised, the capacity for data sources to be traded and combined means that citizens will not be aware of where their data is going and what it might be used for when it is collected. These practices challenge the ongoing viability of traditional data collection processes based on obtaining a citizen’s informed consent.

Technology developments have introduced a more diverse range of participants who are involved in the capture, storage and sharing of data derived from a broad range of social and economic activities. Each of these elements in the digital data environment is having its own identifiable impact on citizens’ personal information experiences.

## Evolving for technical tools and privacy-enhancing services

As the data collection market has evolved, a range of privacy protection products and services have emerged to protect a user’s personal data in various ways. Figure 5 is an overview of three major categories of privacy protection tools. These tools encompass, to varying degrees, several different aspects of privacy including anonymity, security, and the management of digital identity. Organisations may offer a service that relates to all three categories.

|  |
| --- |
| Figure 5 Examples of privacy tools |
| |  |  | | --- | --- | | **Personal data vaults** | * range from basic password protections to full database of a range of personal data * some offer financial incentives for controlled  sharing of data * examples include Singly, Personal, mint.com | | **Personal data monitors** | * provide information on where personal data is being sent and how it is being used * some services offer an ability to monitor the online reputation of an organisation or individual * examples include Reputation.com, Ghostery, Clueful | | **Anonymisers** | * range from do not track tools to encryption of data and other services * examples include Bitcoin, Voucher-Safe and Deadbolt | |
|  |

### Personal data vaults

There is a range of personal data vault services that collect, protect and allow controlled sharing of a range of personal data. These new services present innovative ways for consumers to not only protect their privacy but also to regain some control over where and how their data is distributed online. One example is Personal.com, which stores a range of customer data and allows sharing of this information with partner organisations, according to customer-set rules.[[13]](#footnote-13) The service is based on the idea that people can take control of their personal data and may be able to share that data in exchange for various items of value.[[14]](#footnote-14) The personal data vault market is forecast to reach £30 million by 2016.[[15]](#footnote-15)

### Personal data monitors

There are two types of personal data monitors, those that track:

* the public personal data of an individual or organisation available online
* the personal data being collected, where it is delivered and its uses.

Services that track online information can offer to services ‘clean up’ personal online data. One example is Reputation.com, which offers the ReputationDefender® tool that suppresses negative online content about an individual and replaces it with positive content controlled by the user.[[16]](#footnote-16) Services that track the collection of personal data often provide tools to block this data-collection process. An example is the Clueful app ([www.clueful.com](http://www.clueful.com)) that provides information on the use of personal data by other applications.

### Anonymisers

These services offer various ways to make the user anonymous by blocking tracking, encryption or other methods. One common method is the use of a Virtual Private Network (VPN) that can be used to hide the location, identity and other information associated with a user. Another example is Deadbolt, an application that enables the encryption of digital documents.[[17]](#footnote-17)

## Changing definitions of personal information in the networked digital environment

Personal information has a particular meaning for the purposes of privacy and communications data protections.[[18]](#footnote-18) The types of digital information that are now able to be created, collected, exchanged and reused include information about an individual’s search history, social connections, interests, purchasing history, location, and calendars and contact sources.[[19]](#footnote-19) Digital data that underpins this information can be categorised three main types:

* volunteered—that is, data created and explicitly shared by the individual, such as data posted on social networking services (SNSs)
* observed—includes data harvested about an individual, such as their current location, or data harvested from third parties, such as an individual’s purchasing history
* inferred—individuals volunteered and observed data that is processed to produce a new source of information and anonymised data that relates to groups of individuals, such as groups of individuals who ‘like’ the same activity.

Current data practices now support inferred information about personal behaviour and preferences. This does not directly or indirectly identify a person and is a category of digital data has ambiguous status within the privacy regulatory framework. For example, a consumer may be familiar and comfortable with data about the date, time and location of a credit card purchase being recorded as part of a transaction. They may be less familiar with technology and practices that record their movement through a store and associated purchasing behaviour and uses this data to target marketing material to them.

Nonetheless, ACMA research indicates that citizens are concerned about the collection of this data, how it might be used and who has access to it. Consumer and community expectations and concerns surrounding personal information practices are explored further in the next chapter.

# Citizens’ attitudes to digital data sharing and security

Concerns about the protection of personal data traditionally have focused on the practices of government entities, financial institutions and utilities. With a broadening of citizens’ engagement with digital communications and social media, there is a widening set of expectations and concerns with digital data practices.

This chapter examines citizen attitudes to the collection and use of their information in the media and communications environment, drawing on ACMA research.[[20]](#footnote-20)

Recent ACMA research examined citizens’ attitudes towards the management of their digital identities and digital footprints. Attitudes to different types of personal information and risk in the online environment were also explored.

The research indicates that citizens have a nuanced view about the perceived risks of operating in a digital data environment. However, they do not always make distinctions between different types of personal data or adopt different strategies to manage different types of digital information. Understanding citizen expectations and behaviour offers useful insights to the framing of possible responses, including protection mechanisms.

## Digital identity an enduring concept

Citizens are establishing digital identities comprised of the credentials they use to identify themselves to service providers and the digital footprints that are created as a by-product of their various online interactions. Individuals may maintain several digital identities, each to be used in specific transactional, professional or social contexts.

Research participants valued maintaining a separation between their name and their physical appearance in the online environment. More than half (53 per cent) said that they will never give inaccurate information about themselves online. More than two-thirds of those indicated that they would simply choose not to log in or register for a service, if they had concerns about the information requested.

|  |
| --- |
| Figure 6 When participants would give inaccurate information |
|  |
| *Source: Taverner Research for ACMA, 2013.* |

The 47 per cent of respondents who acknowledged that they will sometimes provide inaccurate information were asked their reasons for doing so. Relevance (‘I do not see why the information is needed for this site/service’) is the strongest driver to provide inaccurate information, but security and transparency are also important.

|  |
| --- |
| Figure 7 Reasons participants had given inaccurate information |
|  |
| *Source: Taverner Research for ACMA, 2013.* |

At least three-quarters of research participants said that they would stop using an online site if it mishandled their health information, email address, phone number, photograph or credit card details.

