



Australian Government  
Productivity Commission

SHIFTING THE DIAL



5 YEAR PRODUCTIVITY REVIEW

# SUPPORTING PAPER NO. 13

REGULATION IN THE  
DIGITAL AGE

3 AUGUST 2017

© Commonwealth of Australia 2017

ISBN 978-1-74037-641-9 (PDF)



Except for the Commonwealth Coat of Arms and content supplied by third parties, this copyright work is licensed under a Creative Commons Attribution 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/3.0/au>. In essence, you are free to copy, communicate and adapt the work, as long as you attribute the work to the Productivity Commission (but not in any way that suggests the Commission endorses you or your use) and abide by the other licence terms.

### **Use of the Commonwealth Coat of Arms**

For terms of use of the Coat of Arms visit the 'It's an Honour' website: <http://www.itsanhonour.gov.au>

### **Third party copyright**

Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material, please contact them directly.

### **Attribution**

This work should be attributed as follows, *Source: Productivity Commission, Regulation in the Digital Age, Shifting the Dial: 5 year Productivity Review, Supporting Paper No. 13.*

If you have adapted, modified or transformed this work in anyway, please use the following, *Source: based on Productivity Commission data, Regulation in the Digital Age, Shifting the Dial: 5 year Productivity Review, Supporting Paper No. 13.*

### **An appropriate reference for this publication is:**

Productivity Commission 2017, *Regulation in the Digital Age, Shifting the Dial: 5 year Productivity Review, Supporting Paper No. 13*, Canberra.

### **Publications enquiries**

Media and Publications, phone: (03) 9653 2244 or email: [maps@pc.gov.au](mailto:maps@pc.gov.au)

### **The Productivity Commission**

The Productivity Commission is the Australian Government's independent research and advisory body on a range of economic, social and environmental issues affecting the welfare of Australians. Its role, expressed most simply, is to help governments make better policies, in the long-term interest of the Australian community.

The Commission's independence is underpinned by an Act of Parliament. Its processes and outputs are open to public scrutiny and are driven by concern for the wellbeing of the community as a whole.

Further information on the Productivity Commission can be obtained from the Commission's website ([www.pc.gov.au](http://www.pc.gov.au)).

---

# Contents

<b>Key points</b>	<b>2</b>
<b>Regulation in the digital age</b>	
1 Minimising the burden of regulation	3
2 Empowering consumers makes markets work better	9
3 A regulatory system that facilitates innovation	17
<b>References</b>	<b>44</b>

---

## Key Points

Digital technologies can provide new and better ways of regulating.

- A single digital portal can provide an intelligent interface that allows the user to identify all the regulatory permissions and requirements needed to do some specified task.
- Greater cooperation is needed between government departments and across jurisdictions to share data and implement the machine learning needed to get the full value out of the 'one-stop-shop' approach to regulating.
- Digital service standards can greatly assist agencies to adopt a common approach to digital activities, with benefits to all who engage with the agency, including clients, other agencies, and firms seeking to develop service offerings.
- RegTech has the potential to greatly reduce the compliance costs of regulation in some areas. Regulators can facilitate the development of RegTech through timely approval of services as compliant, machine-readable regulation, and information sharing systems.
- The internet is reducing the cost of collecting and disseminating information that can lead to much better informed consumers, able to impose greater discipline on producers. Where there is potential for substantial harm, government action may be needed to ensure that the information made available to consumers is credible. This could allow a more light-handed regulator approach if combined with effective avenues for complaints and access to redress.

Digital technologies are also challenging regulations and regulators, whose slow response can pose a barrier to innovation, and that may still need to act to manage new risks and facilitate new opportunities.

- Regulators should move to a 'Yes, if' approach, unless consumers would struggle to understand the risks posed by the new product, these risks are material, generic regulations do not offer adequate protection, and/or competition would be significantly reduced.
- FinTech could be boosted by more rapid progress in adoption of digital identities, portability of customer data, sharing of credit history data, requiring firm exit strategies, and liberalising payments regulation.
- For the internet of things to thrive, greater coordination of systems and standards is needed to ensure interoperability as well as optimising the investment in supporting infrastructure and cybersecurity.
- Governments are the collectors and curators of much data, and could stimulate new opportunities by making this data available in forms that still protect the security of data and the privacy of the data sources. Governments can also make better use of data to improve their delivery of services and functioning of government.
- Providing consumers access to their own data will enhance their choices, driving innovation as well as efficiency through greater competition. Policies to encourage more sharing of data in the private sector should also see the development of more differentiated services to the benefit of consumers who are less well serviced by the current providers.
- While limited by international agreements, moves to a less restrictive IP regime could stimulate innovation. Fair dealing in copyright law is particularly restrictive and should be replaced by fair use.

---

This supporting paper reinforces the observations made in chapter 5 of the Productivity Review. It considers the ways governments can make markets work more efficiently and improve firm productivity, largely through the lens of the challenges and opportunities offered with digital technologies. It considers ways in which governments can:

- reduce the burden of regulation and with this costs to businesses and the economy
- empower consumers to make markets work better
- facilitate innovation, looking in particular at two areas — FinTech and the internet of things (IoT).

## **1 Minimising the burden of regulation**

As digital technologies can provide new and better ways of regulating, the time is right to put pressure on governments and regulators to lift their game. Regulators can adopt digital solutions to streamline communication that will lower the cost of engagement, develop lower cost compliance monitoring tools (RegTech), and enhance market mechanisms by giving consumers better and more effective avenues of redress to impose market discipline on producers.

### **Digital services offer ways to lower the costs of engaging with regulators**

Simplifying and streamlining how business engage with regulators and government is a theme that has run through all of the Commission’s regulatory reviews. As ACCI (sub. 37) notes:

A major frustration for the business community is the time taken to navigate important information and services. Public services are fragmented and difficult to navigate. (p. 18)

#### **Single portals for information, applications, and reporting lower costs**

Digital services offer a way of providing a much more seamless and integrated process for business seeking information, approvals, notifications and other compliance requirements. They can provide an intelligent interface that allows the user to identify all the regulatory permissions and requirements needed to do some specified task. This interface could offer the user of one link — for example to purchase a recreational fishing licence — others that may be of value — such as information on fishing locations.

To be useful for businesses (or potential businesses), one site could provide the interface to a number of agencies, prompting the user to ensure that they are aware of the full range of regulatory interactions they will need to satisfy, listing all the information required, providing the submission interface, and directing that information to the relevant agency. Machine learning will improve this service over time, so that someone who wants to start a

---

hairdressing business in Bateman’s Bay not only gets the list of federal and state requirements such as occupational licencing, tax arrangements (BAS and PAYG), award requirements, occupational health and safety, public and professional liability insurance, but also local government zoning rules, and other requirements.

There has been progress on the development of at least a single portal for information and routine applications in Australia. For example, the NSW Government has introduced [onegov.nsw.gov.au](http://onegov.nsw.gov.au) where most services that individuals and businesses want to use can be accessed. They have also introduced a single point for all government procurement. Queensland has a business and industry portal, which does link through to individual services. South Australia has a single entry point. Victoria was the first state to sign up to the Commonwealth’s myGov portal as a single authentication platform (in 2014) (Cowan 2014), but their rollout of Service Victoria (along the Service NSW line) has been slower than expected (Donaldson 2017).

The different approaches raise the question of why, like in the rollout of myKi and Opal, each state feels the need to develop their own unique system. But at least the objective was similar, unlike the Australian Government, which abandoned the single GOV.AU website that was being developed by the Digital Transformation Office — now the Digital Transformation Agency (DTA) — in favour of trimming the 1500 websites and lifting digital standards (Cowan 2017; Towell 2017). The 2017-18 Budget included funding to the DTA to develop a single platform payments system, a simplified system for handling digital notifications, and the ‘Tell Us Once’ service that will update residents’ details across all Commonwealth agencies (Australian Government 2017b).

But more could still be done. This includes better linking Commonwealth and state regulators for businesses that need to meet regulatory requirements at both levels of government. There may well be a case for the Australian Government to delegate the interface for some of their regulatory responsibilities to state and territory governments, if they are the likely first point of contact for firms seeking to undertake new activities. There are moves to develop an end-to-end approvals process for business transactions across all three levels of government, with a test to be undertaken with Parramatta Council and the NSW government (Riley 2017). All levels of government should have an interest in speeding this process, and states that have yet to develop their own single portal should piggy-back on this development rather than reinvent yet another wheel.

Implementation of digital solutions requires buy-in from the different regulators (and their policy departments). This, rather than the technology, can be the bottleneck that slows the process and adds costs. The need to change processes to manage and respond to a digital flow of information can be challenging for agencies and requires skills in change management that may not be available. Risk averse organisations can also be reluctant to delegate even an interface to others, while concerns over the implications for the future of the agency can hinder cooperation. To overcome these sources of reluctance, governments need to fund the transition, and to make it clear that delivery of the one-stop, end-to-end, regulatory communication and approvals process is not negotiable.

---

## Digital standards can make it easier for business to engage

There are models, such as the UK Digital Service Standard, that can assist regulators to develop online services that are easy for businesses (or the general public) to use (box 2). These standards will make government agencies much more responsive as circumstances change, and provide much greater scope for agencies to actively manage the risks associated with online services. Critical elements are the development of in-house capacity and control to allow a continuous improvement model.

Using open source code also brings in much more expertise to assist when problems arise, as well as saving time and money by not reinventing already well tested platforms and code. The model of agencies paying firms to deliver a black box IT solution locks in obsolescence and should not be used except for one-off needs.

Adoption of standard business reporting (SBR) would facilitate the uptake of other digital technologies. SBR is a standardised approach to online or digital record keeping, which incorporates standardised terms used in government legislation and reporting. When it is built into account keeping software, it allows businesses to generate, check and submit reports to government using AUSkey (a secure reporting portal). SBR enabled reports include common Australian Securities and Investments Commission (ASIC), Australian Taxation Office (ATO) and superannuation reports, and payroll tax reports for jurisdictions. The Commission assessed the potential benefits of SBR as in the order of \$500 million a year (PC 2012).

The Australian government has been trying to promote the adoption of SBR since 2010, yet uptake has been slow. This appears to be largely due to lack of awareness, as it was hard to trial SBR and the observability of benefits were low (Lim and Perrin 2014; PC 2012).<sup>1</sup> But it may well be that businesses do not see sufficient value in changing existing processes just to access this functionality, so adoption rates reflect the pace of accounting software updates. As awareness grows and more software is developed that uses the SBR functionality, adoption rates should increase. But it is an illustration of the chicken and egg problem, where low awareness dampens both demand and supply responses — business need to see value in changing their software so that developers see value in investing in applications, which in turn deliver the value businesses need to see.

---

<sup>1</sup> The ‘diffusion of innovation’ model explains the rate and profile of adoption in terms of relative advantage, compatibility, complexity, trialability and observability.

---

## Box 2      **UK Digital Service Standard**

- Understand user needs — develop a deep knowledge of who the service users are and what that means for the design of the service
- Ongoing user research — plan for ongoing user research and usability testing to continuously improve the service
- Have a multidisciplinary team — with the skills to design, build and operate the service, with oversight by suitably skilled managers with decision making responsibility
- Use agile methods — build your service using iterative and user-centred methods
- Iterate and improve frequently — build your service so it can be iterated and improved on a frequent basis and make sure that you have the capacity, resources and technical flexibility to do so
- Evaluate tools and systems — to choose tools and systems that will be used to build, host, operate and measure the service, and how to procure them
- Understand security and privacy issues — evaluate what user data and information the digital service will be providing or storing and address the security level, legal responsibility, privacy issues and risks associated with the service (consulting with experts where appropriate)
- Make all new source code open and reusable — publish it under appropriate licences (or provide a convincing explanation as to why this can't be done for specific subsets of the source code)
- Use open standards and common platforms where available — including GOV.UK Verify as an option for identity assurance
- Test the end-to-end service — in an environment identical to that of the live version, including on all common browsers and devices, and using dummy accounts and a representative sample of users
- Make a plan for being off-line — to manage the event of the digital service being taken temporarily off-line
- Make sure users succeed first time — create a service that is simple to use and intuitive enough that users succeed the first time
- Make the user experience consistent with GOV.UK — build a service consistent with the user experience of the rest of GOV.UK including using the design patterns and style guide
- Measure and report on performance — collect and analyse performance data to guide continuous improvement, identify key performance indicators, including the key four ones, and report on this data
- Test with the minister – test the service from beginning to end with the minister responsible for it.

*Source:* UK Government (2017).



---

#### CONCLUSION 13.1

Greater coordination is needed between state and territory and the Australian governments to make better use of the digital opportunities:

- in linking the entry portals for business and others to:
  - support a ‘no wrong entry’ system in regard to regulatory information
  - offer integrated (end-to-end) application processes for all regulatory licensing and approvals
- adopting AI methods to improve the quality of the advice and service provided to businesses and others seeking information on regulatory requirements
- providing clear guidance on digital standards to all agencies that are technology neutral, consistent across agencies and jurisdictions, and are supported by the business community.

### **RegTech can improve the performance of regulators**

RegTech describes digital solutions that enable firms to meet regulatory requirements at considerably lower cost — embedding ‘compliance by design’. At the World Economic Forum in January 2017, for example, participants were told that ‘as many as 50 000 finance sector compliance jobs’ could be replaced by RegTech solutions (Head 2017). ASIC held a forum in early February 2017 with RegTech companies to explore opportunities.

There are many digital technologies that could improve the ways in which regulators monitor compliance and assess risk. These include blockchain, cognitive computing, the internet of things (IoT), open source and Application Programming Interface (APIs), the cloud and big data. Even digital technologies such as pre-filled forms, and the ability to check whether information entered is likely to be accurate (at the low-tech end of RegTech) can help firms with meeting compliance requirements, such as making sure that customers know what they are signing up to.

At the high-tech end, sensor data could allow some businesses to automate how they prove compliance with regulatory requirements by directing data straight to the regulator. The ability to share data in real time, or closer to real time, would allow regulators to quickly identify if risks are emerging and to advise the firm accordingly. It also means that they only need to contact firms if problems are identified. Compliant firms would not need to do additional reporting. Over time, the data provided could be analysed to better assess where risks actually do eventuate and the consequences of both the regulatory response and the failure to manage a risk (which may well be far less than anticipated). This would enable a much more informed risk-based approach to regulating.

There is value to governments in RegTech solutions. The ATO is developing a single touch payroll system that will require employers (with more than 20 employees) to report payroll and superannuation online as payments are made. This is an example of what can be done with digital technologies, providing better information to monitor compliance,

---

such as the payment of employee superannuation (which can be a problem for failing firms, and end up costing the Government as well as employees). ASIC's Innovation Hub, established in 2015, reported engagement with 30 RegTech companies (Head 2017). The NSW Government has recently released a new digital strategy, with commitments to make the client the centre of service delivery (Bajkowski 2017b). An important aspect of this strategy is to ensure that all legislation enables digital by design — that is, it will not prevent new digital technologies and business models from being adopted.

The private sector sees benefits in investing in RegTech solutions — as demonstrated by the establishment of the RegTech Association in March 2017 (Eyers 2017). The members of the Association see scope in providing apps and other software solutions to firms that will enable them to meet their regulatory obligations, including (but not limited to) reporting requirements.

Machine learning offers the opportunity to distil information on regulatory requirements in a way that can be tailored to the needs of individual firms. If regulators work with RegTech firms, such as by making de-identified data on regulatory actions and compliance available for analysis, intermediaries can assist firms to be compliant for least cost. Data 'matching' where red flags are identified from the regulator's data and these are shared with RegTech firms, rather than data sharing, reduces the scope for misuse of the firm level data. By providing information on the characteristics needed for compliance and those that are problematic, the intermediaries can use their firm-level data to identify the advice they need to give to their clients. The upshot will be that regulatory outcomes improve at a lower cost to business.

Engagement with regulators will be needed to ensure the development of this new set of intermediaries. There is concern in the industry that regulators can be too slow to act, so the big firms, that are potential clients for the new platforms, develop their own solutions (Head 2017). Open access technologies are to be preferred, and regulators should ensure that APIs or other interfaces allow others to read and write data to the regulator's system. The scope to improve regulatory compliance at a lower cost is considerable.

There are challenges that come with trying to design regulation in a way that enables the RegTech applications. Specific rules (such as 'the three measurable things will be done') can be easier to implement (particularly with RegTech) compared with broader principles (such as a requirement to be fit for safe use by an 'average' person). But specific rules are less flexible and have the risk of leading to tighter regulation and higher regulatory cost overall (as tight standards can limit entry or limit the ability to differentiate products). Whereas RegTech will make application of specific rules cheaper, this may move regulation away from the more principles-based approach.

One way this tension could be addressed is to enshrine the principles in the primary legislation and allow regulators to offer guidelines that provide a machine readable interpretation, as well as the more nuanced principles approach, on the understanding that the machine readable rules are subject to change if firms are found to be evading the

---

regulatory intent. Here too, a balance is needed that requires policy departments to provide clear guidance to regulators on how to proceed.

The courts can also play a role here, as they can be called on to interpret how the principles enshrined in legislation apply in practice. The common law system allows for courts to provide guidance on how regulation should be applied. This would be another route through which regulators can update their approaches as technology changes.

For RegTech to develop it needs:

- timely approval or recognition by regulators that the tool delivers on reporting or other regulatory requirements
- machine readable regulation that is not ambiguous or open to interpretation
- private and public information systems that can transfer and share information in real time
- cultural change in regulators ‘from policeman to coach’.

Finance is one of the most prospective areas for RegTech. Once proven it has potential to be applied across many industries.

#### CONCLUSION 13.2

For the RegTech industry to thrive and deliver lower regulatory compliance costs, governments need to provide:

- regulation is digital by design
- a regulatory framework that welcomes digital solutions
- access to deidentified regulatory data, under secure unit record conditions.

Policy departments need to provide guidance to regulators on the balance between moving toward more specific rules that support RegTech solutions and a principles-based approach, given that specific rules have the potential to create unintended distortions.

## **2 Empowering consumers makes markets work better**

A regulatory system that empowers consumers, through information and effective complaint and redress systems, helps bring market discipline to bear on providers. Digital technologies can greatly address the source of market failure known as ‘information asymmetry’ — where providers know a lot more about a product than their consumers are able to find out. For this to reduce the need for regulation, the information must be credible, and redress for harm suffered as a result of purchasing a product must be accessible.

---

## Digital technology can support the provision of credible information

Where the seller knows more about the product (good or service, including labour) than the buyer, the market outcome can be less than ideal. It matters most where transactions are infrequent so the opportunity to learn is low, and they involve financial or other risk to either party to the transaction. In such cases governments can:

- ban or put limits on who can undertake what activities, for example by licencing of professions. While these approaches can be required where the risks and associated costs are high, requirements to meet certain minimum standards can drive up costs, and prevent informed consumers from making a quality-price trade-off that they might prefer.
- mandate provision of information, such as energy ratings information on whitegoods, and food labelling. This imposes costs on firms to provide this information in the form required, and getting agreement on labelling requirements can be hotly debated. The food labelling health ‘stars’ system, for example, fell well short of the intent of its advocates (Lawrence and Pollard 2015).

Easier access to information can reduce the need for government to intervene, and perhaps deliver enough confidence in the consumer’s capacity to know what they are buying to reduce the need for some bans and other restrictions on activities.

The internet reduces the costs of disseminating information. Platform-mediated exchanges, such as Uber and Airbnb, that match buyers to sellers (of ride services and accommodation respectively) aggregate the experiences of users, overcoming the problem of knowing the performance of a provider when their service is used only once by most consumers. The impact of reports of poor services on a provider’s reputation and future sales provides a discipline to deliver as promised (PC 2016a).

Whether better access to information will resolve as many problems as has been claimed (for example, Thierer et al. 2015) needs to be examined. In some areas, such as a ride-sharing service — where the quality of a service is easy to assess, the risk of a very bad outcome is low, and there are many repeat users reporting on their experience — this is undoubtedly true. But there are other areas, such as the proficiency of an orthopaedic surgeon, where this presumption is harder to make. This can be because information alone may not be sufficient to inform choice where decisions have to be made in times of duress, or processing the information into decision criteria goes beyond the capabilities of most consumers.

Where consumers are not in a position to exert discipline through their own purchasing behaviour or unable to share information that affects the reputation of the brand, performance metrics can still encourage producers to lift their game (SP 3). This has been found to be a factor in provision of medical services in the United Kingdom, as hospitals and doctors that were reported as below average have lifted their game not just to protect their reputation, but also from professional pride in what they do (chapter 2). Here too,

---

digital technologies offer ways to disseminate information at a much lower cost. The challenge is to do this in a nimble, low-cost way.