There is also relatively limited use of existing social media-based trusted identity mechanisms to date. While over 80 per cent of individuals are aware of such mechanisms, fewer than one-in-four has used one. Reasons for not using such mechanisms include:

* a preference for keeping activities on different sites separate (45 per cent)
* concern that personal information will be shared across multiple sites (36 per cent)
* a perceived lack of control of how personal information is used (35 per cent)
* concern that the identity provider will track activity on other sites (31 per cent)
* a perception that the trusted identity is not secure.

To the extent that some of these concerns may be unfounded, the research findings point to the need for citizens to have better information about the potential benefits of trusted identity tools. This could include a clearer explanation about how using a trusted identity measure would safeguard a user’s personal information when the user is presented with this option.

## Citizens have concerns about electronic intrusions

Many citizens perceive unwanted electronic contact to be an invasion of privacy In the same way that they may be concerned about unwanted physical contact and physical intrusions into their personal space.

In a recent survey of Australians’ security concerns, unauthorised access to or misuse of personal data was the top concern identified by 62 per cent of those surveyed.[[21]](#footnote-21) Their concerns spanned a range of industry sectors, but were concentrated in telecommunications and financial services.[[22]](#footnote-22)

In the ACMA’s research, just under 40 per cent of online users were confident that privacy settings on websites work.[[23]](#footnote-23) Mandatory authentication procedures that required the user to provide information unrelated to a transaction were seen as intrusive and indicative of an untrustworthy site.

## Citizens are concerned about financial loss

An area of increasing interest to the ACMA is the financial risks arising from disclosures of personal information or financial transactions on a communications network. Financial risks may be incidental to breaches of other communications information and data protection obligations. Risks can occur where personal information is disclosed publicly or to unauthorised third parties, which may result in financial detriment to an individual.

Financial privacy issues also arise from voluntary disclosure of personal information through online social networking and spam-driven scams. Many online social networking sites encourage disclosure and sharing of personal information, including family relationships, employment and education history, and living locations.

In recent ACMA research, a data breach that involved financial loss was a strong concern, with 90 per cent of participants stating that they would stop using a site if their credit card details were stolen from it.[[24]](#footnote-24)

|  |
| --- |
| Figure 8 Events that would annoy users enough to stop using a provider |
|  |
|  |

Another form of financial risk may occur as a result of the malicious use of personal information or information about personal activities. Unwanted communications in the form of spam is a mechanism that may be used to encourage individuals to supply personal details through scam campaigns. These details are then used to defraud them. The ACMA’s research has identified that, in the 12 months to May 2012, approximately 3.2 million internet users in Australia were estimated to have had their computers infected with a malware virus and 1.2 million experienced some form of online credit card fraud. In addition, 625,000 people were estimated to have responded to an unsolicited or scam email and provided either personal information or money.[[25]](#footnote-25)

## Managing reputation

Recent ACMA research on the ways in which citizens manage their digital identities confirms the importance that citizens attach to their reputation in the digital environment. Over 80 per cent of respondents indicated that disclosure of private information that resulted in damage to their reputation would be sufficient to cause them to stop using a service.**[[26]](#footnote-26)**

## Managing location activities

Location information is considered particularly valuable because of the role it can play in targeting marketing activities. It has been claimed that consumers are significantly more likely to respond to advertisements for products and services that are available relatively close to them.[[27]](#footnote-27) ACMA research shows that consumers recognise the value of functionality and content that is tailored to their locations. Nevertheless, they have limited awareness of how this information is collected, stored and shared, and are concerned about these practices. They expect to be informed about this and to be able to make informed choices about how and when their location information is used.[[28]](#footnote-28)

## Malicious activity risks to personal data

The potential for personal data to be exploited for identity theft and other fraudulent activities has made it an attractive target for criminals. Consequently, personal data is the target of a significant proportion of malicious online activity, with criminals employing a range of technical and social engineering techniques in attempts to obtain personal data. Commercial distribution of online child sexual abuse material was largely driven by organised criminal activity aimed at obtaining users’ credit card and other identity details. Users would then find that unauthorised purchases had been made on their accounts. Many were reluctant to report this to authorities because they feared that their purchases of illegal material would be discovered. This fraudulent activity has been effectively addressed through cooperation between law enforcement agencies, online service providers and financial institutions.[[29]](#footnote-29) However, other sophisticated social engineering techniques and ‘malware’-related activities aimed at obtained personal data have continued to emerge.

The most prevalent infection type currently being reported through the ACMA’s Australian Internet Security Initiative (AISI) is numerous variants of ‘Zeus’. It is primarily used for banking fraud and can intercept and modify an infected user's online banking transactions. This then allows cyber criminals to steal money from a user’s infected bank account. Apps are also emerging as a popular platform for malicious activity, with a number of popular game apps found to include Trojans. These collect and share personal information contained on the devices on which the game apps are installed.[[30]](#footnote-30)

## Shared responsibilities

For citizens this is a complex environment as they consider how best to manage the information they generate in their economic and social transactions.

Half the participants in recent ACMA research expected government to play a strong role in protecting their personal data, but relatively few (12 per cent) saw government as *solely* responsible. Forty-five per cent considered that protection of personal information is a responsibility to be shared equally by users, service providers and government.[[31]](#footnote-31)

These conclusions broadly align with earlier findings relating specifically to the protection of location data. These findings emphasised the importance of personal responsibility, underpinned by more transparent data collection practices by service providers, and a regulatory safety net.

The research also shows that consumers expect location service developers and other industry participants to provide information about how location data is used. Relatively few considered this to be a government responsibility.[[32]](#footnote-32)

|  |
| --- |
| Figure 9 Responsibility for providing information and advice |
|  |
| *C8—Who has the most responsibility for providing this information and advice?*  *Base: Total sample n=294.* |

Any future interventions in the digital information environment will need to take account of the shared approach to developing solutions and protection arrangements.

# Implications for regulatory settings

This chapter considers the impact of the integration of digital data in social and economic transactions. It also discusses the implications for existing communications privacy protections and obligations.

There are significant challenges in considering whether:

* the suite of existing regulatory safeguards translates into the digital environment
* other approaches are needed for safeguarding citizens’ privacy and personal data in a networked society and information economy.

## Economy-wide and industry-specific regulation

Citizens have longstanding expectations that their person-to-person communications will be confidential and that they will have control over the range of entities with which information is shared. In many cases, the viability of modern channels of communication is underpinned by an understanding that the information being conveyed will not be disclosed to a third party.

Protection of privacy and personal information has been a core element of the media and communications regulatory framework. It has been supported by a mix of economy-wide and sector-specific measures. Varying protections, obligations and information disclosure requirements and responsibilities are shared among a range of Commonwealth and state regulatory bodies, including the ACMA in its communications and media privacy regulation role.

The Privacy Act—administered by the OAIC—establishes economy-wide protections over personal data, including notification requirements for privacy breaches by government agencies, health service providers and businesses, and non-government agencies with turnover exceeding $3 million.

It includes privacy principles that apply to the handling of personal information by most Australian, ACT and Norfolk Island public sector agencies, large businesses, all health service providers and some small businesses and non-government organisations. It also:

* specifies credit reporting provisions that apply to the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies, credit providers and some third parties
* regulates the collection, storage, use, disclosure, security and disposal of individuals’ tax file numbers
* permits the handling of health information for health and medical research purposes in certain circumstances, where researchers are unable to seek individuals’ consent
* allows organisations to have and to enforce their own privacy codes and permits small business operators, who would otherwise not be subject to the Privacy Act, to opt in to being covered.[[33]](#footnote-33)

International frameworks, such as the OECD Privacy Guidelines, are also relevant as they provide the foundation for the development of national privacy laws in Australia, as well as other nations. The guidelines have been in place since 1980 and establish high-level principles for privacy protection. They also call for OECD member country cooperation through establishing procedures to facilitate mutual assistance in procedural and investigative matters.[[34]](#footnote-34) A review of the guidelines is underway. This includes an examination of cooperation between privacy authorities and global interoperability of privacy frameworks as important elements for improving the effectiveness of privacy frameworks.[[35]](#footnote-35)

### Communications-specific protections

The regulatory frameworks for the previously distinct radiocommunications, telecommunications and broadcasting sectors each contain clear privacy objectives and measures. The ACMA has observed common elements of communications and media privacy that provide insights to the framing of privacy protections (see Figure 10). These elements include:

* identity—to protect a citizen’s or consumer’s personal or private information
* location activity—to protect information about an individual’s location, activities or movements
* intrusion—to protect a citizen or consumer’s personal space from unwanted intrusions
* reputation—to protect a citizen’s name or reputation
* financial—to protect a citizen or consumer’s financial or transactional information.

|  |
| --- |
| Figure 10 Communications and media privacy issues |
| Visio-Privacy Mud Map - ACMA Statuatory Roles and Issues in A4 LC.jpg |
|  |

### Identity of communications customers

Part 13 of the *Telecommunications Act 1997* (the Telecommunications Act) recognises the privacy expectations that are intrinsic to citizens’ use of telecommunications services. It establishes a regulatory framework to protect the confidentiality of information that relates to carriage services and the content of communications carried on them. These measures also protect information about carriage service providers’ customers.

Information protected by these measures may be disclosed only in limited circumstances, which include maintenance of the Integrated Public Number Database (IPND) and law enforcement and national security. Accurate records of disclosure must be kept. The priority placed on protecting the confidentiality of citizens’ communications is reflected in the penalty of imprisonment that applies to breaches of these requirements.

In addition, the Telecommunications Consumer Protections Code and Mobile Premium Services Industry Code, registered by the ACMA under Part 6 of the Telecommunications Act, require carriage service providers to protect their customers’ personal information from unauthorised use or disclosure, and content suppliers to protect the privacy of complainants’ personal information.

### Location activity information

Information about citizens’ locations and activities is collected and used in a variety of contexts. Internet service providers may collect and temporarily store information about their customers’ online actions in the course of providing access to internet content. Carriers and carriage service providers also collect and store data about their customers’ calling and messaging activities for billing and other purposes.

Part 13 of the Telecommunications Actestablishes protections for information concerning carriage service providers’ customers. Safeguards for the protection of information associated with consumers’ identities and accounts are also provided in codes of practice for carriage service providers and content service providers.

A related aspect of telecommunications personal information is the use of this information to identify an individual’s location. This supports emergency services and activities that provide information for law enforcement and national security.

Obligations to provide communications-related location and personal information—including location information—to emergency service organisations are established under Part 8 provisions of the *Telecommunications (Consumer Protection and Service Standards) Act 1997.* Further details are specified in the ACMA’s Telecommunications (Emergency Call Service) Determination 2009.

### Protections against electronic intrusions

Concerns about intrusion arise from electronic media coverage of citizens’ personal and private affairs. Registered codes of practice for each sector of the broadcasting industry include requirements aimed at protecting the privacy of individuals in the making and delivering programs. These codes are supplemented by the ACMA’s *Privacy Guidelines for Broadcasters 2011*, recently updated to take account of changes in community attitudes to media coverage of private matters.

Successive advances in information and communications technology have given rise to other perceived intrusions on privacy through unwanted telemarketing calls and unsolicited email and messages (spam). Most are either commercial or involve some type of financial scam. Governments have enacted a range of measures to deal with these concerns. In Australia, the ACMA administers anti-spam and do-not-call schemes that protect Australians from unsolicited commercial email, messages and telephone calls.

The *Do Not Call Register Act 2006* responds to the community concern about unwanted intrusions through telemarketing calls and marketing faxes. The scheme requires businesses who intend to make telemarketing calls and faxes to check numbers against the ACMA’s Do Not Call Register. The ACMA is responsible for ensuring that telemarketers and fax marketers (collectively referred to as marketers) comply with these rules. There are now over eight million telephone and fax numbers on the register. This substantially enhances the privacy of citizens who would otherwise be the target of unwanted telemarketing calls.

The *Spam Act 2003* (the Spam Act) establishes an opt-in regime for the distribution of commercial electronic messages. The safeguards in the Spam Act were developed to address the specific intrusive characteristics of electronic messaging as a low-cost, high-volume communications medium. They complement the opt-out arrangements that apply to other media under the National Privacy Principles.