With sufficient access to data, firms may well develop as intermediaries, playing the role of trusted brokers. TripAdvisor, for example, has become the bible for some travellers, and unlike ‘Let’s Go’ and other travel information, it is likely to reflect the latest information. Crowdsourcing the information also reduces the scope for businesses to mislead consumers.

These features give users reasonable confidence in the information, but in other situations information quality is harder to establish. For example, if consumers can struggle to assess the quality of the service rather than their individual outcome (a slow recovery from a hip operation may not be the surgeon’s fault) or feel compelled to be positive in their response, some form of quality assurance for the information provided is required.

In other cases, too much information can confuse. Aggregator websites (for example, for insurance) can assist in providing comparator information, but often the products vary across so many parameters that it is difficult to compare like-with-like.

The responsibility for minimising risks with bad outcomes and certifying the accuracy (or at least authenticity) of information could be assumed by the industry. But this poses some risk that certification can be used as a barrier to entry. A social organisation might be able to take on the role, although they too may have a particular perspective. Where these types of ‘market’ solutions pose unacceptable risks, information provision mediated by government can help the market function for efficiently.

Governments may need to be involved in the provision of information to consumers on the performance of a provider or product in any of the following situations:

- providers need to be legally required to provide the information — that is, they would not do so voluntarily
- all feasible indicators of performance could easily be gamed — so their accuracy will be doubtful without penalties for false or misleading information
- the consequence for consumers of a poor choice is high — information alone may be sufficient where the issue is that consumers would have made a different choice (such as not to have a medical procedure if it has been found to be ineffective), but it might be inadequate where the consequence is actual harm — for example, procedures being undertaken by health practitioners who were not competent in the procedure
- the choice of a good or service is one-off and it is difficult for consumers to change provider — making the initial choice more important (such as for university education — SP 7)
- Government is a substantial funder of the service, either directly or through tax or other subsidies.

---

Where there are well known behavioural biases,<sup>2</sup> information can be tailored to provide the right nudge to avoid these biases. As firms will make use of these biases to sell people things that they don't need or that are inappropriate to their needs, and/or that cost more than they should, government intervention may be required to ensure that information is designed to help overcome these inherent biases. Requiring credit card bills to prominently display the full amount owed (rather than the minimum repayment), and providing information on the total cost of just making the minimum repayment, is an example.

Government should also encourage firms to increase their provision of information in digital form. For example, the UK Competition and Markets Authority found that it was not enough to remove regulatory impediments to consumers to switch banks, and that comparable information on products was needed. (The ability of consumers to access their own data is discussed below). In response, they mandated the retail banks to provide an API that allowed access to information on all the products offered by the bank to retail clients (Nicholls 2017).

As a major collector of information on firm behaviour, regulators should consider how their data could be used to provide information to help consumers assess performance of industries, firms and products, either directly or by providing it to a third party that could offer an advisory service. As with RegTech, requirements to deliver information in hardcopy should be reassessed, as digital delivery can lower costs for producers and makes it easier for information to be made available.

### Complaints registers can be an important feedback mechanism

Regulators can also assist in publicising poor performance through open consumer complaints registers. The Commission's recent study on Australian Consumer Law (PC 2017a) concluded that a publicly accessible register of information on consumer complaints and product safety incidents would enhance consumer protection. Recognising the potential for vexatious complaints and proportionality the Commission laid out a set of principles that should guide the register (box 4). They did not go as far as recommending that a national complaints register be established, noting that NSW Fair Trading will evaluate the NSW Complaints Register after 12 months of operation.

---

<sup>2</sup> The main causes of cognitive biases affecting market choices are bounded rationality and cognitive dissonance (reflecting time inconsistency in choice, as in the purchase of clothing and food that are never used), use of heuristics and attribute substitution (where choice is made on only one or a few attributes or assumed attributes, such as red cars go faster), and being guided by emotion (as the upselling of funeral packages indicates).

---

#### Box 4      **Principles to guide a complaints register**

A public complaints register should have the following features:

- appropriate vetting mechanisms to minimise listing of frivolous or vexatious complaints
- detailed information about the complaint or incident, such as identifying the product and the nature of the problem. Personal details would be omitted for privacy reasons
- information on the resolution or outcome of the complaint. This should be as fulsome as practicable and could include: how the complaint was resolved and in whose favour, or if it is still pending; scope for the business to provide a response; and details on the actions of the regulator (such as whether the complaint has led to the regulator taking some form of enforcement action)
- a mechanism to place complaints and incidents in context, for example, by weighting them against sales volume. Clearly there are practical difficulties in determining this information for all suppliers or products, but there should at least be scope for businesses to provide this information as part of their response
- appropriate consultation, with both consumer and business groups, both in the development stages and to subsequently review the effectiveness of the register.

*Source:* PC (2017a, p. 164).

#### CONCLUSION 13.3

Digital platforms offer new ways to collate and compare information, which can better inform consumer choice. Governments may need to prompt industries to ensure that information is accurate and made available in a way that supports comparability. In making information available, governments should be aware of the cognitive biases and work to ensure that information is provided in way that assists consumers and businesses to make more efficient choices.

### **Redress must be provided by effective consumer protection regulation**

While improving the information available to consumers enhances their ability to impose market discipline, these mechanisms work best where there are strong consumer protection measures in place. That is, market participants that seek to exploit consumers, workers and other organisations face sanctions, and those harmed have the right to and can access redress. This requires consumer protection regulation with teeth, and regulators that have the capabilities (skills, culture and resources) to implement the regulation.

The main areas of law that govern consumer protection are:

- the Australian Consumer Law (ACL), which replaced 20 federal, state and territory fair trading laws from November 2011, is administered and enforced jointly by the Australian Competition and Consumer Commission (ACCC) and state and territory consumer protection agencies (with the involvement of ASIC on relevant matters)

- 
- The *Australian Securities and Investments Act 2001* and the *Corporations Act 2001*, which apply to financial products and services (including banking services, credit, insurance and superannuation) are administered by ASIC
  - The *Fair Work Act (2009)* administered by the Fair Work Commission. There are also a range of other laws that help protect workers, such as the *Safety, Rehabilitation and Compensation Act (1988)*, and state laws.

In addition to these broader laws there is specific consumer protection at a national level through laws relating to the: National Credit Code, telecommunications and media services, therapeutic products, food standards, and trade measurement. Consumer protection is delivered through the ACL and these laws are enforced by a large number of institutions.<sup>3</sup> The effectiveness of these institutions depends on their ability to gather and act on information where consumers' rights have been violated. From a consumer's perspective, their confidence in the market depends on the effectiveness of the regulators, and on their ability to apply for and receive redress should they suffer unforeseeable harm from their purchase of a good or service.

It is worth noting that the systematic defence of consumer rights does not ensure all consumers who suffer harm will get redress. No system is perfect, and limits are needed to prevent consumers from exploiting the system. There is also a balance to be achieved as consumers need to be motivated to do due diligence on their purchases, and not rely on the system to protect them from the consequences of their own choices.

Nevertheless, the threat posed to firms by the consumer protection system and exposure to fines and redress can be a critical incentive for firms to deal fairly with consumers, and hence for the market to operate effectively (box 5). It is unclear if the Australian system is adequate in this regard.

The ACL is currently being reviewed (by Consumer Affairs Australia and New Zealand) to see if the law is working as intended, reducing the risk of consumer detriment, while minimising the compliance costs. As input into this broader review the Productivity Commission has recently completed a review of the multiple regulator model, which was found to be working well, albeit with scope for improvement. This review emphasised the importance of a well-functioning consumer redress system, noting that it matters for consumer confidence to send a signal to businesses on the need to comply, and that it can be used to assist regulators to identify systemic consumer issues (PC 2017a, p. 241). Problems were identified with:

---

<sup>3</sup> For example, the Age Care Complaints Commissioner deals with complaints about the quality of care in residential aged care services that receive funding from the Australian Government. The Advertising Standards Board can hear claims of false or misleading advertising. The Australian Press Council responds to complaints about print media (including websites). Consumers with problems with any health or allied health practitioner can complain to the Independent Health Services Commission in each jurisdiction.



- 
- the limited powers of the state and territory ACL regulators, most of whom cannot compel businesses to participate in dispute resolution, nor make determinations
  - gaps in the alternative dispute resolution (ADR) arrangements, such as those offered by industry ombudsmen
  - the ACL reliance on civil litigation as the main avenue for consumers to seek redress. While statutory and industry ombudsman can provide redress, the ACCC does not. Indeed, consumers may be unaware that any action has been taken.

**Box 5            Improving consumer protection requires regulators with teeth: the example of financial advice**

The need for improvements in consumer protection in the finance, insurance and superannuation industry is well illustrated by the cases of exploitation of vulnerable consumers, such as by STORM Financial. The then Government responded to concerns about the way in which financial planners were remunerated in the Future of Financial Advice (FOFA) reforms that were made mandatory from July 2013. These were subsequently amended and a revised weaker Bill (the Corporations Amendment (Financial Advice Measures) Bill) passed in March 2016.

These revisions limited the ban on ‘receiving benefits that could influence the advice’ to ‘personal advice’ and removed ‘promoting basic banking and insurance products’ from conflicted remuneration. As most clients seek general advice, these changes have been labelled as ‘unhelpful and unfair’, given that about 70 per cent of financial advisers are owned by or related to the four big banks and AMP (Smith and Poologasundram 2014).

Recommendations to strengthen product issuer and distributor accountability, and lift standards of competency and transparency for financial advice were made in the Financial System Inquiry (Murray 2014, chap. 4). In response, the Government commissioned the Ramsey Review, and announced in the 2017 budget they will establish the Financial Complaint Authority (AFCA) (Australian Government 2017b). The AFCA will replace the current three financial ombudsmen, and provide more resources to address customer disputes with banks and other financial intermediaries. It remains to be seen whether this new regulator will be an active deterrent to poor behaviour by the banks and other firms offering financial advice.

The cost of civil litigation, and the lengthy processes, puts redress out of scope for many people. Unsurprisingly, consumer complaints have been found to be the highest area of unmet legal need (PC 2014). The Commission recommended an independent review of consumer ADR mechanisms to be tasked with addressing these problems (recommendation 6.2).