### Reputation

A key motivation for a citizen in controlling information about personal affairs and details is the protection of his or her reputation. The manner in which citizens’ personal affairs are described and depicted in radio and television programs is often a matter of community concern and debate. It is one of a number of issues taken into account when considering appropriate community standards for such material.

In the online environment, management of reputation is becoming a more significant issue as information can be created and shared with considerable speed, and the data may be stored in perpetuity. All internet users have a digital or online reputation—the opinion or view that others have about the user, based on what a user says or does online. A communication that was intended to be private can rapidly become public. The evolution of online media outlets is placing considerable pressure on privacy-related safeguards for the broadcasting industry. While broadcasting services are subject to the codes of practice applying to each sector, the online presence of these services is not regulated by those codes. This leaves citizens with incomplete protection from media intrusion.

Current regulatory measures include the *Privacy Guidelines for Broadcasters* and the protection of telecommunications information under the Part 13 Telecommunications Act. Digital reputation management and controlling access to personal communications is an important aspect being addressed by the ACMA’s [Cybersmart community education programs](http://www.cybersmart.gov.au/Parents/Cyber%20issues/Digital%20reputation.aspx). The emphasis of current education and information resources is on privacy controls and tools to help children and parents manage online risks.

## Emerging gaps in personal data protections

A substantial amount of communications activity is occurring in environments that were not envisioned when the confidentiality safeguards in the privacy legislation and communications regulation were designed. The consequences of these developments are that issues previously confined to one sector may span a range of different services. New issues are emerging that do not fit neatly into existing regulatory frameworks. Some types of personal data activity do not appear to be covered by existing protections, because of the type of data being collected, the characteristics of the entity collecting the data, or other circumstances associated with an activity’s supply chain.

### Implications for informed consent

A current focus of regulatory safeguards is securing an individual’s informed consent to the collection and use of their personal information. This approach has worked reasonably well to safeguard personal information that is disclosed in the course of irregular and ad hoc transactions, when users have time to make informed decisions about the information they are disclosing. However, this approach is under increasing pressure in an environment characterised by increasingly frequent, varied and complex transactions in a digital information economy.

Any given online activity is likely to involve disclosure of numerous types of personal data, sometimes over an extended or continuous period. The data collected through these activities is likely to be stored for an extended period and may be put to a variety of uses in the future. In this environment, it would be impractical for individuals and organisations to negotiate the rights to such data, without substantially detracting from a consumer’s experience. Furthermore, it seems unlikely that consumers can be expected to provide informed consent to the use of their data when possible future uses are not known at the time of collection.

These factors suggest that alternative, non-regulatory approaches to specifying rights and permissions to personal data may be required.

### Unattended and poorly attended risks

The capacity to collect, correlate, store and trade personal information, including anonymous information, is raising different forms of risk, not specifically addressed within current protection mechanisms. This includes concerns about the security, privacy and management of personal information that is stored in cloud services, including services housed in other jurisdictions. It is also relevant to practices such as data harvesting from home wireless networks by commercial entities, and the uncontrolled or potential malicious use of information about personal activities collected via location-tracking apps or website-tracking cookies.

Existing protections are largely confined to data which readily identifies a specific individual. However, the capacity for data sets to be combined and correlated means that even data that is thought to be anonymous may be used in ways that raises particular privacy concerns for individuals. The ACMA’s research also shows that individuals also have concerns about the collection and use of behavioural information—including location data and other online behaviour measurements—even though their identities may not be apparent from this type of information. The collection of information about personal activities that take place in public, but where an individual may expect to enjoy seclusion, is another area of potential concern that may not be addressed comprehensively by existing safeguards. This suggests a need to reconsider the scope of existing safeguards and to develop protections, which align with community expectations.

### Coherent frameworks for identification and authentication techniques

There is widespread recognition that existing login and password-based authentication techniques are highly vulnerable to security breaches. This is due to a range of factors, including the difficulties that citizens face in managing multiple passwords that are each sufficiently complex to provide an appropriate level of security. While ACMA research shows that individuals have only limited concerns about the management of their online credentials, this may not be commensurate with the level of risk posed by many citizens’ practices. For example, reusing passwords across multiple sites and using simple, easily guessed passwords is relatively high. This leaves consumers vulnerable to online fraud.

Wider use of trusted identities has the potential to make user identification and authentication processes more secure. Through initiatives such as the OpenID Foundation, a market for trusted identity products is emerging. Such products allow online service providers to identify and authenticate users without the need to store and manage users’ credentials. They also simplify online transactions for users by reducing the numbers of logins and passwords that they need to manage.

The ACMA’s research also identified design features for trusted identity mechanisms that are of high importance to citizens when deciding whether or not they should use one. When asked what features they would consider to be essential, 59 per cent selected the ability to choose which items of personal information are passed from the identity provider to the site being accessed. Forty-seven per cent wanted to make such choices on a case-by-case basis. Some 56 per cent said they would expect the identity provider to reimburse them for any financial loss resulting from a security breach. Respondents also expected to be informed about and have control over any information that was passed on to other organisations.

These findings point to citizens having a strong interest in being able to control the flow of their personal data when using a trusted identity mechanism. Digital identity providers should take these preferences into account when designing and promoting their trusted identity measures.

To date, there has been limited progress on developing trusted identity measures that enable citizens to verify their identities to the range of online services now operating across the digital economy. While some sectors of the economy are now moving to develop trusted identity measures, there is a risk that uncoordinated sector- or industry-specific initiatives will give rise to a plethora of incompatible services.

Interoperability of trusted identities products and services would potentially offer significant benefits, in terms of increased security of online transactions and convenience, by simplifying identity verification processes. Therefore, there may be substantial benefit in formulating a coherent national framework within which trusted identity products and services can be developed.

### Whole-of-economy governance and oversight

Growing pressure on the existing regulatory framework for privacy and personal data protection suggests that overall governance of the diverse suite of measures will become increasingly important. Current responsibilities are highly fragmented across different regulatory bodies and levels of government, all of which have legitimate interests maintaining the effectiveness of safeguards they administer. However, these arrangements mean it is sometimes uncertain where responsibility rests for emerging risks—particularly those associated with the media and communications sector. Emerging privacy concerns associated with technologies such as apps, cloud computing, and data analytics cut across the interests and responsibilities of several regulatory bodies. This can create uncertainty for determining where overall responsibility for privacy outcomes rests in each case.

## A coherent strategy is required to manage personal data in the digital environment

A consequence of this shift to an increasingly networked information economy is the collection of personal data by a significant number of organisations in a wide variety of contexts. This is having profound implications for the task of formulating and administering regulatory safeguards that are sufficiently robust, while also being flexible enough to accommodate innovation.

Most national regulatory frameworks that deal with privacy and protection of personal data are now 20 to 30-years-old. New issues created by technological and market developments have been accommodated through a series of incremental and piecemeal updates.

In its submission to the Australian Law Reform Commission’s 2007 review of the Privacy Act, the ACMA noted the fragmentation of privacy rules across telecommunications and other legislation, and the potential for confusion and anomalies to arise. The issues identified by the ACMA included:

* different obligations relating to the collection, use and disclosure of personal information across the Privacy Act and the Telecommunications Act
* different approaches to information disclosures under Part 13 of the Telecommunications Act and provisions of the *Telecommunications (Interception and Access) Act 1979*
* fragmentation of telecommunications-related privacy responsibilities between the ACMA, Telecommunications Industry Ombudsman and the OAIC.

Recent amendments to national privacy frameworks, including changes to Australia’s Privacy Act, go some way to addressing new challenges to the protection of personal data. However, the scale of current changes to the personal data environment is such that fresh approaches need to be considered. In particular, the scale, diversity and global structure of the personal data ecosystem are likely to challenge the effectiveness of legislative approaches. They also call for non-legislative measures that address the specific contexts in which personal data is being collected.

Consideration of the need or otherwise for future interventions in this area should continue to balance a broad range of economic, social and industry policy considerations relevant in the evolving personal information environment. These include:

* **Market standards**—Of particular relevance to the personal data environment is the desirability of competitive markets, which can be achieved in part by measures which facilitate data portability and interoperability between services and systems. Citizens also require access to effective redress mechanisms to address market behaviour that does not align with community standards.
* **Social and economic participation**—A prerequisite for participation in an information economy is that individuals and organisations have certainty and confidence about their rights and obligations regarding privacy, personal data, and other matters. Individuals and organisations also require the skills, knowledge and behaviour to enable them to engage effectively as digital citizens. This includes them being highly proficient in managing digital identities and digital footprints.
* **Safeguards**—These are designed to protect against individual harm and support national interest protections. One objective of privacy safeguards is the protection of citizens from harm—in the form of financial loss or other adverse consequences—that may flow from unauthorised disclosure of their personal information. Digital identity and personal data are also central to measures which allow citizens to be identified and located in emergencies, and for them to be informed about how to protect themselves in these situations. Law enforcement and national security organisations have relied on the ability to intercept and monitor communications in the course of investigating potentially criminal behaviour.

These ongoing public interest considerations can inform discussion about the need, or not, for intervention in personal data environment. The network layers model provides a useful framework for considering the points at which privacy and personal data issues may arise. Figure 11 is an indicative illustration of the network layers in which particular public interest considerations may need to be addressed.

|  |
| --- |
| Figure 11 Public interest outcomes in the personal data environment |
|  |
|  |

While it is likely that a mix of interventions will continue to be required, the nature and scope of these may need to change to address the specific and changing circumstances of a networked information economy.

The ALRC’s forthcoming inquiry into privacy safeguards for the digital economy will need to consider the range of economy-wide and sector-specific safeguards, which comprise Australia’s privacy regulatory framework. The suite of media and communications privacy measures administered by the ACMA are a significant component of this framework. The inquiry should inform development of a coherent regulatory framework in which solutions can be tailored to address specific privacy risks. Among other things, such a framework could reflect the evolving definition of personal data. This definition could reflect the broadening role of personal information in an information economy and the breadth of citizens’ concerns and attitudes about the handling of their personal information in the modern information economy.

# Enabling strategies for the personal information environment

Many concerns about the protection of digital data derive from lack of transparency in data collection processes and adequate tools for controlling the disclosure of personal data, or both. In such an innovative environment, the regulator’s focus needs to span traditional protections for the privacy of personal communications, as well as consider solutions to emerging areas of citizen concern. In this context, communication strategies and market-based solutions are likely to play an increasingly important role in addressing such concerns before other types of intervention. There is also likely to be a place for direct regulation where it can be applied meaningfully to digital information practices.

This chapter discusses the suite of strategies and tools available to address the emerging privacy and personal data concerns in a networked society and information economy.

## Communication strategies

Communication strategies are particularly useful where improvements in knowledge or industry/citizen behaviour is the intended regulatory outcome.

Research on consumers’ attitudes to the collection and use of their personal data indicates that many want better information about these practices. There is a range of different contexts in which privacy and personal data protection concerns will arise. This requires an increased emphasis on digital literacy to provide citizens with the skills, knowledge and behaviour that they need to manage privacy issues.

Many consumer concerns about their personal data can be addressed with the privacy-enhancing tools and services described above. However, consumers need to be made aware of the existence of such tools and how they can be used. Some companies which collect personal data are also taking steps to modify their practices by ensuring that only necessary information is collected and that this is not personally identifiable. However, individuals may not be aware that these steps are being taken. Personal data collectors could develop effective strategies to better communicate their practices and the safeguards that they have put in place. Experience in the area of cybersafety education has shown that a degree of coordination is required to ensure appropriate coverage of the range of issues and audiences that need to be addressed.

The ACMA’s Cybersmart program is an example of an information and education strategy that provides a range of resources to address online risks and how to manage them. These include resources that deal with a number of privacy-related topics, including social networking, digital reputation, identity theft, sexting and unwanted contact. The ACMA supported 2013 Privacy Awareness Week by hosting a number of Cybersmart Networking and Cybersmart Detectives activities for upper primary and lower secondary students across Australia that helped to raise awareness of online social networking, with a focus on privacy settings.