The Commission’s inquiry into Access to Justice made recommendations to improve third party litigation funding and make it less risky for law firms to take on litigation for retail clients (PC 2014, chap. 18) (box 6). The Commission also made recommendations to streamline and strengthen the ombudsman and complaints system (PC 2014, chap. 9). The Government has yet to respond to these particular recommendations.

---

## Box 6      **The Commission's Access to Justice recommendations**

In its 2014 Access to Justice Arrangements report the Commission noted the potentially large gains from early and informal solutions, including through ombudsmen and alternative dispute resolution. It recommended that:

- government and industry raise awareness of ombudsmen, including among providers of referral and legal assistance services
- governments look to rationalise the ombudsmen services they fund to improve the efficiency of these services
- courts incorporate the use of appropriate alternative dispute resolution in their processes, where they are not already doing so, and provide clear guidance to parties about alternative dispute resolution options.

The Commission also noted that aspects of the formal system are contributing to problems in accessing justice, including 'creeping legalism' in tribunals, uneven reforms in the court system, the adversarial nature of the system and that not all parties are on an equal footing. It recommended that:

- tribunals enforce processes that enable disputes to be resolved in ways that are fair, economical, informal and quick. Restrictions on legal representation should be more rigorously applied
- all courts examine whether their processes for case management, case allocation, discovery and the use of expert witnesses are consistent with leading practice
- statutory obligations be placed on parties and enforced to facilitate just, quick and cheap resolution of disputes. Targeted pre-action protocols may also assist
- a more systematic approach is required for determining court and tribunal fees, in which fees are set to recover a greater proportion of costs, depending on the characteristics of the parties and the dispute. Fee waivers should continue to be provided for disadvantaged litigants.

Other recommendations focused on improving legal assistance services for disadvantaged people, data collection and reporting, assisting the 'missing middle', and improving information for consumers.

*Source: (PC 2014).*

---

### CONCLUSION 13.4

Regulators demonstrable capacity to act to enforce consumer protection laws is key to consumers having confidence in the market. But the ability to address systemic risks is not sufficient — consumers need access to redress. In addition to responding to the recommendations of the Ramsey Review that seek to address concerns in financial services, the Commission's Access to Justice report made a number of recommendations aimed at improving the capacity of people to seek redress for harms. These reforms have the potential to improve consumer confidence in the market system.

---

## Regulators need to become more consumer centric

While consumers (and workers) can turn to the current system to seek redress, it is the activity of regulators responsible for enforcing consumer protection regulation that determines how much it disciplines firm behaviour. STORM and other financial imbroglions have led to doubts about the capacity of regulators to enforce the law. The Murray Inquiry recommended that all regulators of financial institutions undergo periodic capability reviews to assess if the regulator has the ‘skills and culture to be effective in an environment of rapid change’. The ASIC Capability Review (Australian Government 2016) found large gaps between the external expectations of ASIC and ASIC’s own view. The Government has responded by strengthening powers and resources of ASIC (Morrison 2016a). The regulator’s response to the 34 recommendations has been positive, but to achieve a more risk-based mindset will take culture change — which has to come from the top.

The culture of the regulators responsible for enforcing consumer protection regulation is important. They need to be consumer centric in identifying and acting on systemic risks (such as those that arose with the structure of compensation for financial advisers), but not so reactive that they prevent products being on the market that would be valued by consumers who are aware of the risks. To do this regulators need clear guidance on the acceptable levels of risk in the system so that they can offer firms permission to innovate. This guidance should be set out in the Minister’s Statement of Expectations, and the Regulator’s Statement of Intent should set out how much risk is considered acceptable, and the scope for those who are disaffected to seek redress (PC 2011). While the level of performance reporting by regulators has increased it is governments holding the senior management of the regulators to account against expectations that will drive cultural change. And it is the Minister’s job to explain to the Australian public why some risk must be borne, not to blame the regulator when idiosyncratic events within the defined risk profile do occur, as they will on occasion.

### CONCLUSION 13.5

Capability reviews of regulators can be an effective tool to prompt reform, but culture change has to start from the top. Ministers need to make the Government’s risk appetite clear in the Statement of Expectations, and hold regulators to account in delivering against their responding Statement of Intent.

## 3 A regulatory system that facilitates innovation

Although there is some debate about the potential of digital technologies to transform economic activity in the way that railways, electricity and the telephone have done in the

---

past,<sup>4</sup> few dispute the acceleration in the pace of change. For example it has been estimated that it has taken an average of 16.1 years to reach IP saturation (defined as 3 or more IP addresses per person), compared with 100 years for steam power and 60 years for electrification (Ackermann, Angus and Raschky 2017). This pace poses challenges for regulators that have to ensure that the technologies and products do not pose an unacceptable personal, environmental, or social risk (box 7).

### **Box 7      Some digital developments that are challenging regulators**

Some of the challenges for regulators are:

- Being an early mover increases the probability that the firm's IP drives the standard, so to be successful in fast moving markets, firms may need to be able to clear the regulatory hurdles quickly (Brynjolfsson, McAfee and Spence 2014).
- Market power from networks poses new challenges. For example, where a firm can develop a network of users, this provides data that can be used to enhance the product, as Google has done with its search engine. For firms offering intermediation services, such as Airbnb, the network — the extent of the connections they can provide — is a large part of the service. This gives some firms considerable market power that may need to be regulated.
- There is greater scope for firms to outsource the lower value-added parts of the production value chain, enabling concentration on the design and development and the marketing and distribution ends. This can make it difficult for firms to identify the regulators with which they must engage.
- When a firm takes on more of an organising role, either coordinating outsourced activities along the whole value chain, or acting as a platform to mediate exchange (as with Uber), it can be unclear what party is responsible for upholding the regulations. For example, if Uber drivers are considered independent contractors then they face regulatory requirements, while if they are employees then the firm is responsible.
- There can be uncertainty about what party faces the legal liability for a product that causes harm, where the design of a product, its manufacture, and its marketing are all outsourced. Ponoko, a New Zealand firm, which produces on-demand manufactured goods, has 12 digital 'maker centres' operating in the United States, the European Union and New Zealand (PC 2016a). For a regulator, this raises questions about where liability for a faulty product would lie — at the software point or the point of 3D printing.

A regulatory system that is responsive would be quick to resolve these questions, but if regulators are risk-averse, they may err on the side of subjecting all parties to the same regulation. A regulatory system that is responsive and permissive would respond to actual risks. To illustrate the point, we focus on developments that pose regulatory challenges — those that affect the adoption of the IoT and the development of FinTech.

---

<sup>4</sup> See for example Schwab (2016) who labels digital technologies the 'fourth industrial revolution' while Gordon (2015) argues that digital technologies lack the transformative power of previous revolutions.

---

## Removing barriers to innovation

Market opportunities for new technologies and products can have only brief windows of time in which a firm needs to move rapidly to establish their product. So being able to ensure that new products meet regulatory requirements quickly can be critical in bringing them to market. This requires a highly responsive regulatory regime that also gives consumers confidence that the risks are managed. With digital technology accelerating the pace of change, regulators can struggle to be responsive, creating an environment of uncertainty that can hamper innovation.

Regulatory issues that can pose a barrier to innovation include:

- regulation that dictates the type of technology that must be used, or process followed
- regulation that bans some types of technology (or uses of technology) that may have been problematic in the past, even where those risks have fallen and can now be managed
- high costs of, and delays in, seeking and gaining approvals for new technologies, processes or outputs
- the public nature of intellectual property (IP) applications combined with delays and costs that erode the first mover advantage
- the risk that new technologies will not be approved (or that approval will be delayed) or that technologies will subsequently face high barriers to entry, reducing the incentive to innovate.

Many of these issues arise out of a lack of clarity about what regulator is responsible for new technologies — they can fall between the cracks or, more problematically, be in a contested space between regulators. Approaches may differ between jurisdictions, adding another layer of complexity. Coordination between regulators to resolve these issues quickly is needed (see below).

One question is whether a positive list approach to regulation — where activities require permission to occur, or outcomes have to be approved — acts as a barrier to new technology. This is the ‘No, but’ approach to regulation, where ‘but’ defines what a firm must do to be compliant — sometimes at a highly directed level. In a rapidly changing business environment, it can be very hard for regulators to keep the list up to date with activities that are compliant with the objectives of the regulation.

A negative list approach, where permission can be assumed unless something is prohibited, could reduce regulatory uncertainty for innovative activities. This is a ‘Yes, if’ approach, where the ‘if’ is about achieving the objectives of the legislation rather than how these objectives must be satisfied. Such an approach was proposed by the IPA (sub. 15), which cited its submission to the Commission’s inquiry into Business Set-up, Transfer and Closures (the ‘Business Inquiry’):

---

Permissionless innovation is critical because it allows market trial-and-error, learning and experimentation. Regulators must understand that no one knows the future of technology, or what it must be used for. What is historically evident is that this can be determined by the free market. (p. 19)

The ATA (sub. 19) also support implicit permission recommending a:

... policy approach that considers the current contribution of disruptive technologies to productivity by allowing for “bottom-up, organic, self-regulating institutions” before “introducing top-down government control.”(p. 7)

The Harper Review suggested that innovation in service delivery should be encouraged through positive, flexible regulatory frameworks, that ‘market regulation should be as ‘light touch’ as possible, recognising that the costs of regulatory burdens and constraints must be offset against the expected benefits to consumers’ (Harper et al. 2015, p. 24). Where emerging technologies and delivery models disrupt infrastructure markets, governments should respond quickly to ensure regulatory settings maximise productivity growth and reflect the long-term interests of customers. The Commission’s Business Inquiry recommended that ‘regulatory holidays’ be allowed for innovative new products, noting that this would require a legislative framework allowing fixed-term exemptions with safeguards. They also pointed to the need to review industry specific regulatory approaches (PC 2015a).

Some (such as Thierer 2014) have argued that digital technologies will encourage industries to self-regulate. The ATA (sub. 19, p. 7) points to the greater potential for self-regulation through agencies such as the Australian Digital Currency Commerce Association. Self-regulation by industry can be encouraged by the threat of government action if industry fail to address risks. This threat of action should extend to situations where some industry players seek to exclude competitors in the way they establish self-regulation. Regulators need to continue to be vigilant in overseeing the consequences of self-regulation and need to have the power to act if self-regulation is anticompetitive, or otherwise failing to meet its objectives.