## Facilitation of industry co- and self-regulation

Non-regulatory solutions potentially offer greater flexibility to protect personal data in the myriad contexts in which it is collected, stored and shared. Facilitation strategies such as industry co and self regulation are particularly useful where the intended outcomes are improvements in service, standards, knowledge about obligations, or incentives for behavioural change by industry participants or individual citizens. Many of these conditions are present in the evolving personal data market.

There are a number of examples of self-regulatory initiatives that aim to address growing citizen concerns about privacy in the digital environment.

A prominent area of concern for many citizens has been online advertising, and the use of personal data and data about online behaviour target advertisements that appear on websites. As noted above, many citizens are taking steps to block online tracking activity and are reluctant to divulge personal information that may be used to target advertising. In response to these concerns and in an effort to restore citizens’ confidence in online data collection practices, Australia’s Interactive Advertising Bureau has developed a Best Practice Guideline for Paid Social Advertising.[[36]](#footnote-36) The guideline includes recommendations that consumers be given opportunities to opt in and out of certain data collection practices plus guidance on how social media profile data should be captured, used and disclosed in marketing activities. While compliance with the guideline is voluntary, their development and publication informs adoption of good industry practices and provides a basis for stakeholder engagement on personal data usage.

Regulators can play a role in informing development of such initiatives through independent research, development of good practice principles and stakeholder engagement. The OAIC has developed a consultation draft better practice guide for app developers. The draft guide suggests that developers be aware of privacy responsibilities, be open and transparent about privacy practices, only collect personal information that the apps need to function and securing that information. It also suggests ways to facilitate more meaningful user consent, such as short-form notices and privacy dashboards.

The Privacy by Design framework developed by the Information and Privacy Commission of Ontario, Canada has been influential in guiding the adoption of better personal data practices at various points along the personal data supply chain. The Personal.com data vault has been designed to comply with the Privacy by Design framework. Canada’s Information and Privacy Commissioner recently presented a case study of Personal.com focusing on its alignment with Privacy by Design[[37]](#footnote-37) principles. This analysis showcases the innovative practices that Personal.com presents, including:

* Data fields marked as sensitive are encrypted and can only be viewed with a password the user chooses. The fields marked sensitive go beyond legal requirements. The password is not stored, only the user has the password.
* Access to any information is permission-based, which means it is totally dependent on the user to give access, not Personal.com.
* Users can port their information out of the Personal.com database in XML format.
* Personal.com has a built-in ‘delete’ button that allows users to easily delete their accounts. In addition, if a user forgets or resets their password, all the data fields marked sensitive are deleted to ensure extra data security.[[38]](#footnote-38)

In the mobile applications environment—where increasing amounts of personal data are being created and collected—application store providers and other industry participants have established governance arrangements and guidelines which aim to foster citizen-friendly data practices by application developers and other parties in the applications supply chain. For example, the GSM Association (GSMA) has developed high-level principles for protection of privacy on mobile networks, devices and apps. These include:

* Data minimisation and retention—only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop apps and services should be collected and otherwise accessed and used. Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous.
* Children and adolescents—an application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information are appropriate in all given circumstances and compatible with national law.

Recognising the growing significance of mobile location information as personal data, a group of industry participants has formed The Location Forum. This group has recently published Location Data Privacy: Guidelines and Assessment Recommendations which aims to inform collectors and users of location data about the range of privacy risks associated with it and foster approaches which reduce these risks and address individuals’ potential concerns.

The Internet Industry Association’s iCode is another self-regulatory initiative, which addresses e-security and cybercrime-related threats to personal data. It sets out a range of actions that participating ISPs may take to protect their customers from malicious activities that may jeopardise customers’ privacy. Participation in the ACMA’s Australian Internet Security Initiative (AISI) is one of the code’s main elements. The AISI collects data from various sources on computers exhibiting ‘bot’ behaviour on the Australian internet. Using this data, the ACMA provides daily reports to ISPs identifying IP addresses of compromised computers on their networks. ISPs then inform their customer of the compromise and advise them how to fix their computer.

It is notable that in such an innovative environment of personal information practices that there are disparate industry efforts to promote good personal data management and privacy practices. There is a continuing risk that the separate efforts dilute the benefits for citizens and industry, where there is no overarching coherent framework to guide their efforts. Another important component to the success of industry self-regulatory approaches is likely to be effective mechanisms that hold industry participants accountable for compliance. Experience with the MPS market has shown that self-regulatory arrangements may not be effective, if there are strong financial incentives to not comply with self-regulatory measures.

## Direct regulation will continue to play an important role where it can be meaningfully applied

Existing privacy interventions have a strong regulatory emphasis and it is likely that regulation will continue to play an important role in holding organisations accountable for privacy outcomes and promoting confidence in global governance arrangements where digital data is exchanged globally.

To date, personal data protection issues have been addressed by a mix of measures administered by a number of different bodies. Alongside the national privacy framework administered by the AGD and OAIC, the ACMA administers a range of privacy safeguards specific to media and communications-related matters.

While the growing complexity of the digital environment may be undermining the effectiveness of some direct regulatory measures, direct regulatory approaches may continue to be effective in addressing specific problems. Regulators in a number of jurisdictions have already moved to tighten privacy online privacy safeguards, or signalled the possibility of taking such action. Regulation of the use of cookies in the European Union, introduced in 2012, is an example of increased direct regulation being applied. In the United States, the Federal Trade Commission’s inquiry into privacy issues associated with ‘the internet of things’ raises the possibility of increased regulation.[[39]](#footnote-39)

Given the global structure of the personal data environment, international collaboration is likely to play an important role in ensuring that efficient and consistent approaches to privacy and personal information protection. The development of international frameworks for the protection of citizens’ personal data attempts to provide international consistency in this area, and to avoid regulatory anomalies that might otherwise arise when data collection, storage and processing activities take place across two or more jurisdictions.

Measures to address data breaches are another example of where direct regulation may continue to play an important role in protecting personal data. A data breach notification regime that provides strong incentives to protect citizens’ data would therefore contribute to achievement of sound privacy outcomes. The recent introduction into the Parliament of the Privacy Amendment (Privacy Alerts) Bill 2013, would establish such a mechanism to protect Australian citizens.

Privacy and personal data considerations pose a range of regulatory issues that need to be transitioned to the evolving networked digital environment. As the range of social and economic activities being undertaken online increases, so too does the volume of personal data being collected, stored and shared online. The varied contexts in which these practices occur will require safeguards that are tailored to the specific contexts in which privacy concerns arise. However, stakeholders will expect and benefit from a coherent regulatory framework which facilitates the development of logical and predictable outcomes.

# Conclusion

Digital data is the currency of social and economic transactions in the networked society and information economy. Key developments that include high-speed network connections, increases in computing processing power and data analytics have supported increasing volumes of personal information being created, stored and analysed. These developments are also broadening the concept of what personal information means in a digital data environment. It not only includes information that is volunteered and observed about an individual, but also includes inferred information about personal behaviours and preferences.

With these changing practices in the treatment of personal information in a digital data environment comes a widening set of consumer and citizen concerns about data storage and sharing practices. But citizens have a continuing expectation that industry participants and government also assist them in managing their personal information in this environment.

Protection of privacy and personal information has been a core element of media and communications regulation. However, a substantial amount of communications activity is occurring in environments that were not envisioned when the confidentiality safeguards of privacy and communications regulation. This has profound implications for the formulation and administration of regulatory safeguards that are robust but sufficiently flexible enough to accommodate innovation. It underscores the need for issues to be addressed within a single coherent regulatory framework that recognises the evolving forms of personal information in an information economy, as well as the different roles and respective responsibilities of citizens, industry and governments in a networked society.

# Appendix 1

## ACMA research relating to privacy and personal data protection

The ACMA has undertaken a range of research to provide an evidence base to inform the development of regulatory safeguards and other measures aimed at protecting the privacy of Australians in the media and communications environment. The most recent examples of this research include:

* [***Here, there and everywhere—consumer behaviour and location services***](http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/here-there-and-everywhere-consumer-behaviour-and-location-services). This report presents findings of both qualitative and quantitative research into consumer attitudes, behaviour and perceptions of location services, to inform development of appropriate policies and/or educational resources.
* **Unsolicited communications and malware—consumer experiences** (research undertaken June 2012, not yet published).
* [***Digital Australians—Expectations about media content in a converging media environment, Qualitative and quantitative research report***](http://www.acma.gov.au/~/media/Digital%20Society%20Policy%20and%20Research/Information/Word%20Document/Digital%20Australians%20Expectations%20about%20media%20content%20in%20a%20converging%20media%20environment.PDF), October 2011. Examines the impact of the increasing use of digital media on Australians’ attitudes and expectations about media content issues and explores privacy concerns: Chapter 7—Privacy and consumer protection.
* [***Community research on informed consent—Qualitative research report***](http://www.acma.gov.au/~/media/Consumer%20Interests/Research/pdf/Community%20research%20on%20informed%20consent%20Qualitative%20research%20report%20MARCH%202011.PDF),March 2011. This report presents the findings of qualitative research into community attitudes, perceptions and understandings of informed consent across a range of communication platforms.
* [***Attitudes towards use of personal information online*—*Qualitative research report***](http://archive.acma.gov.au/WEB/STANDARD/990952/pc=PC_311473), August 2009.This qualitative research report examines attitudes towards disclosure of personal information when using the internet or other digital media and communications such as mobiles or other devices.
* [**Research undertaken for the review of privacy guidelines for broadcasters**](http://archive.acma.gov.au/WEB/STANDARD/pc=PC_410120), August 2011. Community research into broadcasting and media privacy and Australians’ views on privacy in broadcast news and current affairs.
* [***Click and connect: Young Australians’ use of online social media—02: Quantitative research report***](http://archive.acma.gov.au/WEB/STANDARD/pc=PC_311797), July2009. This research focuses on young people's use of social media, including content, contact and privacy risks.