Some technologies are just difficult to regulate. For example, as they are created in the cloud, the supply of bitcoin and other digital currencies are hard to regulate directly. And while it could be possible to apply anti-money laundering measures (such as customer due diligence) at the point at which they are used for payment, it could be difficult to require reporting of suspicious activity, as identification can be avoided (Shillito and Stokes 2015).

In these cases, regulators need to work with industry on how to best identify risks. For example, the Australian Transaction Reports and Analysis Centre (AUSTRAC), which is Australia’s anti-money laundering and counter-terrorism financing regulator and specialist financial intelligence unit, undertakes data matching exercises to inform payments providers of their risk exposure. AUSTRAC have identified the need for a high-level guiding legislative framework and an agreed set of rules that determine the operation of the algorithms encoded in the software, to ensure that new technologies, such as blockchain, are adequately regulated in their application to financial data (Australian Treasury 2017).

---

Given the risks of new technologies can be considerable (for example in the area of chemicals), it would be unwise to simply switch to a negative list across all regulators. In testing whether permission could be the default (the ‘Yes, if’ approach), regulators (and government) need to consider whether:

- consumers would struggle to assess the quality of the product (information asymmetry)
- consumer protection regulation and the institutions that administer it are adequate to manage the risks to consumers (similarly, whether occupational health and safety and workplace relations laws adequately manage risks to workers, and environmental laws manage the risks to the environment)
- the harm to consumers (or workers or the environment) that could be caused would be material
- it would restrict competition by locking in a proprietary technology, or providing control over data that would be essential for others to enter the market.

For firm activities that do not pose these risks, consumer protection regulation may well prove adequate, and permission could be assumed. However, in other areas, specialist knowledge may be required (such as in electrical safety) to be able to assess the risks. As regulators tend toward risk aversion and are less likely to give permission where they have any doubts, it is likely they need to be ‘nudged’ toward a less restrictive approach. Policy departments could provide guidance to their regulators on the thresholds they should apply.

The Commission’s Business Inquiry also looked at how regulators could respond to the challenge of innovative products. They concluded that some regulators, such as ACCC and ASIC, have the power to provide a conditions-based regulatory exemption, providing it meets a public benefit test. They suggested that this model would reduce the need for constantly reviewing and updating regulation in order to accommodate some new product — which has been described as a patchwork approach. The Commission went on to recommend:

All jurisdictions should provide a legislative framework for fixed-term exemptions to specific regulatory requirements that deter entry by business models that do not fit within the existing regulatory framework. Such regulatory exemptions should be disallowable instruments and subject to public review prior to expiry.

Legislative safeguards should be put in place to ensure the regulatory exemption does not lead to a material increase in the risk of adverse outcomes to consumers, public health and safety, or the environment.

More generally, governments should:

- continually review industry-specific regulatory approaches to assess whether they remain relevant and provide a net benefit to the community and are the most effective and efficient means by which objectives can be achieved
- ensure that regulation and regulators are flexible and adaptive in the face of evolving technologies and business models and properly funded for this task. (Rec 8.1)

---

This requires governments to put their trust in their regulators. As such, ensuring that regulators face the right sets of incentives and are adequately resourced will be critical. Rankin (sub. 26) questioned how much Australian regulators have done to ‘create the institutional structures and regulations that will enhance long-term productivity and innovation’. (p. 4). Another question is how much control (and resources) regulators have to be able to play this facilitative role. The slow regulatory response to the development of FinTech in Australia provides an illustrative case study.

#### CONCLUSION 13.6

Regulators, by construction, are risk averse. If governments want regulators to take a more permissive approach they will need to provide clear guidance on what kinds of activities in the areas they regulate could proceed without requiring prior permission. The regulators could then make this information available in an easy to use format so that firms are able to check if they need to seek permission for an activity.

#### FinTech — a case study of how regulation must be adaptive

FinTech — the application of digital services in finance — has been heralded as offering lower cost financial services, and to a broader range of clients than are served by the current financial system. FinTech is not limited to start-ups — the major players are also investing in digital products — but it does offer an opportunity to level the playing field in an area where the big players have long had a competitive advantage.

World-wide, FinTech is estimated to have attracted USD20 billion in investment in 2015, a 700 per cent growth over the previous 3 years. In Australia, FinTech was responsible for an estimated \$247 million of capital raising in 2016, and has been estimated to grow to \$4.2 billion by 2020 (Australian FinTech 2016).

The Australian Government has also argued that Australian firms are well placed to provide FinTech services into Asia, and that China Australia Free Trade Agreement includes elements aimed at improving access for Australian financial services, including ‘provisions on transparency, regulatory decision-making and streamlining of financial services licence applications’ (Australian Government 2017a). The Australian Government formed the Fintech Advisory Group in Feb 2016, but many in the industry have been arguing that, while the intent might be there, progress is far too slow.

FinTech proponents argue that they are limited by lack of access to bank data and face barriers doing business because a banking licence is required to conduct certain types of transactions. A survey in 2016 found that 40 per cent of FinTech companies surveyed had at least one financial services licence, which took an average of 6 months to acquire and cost \$61 000 in legal fees (EY 2016).



---

Another example of where progress has been slow is on legislation to support crowdfunding, as the first legislation precluded all but publicly listed companies. The proposed amendments to allow private equity access to this source of capital is considered by many to impose reporting requirements and revenue limits that are too restrictive. At time of writing, the amendments had not been passed (Sadler 2017a).

The finance sector is heavily regulated because the individual risks of a bank or non-bank financial company can become risks to the system. This arises as the financial system is highly leveraged, so a loss of trust in one financial provider that spreads to other providers can put the system at risk as lenders seek to recall their funds to convert them into less risky assets, such as cash or foreign financial products.

The Australian Prudential Regulatory Authority (APRA) and the Reserve Bank of Australia (RBA) are the main regulators in the financial system, although ASIC also plays a role in regard to governance, competition and consumer protection. A major task of the regulators is to maintain system stability. Yet, to build a healthy FinTech sector, regulators need to allow new types of services and products, some of which will fail. Hence, regulators have to balance risks to system stability with the productivity gains that come from greater competition in financial services. The formation of the Digital Finance Advisory Committee in 2015 by ASIC, members of which are drawn from across the FinTech community, is one means of providing input into getting this balance right.

The first task of the regulator is to ensure that FinTech customers are fairly protected — facing enough risk to make the customer suitably sceptical of product claims, but not enough to prevent them making transactions that are in their interests. One approach is to provide a pathway to transfer customers to other providers when a provider fails. This is important for products such as peer-to-peer lending, where the platform could fail while both the debtors and the creditors are willing to continue the relationship. The US regulatory authority, the Office of the Comptroller of the Currency (OCC), has gone part of the way by informing firms that they ‘may also require a company to have a clear exit strategy’ (Klein and Knight 2017).

The second task of the regulator is to provide the most level playing field possible. The Australian Government moved in this direction with announcements in the 2017-18 Budget. Actions include relaxing the 15 per cent ownership cap for innovative new entrants, and lifting the prohibition on use of the word ‘bank’ by authorised deposit taking institutions (ADIs) with less than \$50 million in capital (APRA are reviewing prudential licensing arrangements). Two areas where progress had stalled were also addressed — namely the removal of the double taxation on digital currency (which was treated like a separate product for GST) and extending the crowded sourced funding legislation to include proprietary companies (the recent legislation only covered public companies).

Ownership or control of data can pose a considerable barrier in an industry where people’s historical transactions are an important part of assessing their credit risk. Given the need to provide a new account number for all connected digital transactions, lack of portability of account numbers raises the costs for consumers to shift providers. Australian banks have

---

been cautious on the sharing of data, for security as well as commercial reasons. The NAB is the first to launch a developer portal for APIs in late 2016. Westpac and ANZ have called on the Australian government to create data sharing standards via a licencing regime (Eyers 2016).

These developments fall well short of the openness required of the banking system in some other countries. The UK Competition and Markets Authority open banking reforms require banks to allow customers to be able to write to, as well as to read their data by 2018. As a result, individuals, small firms and not-for-profit organisations have been able to switch accounts for free since 2013, using a ‘current account switch’ facility operated by Bacs, a company responsible for Direct Debit and Bacs Direct Credit in the UK (Payments UK 2017). The formation of this company was the industry response to the government demand that they make it happen within two years of the Independent Commission on Banking report (HM Treasury 2013).

The likelihood of progress in this area has improved. The 2017-18 Budget announced a move to open banking by 2018. This follows recommendations from the Commission’s inquiry into Data Availability and Use (the ‘Data Inquiry’) that consumers be able to obtain their data on request, which, as part of a comprehensive right, they could transfer to designated third parties (PC 2017b, rec. 4.1). Applied to bank data, this results in the ability to share account data with other providers. To enhance the value of this capability, the Commission suggested that banks build APIs to facilitate data sharing with customers. In relation to credit providers, the Commission recommended that the government legislate mandatory participation in comprehensive credit reporting in 2018, if voluntary participation failed to achieve 40 per cent coverage (rec 5.5). The Budget announcement was that banks will be required to provide customer transaction histories on request, and Treasury has been funded (\$1.2 million) to undertake an independent review to design the system.

The third task of the regulator is to develop sound legal foundations for FinTech activity. For example, only Government can introduce a biometric identity standard, which is valuable in reducing identify theft, and can substantially reduce the costs to consumers of switching service providers (currently 100 points of ID are required). Building on the standard business reporting, unified open aggregated financial data standards are also something that government is well placed to introduce. While the industry may eventually be able to develop such standards, the industry regulators can be more proactive.

The Australian Government is also moving in this area with the announcement in the 2017-18 Budget of funding to the DTA, which would allow it to develop further the GovPass digital identity system. This will be launched as a beta in 2018, and will be opt-in, but could provide a considerable boost for FinTech products where accurate identity is critical to managing cyber security (see below).

The RBA’s new payments platform is designed to make it easier for customers to switch providers, but there are concerns that it lacks the flexibility and consistency of the UK approach (Nicholls 2017). This platform, which is to be launched in October, will allow

---

payment to be sent in real time 24/7 using a mobile number (currently payments require a BSB and account number). It also will support sending more than 18 characters of data (so you can finally type enough to identify what payment you are making). This expanded ability to send data, including links to other documents, such as invoices, will facilitate straight-through processing for businesses.