1. [www.guardian.co.uk/commentisfree/2013/jun/12/david-simon-wrong-nsa-capabilities](file:///C:\Users\bduhigg\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\MVD1MCFU\www.guardian.co.uk\commentisfree\2013\jun\12\david-simon-wrong-nsa-capabilities) [↑](#footnote-ref-1)
2. In the Privacy Act, ‘personal information’ means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics. It excludes information about an individual that is contained in a [publicly available publication](http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/s3.html#publicly_available_publication). [↑](#footnote-ref-2)
3. World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, January 2011, pp. 5–6. [↑](#footnote-ref-3)
4. Forrester research cited in David Zax, ‘[Is Personal Data the New Currency?](http://www.technologyreview.com/view/426235/is-personal-data-the-new-currency/)’ *MIT Technology Review*, 30 November 2011. [↑](#footnote-ref-4)
5. ACMA, [*Communications report 2011–12 series, Smartphones and tablets: Take-up and use in Australia*](http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/communications-report-201112-library-landing-page), 2012, p. 2. [↑](#footnote-ref-5)
6. Nielsen, *Australian Connected Consumers (15th Edition)*, 2013, p. 21. [↑](#footnote-ref-6)
7. Ericsson, *Ericsson Mobility Report—On the pulse of the Networked Society*, June 2013, p. 10, [www.ericsson.com/ericsson-mobility-report](http://www.ericsson.com/ericsson-mobility-report). [↑](#footnote-ref-7)
8. Hoffman, D., ‘Exposing Your Personal Information—There’s An App For That’, <http://forums.juniper.net/t5/Security-Mobility-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058>. [↑](#footnote-ref-8)
9. International Telecommunications Union, *Trends in Telecommunications Reform 2013: Transnational Aspects of Regulation in a Networked Society*, pp. 169–171. [↑](#footnote-ref-9)
10. Meet IAN: Our On-Demand Marketing Analytics, Identification, Verification and Customer Insights Engine, [www.neustar.biz/infoservices/technology/ian](http://www.neustar.biz/infoservices/technology/ian). [↑](#footnote-ref-10)
11. Obiodu, E., ‘Big Data Telco Services Case Study: Telefonica and Verizon Wireless’, Ovum Ltd, 12 March 2013, [ovumkc.com/Products/Telecoms/Telco-Operations/Big-Data-Telco-Services-Case-Study-Telefonica-and-Verizon-Wireless/Telefonica](http://www.ovumkc.com/Products/Telecoms/Telco-Operations/Big-Data-Telco-Services-Case-Study-Telefonica-and-Verizon-Wireless/Telefonica). [↑](#footnote-ref-11)
12. ‘No Hiding Place’, The *Economist*, 25 May 2013. Available at [www.economist.com/news/science-and-technology/21578357-plan-assess-peoples-personal-characteristics-their-twitter-streams-no?fsrc=nlw|hig|5-23-2013|5763538|37806856|](http://www.economist.com/news/science-and-technology/21578357-plan-assess-peoples-personal-characteristics-their-twitter-streams-no?fsrc=nlw|hig|5-23-2013|5763538|37806856|). [↑](#footnote-ref-12)
13. See [Personal.com](https://www.personal.com), accessed 21 May 2013. [↑](#footnote-ref-13)
14. Joshua Brustein, ‘[Start-Ups Seek to Help Users Put a Price on Their Personal Data](http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html?_r=1&ref=business)’, 12 February 2012, *New York Times*, accessed 21 May 2013. [↑](#footnote-ref-14)
15. [*Privacy by Design and the Emerging Personal Data Ecosystem*](http://www.guardian.co.uk/technology/2012/oct/16/google-privacy-policies-eu-data-protection), October 2012, case study of Personal.com, p. 10. [↑](#footnote-ref-15)
16. [Reputation.com](http://www.globalservices.bt.com/uk/en/footer_links/privacy_policy) website, accessed 24 May 2013. [↑](#footnote-ref-16)
17. See [www.rune.com.sg/index.php/products-solutions/products/deadbolt](https://www.rune.com.sg/index.php/products-solutions/products/deadbolt). [↑](#footnote-ref-17)
18. In the Privacy Act, ‘personal information’means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics. It excludes information about an individual that is contained in a [publicly available publication](http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/s3.html#publicly_available_publication). [↑](#footnote-ref-18)
19. World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 2011, p. 9. [↑](#footnote-ref-19)
20. See Appendix 1 for a list of recent ACMA research activities relating to privacy and personal data in the media and communications environment. [↑](#footnote-ref-20)
21. *Unisys Security Index*, Australia, May 2013, available at [www.unisyssecurityindex.com/usi/australia](http://www.unisyssecurityindex.com/usi/australia). [↑](#footnote-ref-21)
22. ibid. [↑](#footnote-ref-22)
23. ACMA, *Digital footprints and digital identities—Community research*, 2013 (unpublished). [↑](#footnote-ref-23)
24. ibid. [↑](#footnote-ref-24)
25. ACMA, [*Australia’s progress in the digital economy: Participation, trust and confidence*](http://www.acma.gov.au/WEB/STANDARD/pc=PC_600063), November 2012,

    p. 1. [↑](#footnote-ref-25)
26. ACMA, *Digital footprints and digital identities—Community research*, 2013 (unpublished). [↑](#footnote-ref-26)
27. ‘How Location-Based Services are Transforming the Mobile Industry’, *Business Insider Australia*, <http://au.businessinsider.com/location-data-is-transforming-mobile-2013-55>. [↑](#footnote-ref-27)
28. ACMA, [*Here, there and everywhere—Consumer behaviour and location services*](http://www.acma.gov.au/theACMA/Library/researchacma/Digital-society-research/here-there-and-everywhere-consumer-behaviour-and-location-services). [↑](#footnote-ref-28)
29. For information about the Financial Coalition Against Child Pornography see [www.financialcoalition.se/internationellt-arbete/](http://www.financialcoalition.se/internationellt-arbete/). [↑](#footnote-ref-29)
30. ‘Beware, Your Favourite App Can Be a Virus’, <http://news.mindprocessors.com/technology-news/beware-your-favourite-app-can-be-a-virus/>. [↑](#footnote-ref-30)
31. ACMA, *Digital footprints and digital identities—Community research*, 2013 (unpublished). [↑](#footnote-ref-31)
32. ACMA, [*Location services, personal information and identity—Exploratory community research*](http://www.acma.gov.au/webwr/_assets/main/lib310665/location_services_research.pdf),   
    pp. 34–35; 54–55. [↑](#footnote-ref-32)
33. Further information about matters covered by the Privacy Act is available at [www.oaic.gov.au/privacy/privacy-act/the-privacy-act](http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act). [↑](#footnote-ref-33)
34. OECD, *Implementation of the 2007 Recommendation on Privacy Law Enforcement Co-operation*, 2010, as reprinted in *Thirty Years After the OECD Privacy Guidelines*, 2011, p. 76. [↑](#footnote-ref-34)
35. OECD, [The Review of the OECD Privacy Guidelines](http://www.oecd.org/internet/interneteconomy/thereviewoftheoecdprivacyguidelines.htm). [↑](#footnote-ref-35)
36. See <http://iabaustralia.com.au/sitecore/shell/Controls/Rich%20Text%20Editor//-/media/IAB/Resources/Presentations%20and%20Guidelines/Social%20Advertising%20Paid%20Guidelines%20April%202013.pdf> [↑](#footnote-ref-36)
37. The Canadian Information and Privacy Commissioner developed the concept of Privacy by Design that promotes the view that compliance is not sufficient to ensure privacy by that instead privacy should be ‘ … an organisation’s default mode of operation.’ Refer [Privacy by Design](http://www.ipc.on.ca/english/privacy/introduction-to-pbd/) websites, accessed 21 May 2013. [↑](#footnote-ref-37)
38. [*Privacy by Design and the Emerging Personal Data Ecosystem*](http://www.guardian.co.uk/technology/2012/oct/16/google-privacy-policies-eu-data-protection), October 2012, case study of Personal.com, pp. 23–29. [↑](#footnote-ref-38)
39. ‘FTC Seeks Input on Privacy and Security Implications of the Internet of Things’, media release, 17 April 2013, [www.ftc.gov/opa/2013/04/internetthings.shtm](http://www.ftc.gov/opa/2013/04/internetthings.shtm). [↑](#footnote-ref-39)