One area where further simplification is possible, raised in the discussions at the Productivity Conference, is to move away from the regulation of interchange fees and credit transaction surcharges (first introduced in 2004), to a system that allows direct charging for customer card fees. Under this system, merchants would not face a fee. Rather, the card provider would set the fee to the consumer. As this would be disclosed to the consumer at the point of sale, they could choose which card they wish to use. Competition should see consumers look for low transaction fee cards, which would drive down the fees over time.

The regulators may need permission to be proactive in this space. ASIC introduced a regulatory sandbox that allows firms to test new financial products with a limited number of sophisticated (wholesale) consumers, in December 2016. The Australian Government has since announced an extension of the sandbox to allow retail (not just wholesale) products to be tested (Morrison 2016b). As at the end of May 2017, only one product has used the ASIC sandbox, suggesting either that it is poorly designed, or that the appetite for trialling products is less than the proponents of FinTech have claimed (Sadler 2017c).

The 2017-18 Budget also included considerable additional resources for the regulators — the APRA, ASIC, and the ACCC (box 8).

---

## Box 8      **2017-18 Budget additional resources for financial regulators**

The budget directed additional resources to a number of regulatory areas that are relevant to FinTech:

- \$4.2 million to APRA over 4 years to make Authorised deposit taking institutions more accountable (focusing on senior managers accountability) – with an offsetting increase in the APRA levy to pay for this.
- \$2.6 million and additional powers to APRA to monitor provision of credit by lenders that are not ADIs, partly offset by Financial Institutions Supervisory levies
- \$28.6 million to APRA for new regulatory activities – offset by an increase in the FIS levies
- \$13.2 million for ACCC to establish a unit to undertake regular inquiries into specific financial system competition issues (a House of Representatives Standing Committee recommendation) – offset by an increase in APRA levy
- \$4.3 million to ASIC to monitor the AFCA – offset by increase in levies of \$3.6 million under ASIC industry funding model
- \$16 million to ASIC to improve financial literacy – offset by \$12 million from statutory levies
- \$4.5 million to ASIC to implement and monitor extension of crowdsourcing – partially offset (\$3.4 million) by increase in charges from related entities
- \$7.9 million for ACCC to monitor and report on prices, costs and profits in insurance products for northern Australia.

*Source:* Australian Government (2017c).

The Murray Inquiry identified the lack of any forum to provide a system wide view on the regulatory approaches that would best meet the needs for system stability and consumer protection, and support market development through innovation. The report point to the statutory mandate on some Asian monetary authorities to ‘promote and market financial sector development, including streamlined entry points for new entrants’ (Murray 2014, p. 149).

There may be tentative steps in this direction. At a RegTech Roundtable, ASIC Commissioner John Price was reported as saying that RegTech offered an ‘Opportunity to move from a rear view mirror to a learning and predictive approach — to change the role (of regulators) from policeman to coach’ (Head 2017).

AFMA (sub. 32) asks what happened to the recommendations in the Johnson Report (Australian Financial Centre Forum 2009). The then government established a Financial Centre Taskforce to monitor the implementation of the recommendations in the report and to report every six months on progress towards developing Australia and a leading financial centre.

One of the recommendations was that an Asia Regional Funds Passport be established. This would involve a ‘commonly agreed set of licensing arrangements, investment restrictions and, where possible, offer conditions that would allow complying funds registered in one passport country to be offered in each of the other passport countries’

---

(Bowen and Sherry 2010). A memorandum of understanding was signed by the Finance Ministers from Australia, Japan, Korea, New Zealand, the Philippines and Thailand in September 2015, and the Joint Committee met for a second time in April 2017, with the aim of effective implementation by the end of 2017. The time lags involved point to the challenges in implementation, rather than agreement on the broad policy direction. Governments should ensure that regulators have the scope and incentives to respond more quickly.

The process of Treasury consideration and policy formation, followed by budget allocations and permission, can be too slow for the FinTech industry to thrive. However, this process is needed if the risks posed are high and there is uncertainty about the right policy direction. The 2017-18 Budget is a big step in the right direction, but there could be merit in the idea proposed by Rankin (sub. 26):

My recommendation is that Government considers instructing APRA, ASIC and the RBA and all government departments and statutory bodies, to adopt and fund Innovation Offices modelled on the OCC policy - to help establish institutions and regulatory structures, which encourage and facilitate productive innovation by industry. (p. 6)

#### CONCLUSION 13.7

If Australia is to be a leader in FinTech, the Australian Government and the financial system regulators will need to be more responsive. Areas where progress could be accelerated include:

- establishing digital identity protocols
- allowing portability of customer data
- sharing of credit history data
- developing strategies for transferring liabilities and assets where business models fail but the underlying relationships are sound, which includes requiring firms to have clear exit strategies
- liberating payments regulation
- providing regulators with greater guidance and scope to react more quickly to changing technologies.

### **Greater coordination by regulators is needed**

There is an urgent need for better coordination across regulators in some areas. For example, the ASIC Capability Review (Australian Government 2016) noted that the level of coordination between regulators was an external constraint on ASIC performance.

Government needs to ensure that regulators and regulations:

- are not contradictory or overlapping and that areas of responsibility are clearly communicated (see below)
- share data and information, including with the businesses they regulate (see below)

- 
- are coordinated by an overarching strategy that has at its heart creating a regulatory environment that is permissive, low cost and easy to navigate.

These strategies will often need to cut across jurisdictions, as digital technologies are rarely applicable to only one jurisdiction.

A national coordination role can be vital where states have the responsibility for regulation. For example, in Australia, national strategies have been developed in health (immunisation, tobacco use reduction, asthma), transport (road safety, port infrastructure, maritime safety), security (identity security), and international education.

Yet, there are other areas where there is a call for better coordination. The Australian College of Road Safety (sub. 34), in making their case for the funding of the Australian National Road Safety Strategy, argue that an overarching coordinating mechanism is needed, despite a range of government collaborative mechanisms (they list, for example, Austroads, National Transport Council, Heavy Vehicle Regulator, National Road Safety Partnership, BITRE (p. 8)). ACCI (sub. 37) make the case for a National Freight and Supply Chain strategy, to ‘increase supply chain efficiency, connect our cities and regional centres and support fast-growing regional hubs to be as productive as possible’ (p. 9). This was recommended in Infrastructure Australia’s 15 year plan, as integrated planning and investment is needed to accommodate the expected 86 per cent growth in land freight, and 165 per cent growth in containerised trade between 2011 and 2031 (IA 2016). Such national approaches need to be developed in conjunction with industry and to be as least restrictive as possible.

Governments can also provide core services where comprehensive data are needed. The private sector is unable to operate where some element of compulsion is required to get the coverage needed. For example, Raymont (brief sub. 2) suggested that the government establish a single place to update addresses and phone numbers, which can then write to all the organisations you select to update their records. This could also be used for changing names, which as Body (brief sub. 2) reported, involves considerable effort. A number of other comments made in regard to this review also asked why MyGov does not facilitate updating addresses for people across all their government interactions. (This does seem to be addressed by the initiative funded in the 2017 Budget).

Digital technologies can make cooperation and coordination easier. For example, Cullen (brief sub. 7) asks why we do not have a national driver’s licence. Scott (brief sub. 10) would extend this to vehicle registration, and Corr (brief sub. 13) to boats and firearm licences. Ligett (brief sub. 18) reports on the unnecessary cost of having to register with the Teachers Registration Board when moving state. Teachers are part of the COAG mutual recognition agreement, which recognises that the standards in one jurisdiction are sufficient for licensing in another. So in this case, it is not the standards that are the problem, but the ability to send data — which is why digital technologies should make the mechanics of mutual recognition much easier. Several respondents also asked why road rules could not also be amalgamated, with the more liberal rules being adopted (such as the

---

ability to turn left on red unless otherwise signposted, and a zip requirement for merging traffic, using blinking orange lights at night when traffic is very light).

Digital technologies are creating new areas where national coordination is needed. For example, it has been reported that, in the United States, 23 states have introduced 53 pieces of legislation to regulate self-driving cars ‘all of which include different approaches and concepts’. Further, for the legislation that has been passed, ‘none of those laws featured common definition, licensing structure or sets of expectations for what manufacturers should be doing’ (Urmston, cited in West 2016).<sup>5</sup> Common definitions and standards are needed to ensure system interoperability, while coordination on infrastructure can substantially lower costs.

Although the market will sort things out eventually (for example, VHS rather than BETA became the video standard), the transition can take considerable time and many firms can be left with products that are no longer viable, even if they are a better technology (as some argue BETA was). This matters, not because firms fail, but because more rapid adoption has considerable economic value. For example, it has been estimated that a 10 per cent increase in Internet Protocol addresses per capita corresponds to an 0.8 per cent increase in GDP per capita (Ackermann, Angus and Raschky 2017).

### The Internet of Things — a case study on the need for coordination

The IoT is a challenging area for government, as many aspects of the market potential are unlikely to develop efficiently without cooperation between firms, as well as between firms and government. The core of the IoT is connected sensors that are used to collect data, which are then shared with the network of other devices. It is more than the fridge ordering milk when supplies are low, as the value comes in the ability to use big data to optimise specified outcomes. This could be smoothing power usage across electricity grids, minimising delays along transport routes, or alerting airlines to when their planes need attention on landing (which they do using an information tool called Airplane Health Management; Maggiore 2007).

The IoT market in Australia has been estimated by the International Data Corporation (IDC) to be worth \$18 billion by 2020, connecting 2.7 million commercial vehicles, 1.8 million health care appliances, and interestingly 1.7 million pets (Lim 2017). In a survey, 81 per cent of organisations rank common data and connectivity standards as extremely or very important, as were open software standards for 63 per cent of respondents. It appears that Australia is lagging similar countries (such as New Zealand) in setting out the rules to support the development of the IoT.

---

<sup>5</sup> The US National Highway Traffic Safety Administration has drafted guidelines for uniform regulations, which will help to overcome this problem. But some of the requirements, such as requiring a driver in the front seat, may hinder the introduction of the technology (West 2016).

---

The complexity of the regulatory environment facing firms that want to invest in the IoT is considerable, as is the complexity for regulators.

- There are uncertainties about what regulators are responsible for activities that increasingly cross traditional industry boundaries. Digital technologies are undermining the traditional definitions of industries, not least the distinction between manufacturing and services (PC 2016a). For example, trucking companies buy tyre miles for their trucks rather than tyres, and logistics firms offer customers real time tracking of their packages along with delivery. The IoT data are used to offer a service, raising questions about whether to regulate the service (tyre monitoring) or the thing (tyres) or both, or neither. These new ways of doing business cut across industry and regulator lines of responsibility.
- As many of the services where the IoT can improve outcomes lie in highly regulated industries such as electricity, water utilities, and smart cities, they are entering markets that already have a complex regulatory environment. In some cases, there are major infrastructure investments and legacy systems that IoT solutions will undermine. Providers can struggle to maintain a full range of services if the more profitable elements are captured by new providers. Equity can be an issue, as better off consumers can link into solutions that minimise their costs, while other consumers cannot afford access.
- Opportunities also lie in areas where government is a major service provider (such as education and health) where sharing data, in particular at a unit record level, can provide for joined up services and better service selection. However, access to such data faces legislative and cultural barriers. Some solutions to this problem are set out in chapter 2, and recommendations made in the Data inquiry (PC 2017b). Moreover, as these services are funded, at least in part, by government, the funding arrangements will affect the incentives for individual firms to offer connected products.
- While there is considerable scope to use the IoT data to better design effective services and products, the data need to be shared to maximise their value, so underinvestment by individual providers is likely. For example, a smart grid is needed to integrate renewable sources of generation, and to manage demand (for example by switching air conditioners to fan only in periods of peak electricity demand). No single generator, or retailer, will make the investment needed, as the benefits accrue across all in the system (SP 11). Scale is also an issue. Networked data provide the greatest value where they include all sources of information rather than a subset of customers or users.
- Related to the need to ensure data are shared is the potential for the IoT to increase the share of the market that is served by vertical relationships (industry verticals). These occur where consumer demand for two products is closely related. Strong compliments, such as the iPhone and the mobile phone service, if dominated by one firm can potentially reduce rather than increase competition. The need for regulators to scrutinise whether such relationships are restricting competition has been recognised in the United States, and should be on the radar of the ACCC and ASIC in Australia (Sallet 2017).



---

Australia is not alone in facing these regulatory challenges, and can learn from developments in other countries. For example, in 2016, the Developing Innovation and Growing the Internet of Things (DIGIT) Act was introduced in the US House and Senate, which funds a broad working group to ‘report on policies and practices that hinder IoT development, propose policies to improve federal agency coordination on IoT issues, and identify opportunities for federal agencies to make better use of the Internet of Things’ (New and Castro 2016, p. 10). Also in the United States, the Smart Cities and Connected Communities framework, released in 2014, provides a guide to coordinate federal agency investment and collaboration for smart city technology (The Network and Information Technology Research and Development Program 2014).

Some areas that have been identified to support the IoT (New and Castro 2015) are:

- radio frequency allocations so that mobile devices (whether as part of vehicles, phones, or other devices) can communicate. For example, tollway payment is much easier if one device can communicate with all toll sensors, an outcome in which Australia has been a leader, with toll payments systems linked in New South Wales and Queensland (ITS Aus 2012).
- spectrum allocation, especially where Wi-Fi is not adequate to support the volume and/or speed of data transmission required. For example, farmers can establish their own local WiFi to support precision farming, but may compete for the spectrum to do so. Even where there is no competition for spectrum, interconnectedness between the personal area, local area, metropolitan area, and country wide networks can be required to support the IoT activity (Stratix 2015)
- open access code and standards that support large scale deployment of sensor networks across different infrastructure types and locations (Linux was developed as open source and is used to run android phones)
- cybersecurity standards and resources.

Failure to resolve these types of issues quickly slows the development of the IoT. A report for the Netherlands government identified a need for international harmonisation in standards, such as spectrum frequencies, to facilitate interoperability of the technologies (Stratix 2015). This is needed for achieving economies of scale, and would promote trade in technologies. It reports that the United Kingdom has made the 870-876 MHz the 915-921 MHz spectrum available for license-free use, with the latter potentially dedicated to IoT. Other issues to consider are potential spectrum bottlenecks, due to too many applications requiring data transfer at any point in time. For example, in cities there could easily be 2600 connected devices per square kilometre, all competing for the same spectrum (Stratix 2015).

In Australia, 25 organisations (including government agencies) formed the Internet of Things Alliance Australia in July 2016 (Coyne 2016). It aims to focus on spectrum availability and management, network resilience, industry verticals, data sharing and privacy, and fostering IoT start-ups. As it stands, this looks more like a list of the members’ current areas of concern than a concerted effort to identify and address where

---

coordination is needed. It will be important that this does not become a forum to lock in proprietary technologies and that a true cooperative approach seeking open source solutions is developed.

Coordination across the levels of government on regulatory approaches can assist firms to take full advantage of the fast moving world of digital technology. The Australian government could support the development of the IoT by developing a national strategy, in consultation with the state and territory governments.

#### CONCLUSION 13.8

Coordination across the levels of government on regulatory approaches can assist firms to take full advantage of the fast moving world of digital technology. The Australian government could support the adoption of the internet of things (IoT) by developing a national strategy for the IoT in consultation with the state and territory governments.

### **Forging common standards can reduce costs**

Common standards across jurisdictions can reduce costs for users and assist firms to sell into other markets. The failure to standardise electrical plugs, voltage, emergency beacons, and (most famously in Australia) the rail gauge across states, illustrate the barriers that different standards can erect. Occupational licencing, which expanded rapidly in the United States over the past decade, has been credited as playing a role in reducing competition (Kleiner 2015).

In Australia, despite many attempts by COAG, and reviews by the Commission of mutual recognition arrangements between Australian jurisdictions and New Zealand, there remain areas where agreement to recognise the standards of other jurisdictions cannot be reached (PC 2015b). There is still a balance to be sought, as the costs of seeking mutual recognition (or the more challenging agreement on harmonisation of standards) can outweigh the benefits. For example, HIA (sub. 28) raise the cost of red tape in the building industry, but also point out that regulatory harmonisation across jurisdictions might cost more than it delivers in benefits.

#### Open standards encourage innovation

Open standards should be encouraged for regulators, and Australia should look to other countries that have already solved the problem. For example, HyperCat is an open standard for the IoT developed cooperatively by an industry working group in 2014 with USD12.2 million funding from the UK government's Technology Strategy Board. In 2015 HyperCatCity was developed by the same group to encourage the adoption of the HyperCat standard by firms working on smart city initiatives. Adoption of open standards

---

used in other countries not only speed transformation at home, it means that Australian firms have a base from which to compete in other countries.

... Nation-specific standards limit the ability of international companies to enter domestic markets and actually reduce domestic firm's ability to compete internationally. (New and Castro 2015, p. 6)

The suggestion that Australian governments and their regulators be open to adopting international standards is not new. The Harper Review commended 'COAG's recent decision to examine whether international standards can be more commonly accepted in Australia and the Australian Government's recent reforms announced in its Industry Innovation and Competitiveness Agenda' (Harper et al. 2015 Part 3 p. 45). The Review urged governments to review product standards that are directly or indirectly mandated by law as a priority (recommendation 10). The Commission's report on Regulation of Agriculture (PC 2016d) argued that there were significant gains in time to market and cost savings by accepting US and European standards and approvals in agricultural and veterinary chemicals.

#### Where standards are proprietary, having a seat at the table benefits firms

In some areas, having a 'seat at the table' when international standards are set (such as those that allow for interoperability) is important for firms to ensure good market access for their products. Patents that need to be used to comply with a technical standard are designated as Standard Essential Patents (SEPs). SEPs are meant to be licensed on a 'Fair, Reasonable and Non-discriminatory' basis. What this means in practice and how it is determined by the courts varies across jurisdictions, so being able to influence these SEPs can provide a competitive advantage. For example, Apple and Google have both bought companies to get patents that gives them a seat at the 5G standards setting table.

Governments could assist firms to be aware of such international standard setting, and where national interest is at stake, could be more proactive in representing Australia's interests.

#### Standard approaches to digital identity can save costs

Digital identity is another area where common standards could greatly reduce costs for individuals, business and government. While Australians are historically suspicious of a single personal identifier, such as a social security number, digital identity is about lowering the cost and improving the accuracy of identifying an individual in electronic transactions. Currently, passwords are the main way in which identity is established in a digital transaction. Banks and government agencies require a 100 point check when opening an account, or applying for a passport. AustraliaPost is reported as having estimated the costs of processing identity as up to \$11 billion across the Australian economy (Bajkowski 2017a).

---

The DTA and AustraliaPost have recently established a partnership to ensure that their systems are interoperable. The DTA is developing GovPass that will allow people to do all the transactions that they have previously done at the government shopfront electronically. Digital identity would also greatly facilitate consumer mobility across different suppliers, and can help address the concerns raised by the banks in regard to data sharing.

#### CONCLUSION 13.9

Adopting international standards can save both regulators and firms considerable time and money. The decision on whether a standard is suitable could be facilitated by the Australian Government developing a positive list of foreign testing agencies where they will recognise the product approvals by these agencies as meeting Australian standards.

Governments should work together to establish an agreed digital identify standard.

## Improving access to data

Data are increasingly seen as resources that can be mined to produce valuable new products. Governments are the collectors and curators of much data, and could stimulate new opportunities by making this data available in forms that still protect the security of the data and the privacy of the data sources. Governments can also make better use of data to improve their delivery of services and functioning of government. This theme is taken up in chapter 2, where data form the core of delivering integrated health services. In addition, as control over data also brings market power, governments can play a role in facilitating access to data by competing firms, where lack of access would otherwise trap customers into poorer quality services than available elsewhere. Greater access to this data also provides raw material for firms to mine to produce new information services that can be applied in diverse areas (from managing electricity consumption to planning the ideal holiday).

The benefits of improving access to data are potentially very large

Public service agencies collect a considerable amount of information, on locations (geospatial), people, and businesses. Although there are costs to providing free data (in ensuring quality and privacy are maintained and any forgone fees), the direct savings to those accessing the information, and to those that do not have to provide the same information again, are considerable. For example, the G-NAF, a geocoded address database of all physical addresses in Australia was developed by a not-for-profit consortium (PSMA Australia) of the Australian and state and territory governments in 1993. It had been available on a fee for service basis to government departments and industry, but large parts of G-NAF have recently been made available on the [opendata.gov](http://opendata.gov) website. By making this information openly available other firms can develop value-adding tools.

---

The benefits of greater data sharing across governments and service providers can save service providers' and clients' time and, more importantly, allow for a much better service to be delivered. For example, health services can be coordinated through the electronic health record (chapter 2). There are many other areas of public services where coordination would reduce the need for people to provide repeat information, and allow services to be better targeted and tailored to individual need.

There is also scope for much greater application of public sector data in other areas, which can be used to inform choice (improving consumer discipline) and to develop new services. For example, OzCoast uses geospatial data from Geoscience Australia to provide a wide range of mapping services.<sup>6</sup>

The benefits generated by ABS, from 2008, in making its publications and statistics freely available online (under Creative Commons licensing) provide an indication of the potential return from improving access to data. For an annual cost to the ABS of about \$3.5 million, the costs saved by the direct users of the data were estimated to be \$5 million (the net gain due largely to less time taken to access data, as the savings on fees were a transfer from the ABS to the users). However, it is the substantial increase in the use of the data and the value of its applications that delivered the biggest benefits — conservatively estimated as \$25 million (Houghton 2011). These estimates imply a return of about five times the investment cost (by the ABS and users). Top down approaches to estimating the value of public service data range from a boost in GDP by anything from 0.05 per cent to 1.4 per cent (from studies reported in Houghton 2011). The lower estimate still puts the potential annual value of public sector data provision at about \$85 billion.

There is also considerable value in freeing up the use of commercial data. Indeed aggregators, such as Quantum, already compile datasets from social media, loyalty cards and other sources to provide information services to firms on their customers, and the nature of different markets. Much of this is used to target advertising, but it also guides firms in developing products that will better suit what consumers want. This all happens without government intervention (although to the extent that people are unaware of how their data are traded and applied, some oversight might be warranted).

Where policy intervention is needed is where data are a source of market power for the firm that collects the data. Firms can be reluctant to give up this source of advantage. Lack of access to their own records can reduce the ability of consumer to switch suppliers, while lack of access to information about the market can reduce the ability of suppliers to offer new products that will compete in existing markets. This is not a zero sum game — the benefits to consumers of getting a preferred product are large. For example, the Australian Communication and Media Authority estimated that the industry behaviour changes

---

<sup>6</sup> A new initiative in the 2017-18 Budget is funding for Digital Earth Australia for an open access online platform for satellite imagery. This is the sort of initiative that it is difficult for a firm to value capture, given the ease of sharing.

---

following the revised Telecommunications Consumer Protection Code (along with number portability codes), delivered benefits of at least \$545 million a year (ACMA 2015). The gains to consumers of greater portability of their own data in areas such as banking, insurance, electricity, water, and other utilities are likely to be of at least this magnitude.

The Commission has provided a roadmap for reform

The Commission's Data Inquiry (PC 2017b) canvassed all these issues, making a number of recommendations that, if followed, will unleash considerable scope for improvements in service delivery. The Inquiry concluded that governments could stimulate innovation and new opportunities by:

- making the substantial data that they collect and curate more readily available in forms that still protect the security of data and the privacy of data sources
- empowering consumers to use and benefit from their own data.

Data that allow performance monitoring and comparison of government activities is a fundamental starting point. Governments themselves can make better use of data to improve delivery of services and enhance their own functioning and efficiency (SP 3).

Access to data more broadly would enable capable and trusted researchers to play a more active role in developing solutions to seemingly intractable problems. This can be achieved through early and routine release by governments of non-sensitive datasets, and the adoption of robust processes for assessing and managing risks associated with other datasets to better allow sharing. This theme is also taken up in chapter 2, as data are at the core of delivering higher quality, integrated health services.

In addition to these benefits from improved access, the Commission's Data Inquiry highlighted its role as a potential barrier to competition, but also an important enabler of consumer control and choice.

The central plank of the Commission's report and recommendations was an overarching data access law (a Data Sharing and Release Act) that would give consumers — individuals and small businesses — a comprehensive right to access their data and direct that they be provided to third parties. This would enhance competition by enabling consumers to have their data (such as that accumulated over years by their bank or telecommunications company) transferred to potential alternative suppliers.

The ability to drive competition in this way will likely significantly increase in value as data collection continues to grow. The benefits of the comprehensive right could extend beyond competition between existing providers by enabling further innovation in products and services. The Commission's report recommended allowing each sector to develop its own rules about what data the comprehensive right will apply to, and how they will release that data.

---

If these reforms can release even 5 per cent of the potential value of public sector data, they are worth over \$4 billion to the Australian economy. Moreover, reforms that allow consumers greater control over sharing their data could be worth over \$1.5 billion a year through greater, and better-informed, choice in banking, insurance and utilities.

#### CONCLUSION 13.10

The recommendations made in the Commission's inquiry into Data Availability and Use will make a substantial change in how consumers can access and direct their data, which should strengthen competition across a range of services, not least financial services.

Greater availability of the data that governments' collect will provide a new resource to which firms can add value. This should help to drive productivity improvements across a wide range of industries in the future.

The Australian Government is currently considering its response to the report.

## Improving the treatment of intellectual property

As a net importer of intellectual property (IP), Australia would benefit from a less restrictive IP rights regime. The impact on incentives to invest in research and development (R&D) that form the foundation of the IP law are also likely overplayed by firms with existing commercial interests. And many smaller firms face major barriers in using the system to protect their IP once obtained, as deep pockets are often necessary. While international agreements severely restrict the scope for the Australian government to overhaul the IP protection system in Australia, there is still scope to improve the current arrangements. The Commission, in a major review of the IP system completed in 2016, found that the Australia's patent system 'grants exclusivity too readily, allowing a proliferation of low quality patents, frustrating follow-on innovators and stymieing competition' (PC 2016b, p. 2).

The recommendations that expected to deliver the greatest benefit related to:

- less prescriptive provisions on the fair use of copyrighted material (replace fair dealing with fair use)
- clarifying the law on geoblocking, which the Commission regards as a restraint on trade rather than protection of IP
- a higher inventive threshold test for patents and restructure of patent fees
- enhancing the role of federal circuit court to improve access to enforcement mechanisms, especially for small and medium sized firms
- expand safe harbour schemes, allowing use of IP that will not be considered to violate the IP rules, such as one off use of a design under copyright
- reforming extensions of term for pharmaceutical patents.

---

It is hard to estimate the impacts on productivity of the Commission's IP Inquiry's recommendations, but even shifting the dial by 0.1 percentage point in multifactor productivity is worth almost \$1.9 billion to the Australian economy (after taking account of general equilibrium flow on effects).

While copyright encourages investment in creative works by allowing creators and rights holders to exploit their value, the IP review noted it is poorly targeted and broader in scope than needed. It provides the same levels of protection to: commercial and non-commercial works; to those no longer being supplied to market; and to those where ownership can no longer be identified.

A system of exceptions to copyright enables limited use of copyright material without the authorisation of rights holders. However, the IP review found Australia's current exceptions for fair dealing are too narrow, inflexible and prescriptive. They do not reflect the way people consume and use content in today's digital world, nor do they accommodate new legitimate uses of copyright material. For example, the existing law only introduced limited permission to make a personal-use copy of a videotape in 2006, which was 26 years after VCRs were introduced, and 8 years after the arrival of DVDs, which superseded VCRs. As a result of the existing prescriptive exceptions, a representative consumer is estimated to infringe the copyright of non-commercial and commercial works over 80 times a day (PC 2016b).

Problems caused by the current prescriptive system include: frustrating the efforts of online businesses seeking to provide cloud computing solutions; preventing medical and scientific researchers from taking full advantage of text and data mining; and limiting universities from offering flexible Massive Open Online Courses.

Moving from the current legislated mechanisms that only enable use of copyright material in tightly defined situations ('fair dealing' exceptions) to a principles-based system, as operating in the United States and other countries, that considers whether use of copyright material would harm the right holder's interests ('fair use'), would allow Australia's copyright arrangements to adapt to new circumstances, technologies and uses over time. A 'fair use' system would also unlock many opportunities and avoid unnecessary payments. For example, moving to 'fair use' would avoid the current situation where education and government users pay \$18 million dollars per year for materials that would be accessible under fair use provisions (chapter 3).

The consultation draft of the Copyright Amendment (Disability Access and Other Measures) Bill that was released in December 2015 proposed expanding the safe harbour protection from copyright infringement to include search engines, universities and libraries (Department of Communications and the Arts 2015). However, the provisions relating to



---

safe harbour were subsequently removed from the bill,<sup>7</sup> with the Government noting it would further consider feedback received on the proposal (Fifield 2017). The removal raised concerns from a number of tech firms, particularly those that offer two-way platforms that allow users to upload their own content, which is then purchased by other users, such as Redbubble and Envato (Sadler 2017b). The inclusion of fair use provisions in Australian copyright law (as recommended by the Commission in its IP Inquiry) could address this problem by allowing use of copyright material in a way that does not affect the revenue stream from the intellectual property rights of the creators.

An issue that was raised by both the Commission's IP Inquiry and the Harper Review is that conditions in registered designs, copyright, eligible circuit layout rights, and licences and assignments of patents are currently exempted from most of the competition law prohibitions by subsection 51(3) of the *Competition and Consumer Act 2010* (CCA). Both the IP Inquiry and the Harper Review recommended repealing the section, noting that commercial transactions involving IP rights should be subject to competition law in the same manner as transactions involving other property and assets (Harper et al. 2015; IP Australia 2016).

#### CONCLUSION 13.11

While restricted in how much it can tailor the IP system to better suit Australia's needs, the Australian Government could reduce costs and improve incentives for inventiveness by adopting the recommendations made by the Productivity Commission in its 2016 inquiry into Intellectual Property Arrangements.

## Cost sharing arrangements can be poorly designed

It can be difficult to get the balance right in cost sharing arrangements that cover regulatory costs and community service obligations (CSO). Passing all costs onto the regulated entities can allow the regulator to indulge in inefficiencies, while failure to pass on the regulatory costs to regulated businesses effectively means the public pays for regulation that ultimately benefits regulated entities.

Ideally, the public pays to enforce regulation that delivers public goods, while the businesses pay for regulation that enhances their industry's functioning and reputation. While a CSO that benefits a particular community with a low capacity to pay is best funded by taxpayers, it is not clear that the costs of a CSO that benefits high-income communities should not be passed onto these communities. These situations arise where the challenge is achieving collective action, rather than seeking to alleviate economic

---

<sup>7</sup> The Bill, which was introduced on 22 March 2017, passed both houses of parliament unamended and received Royal Assent on 22 June 2017.

---

disadvantage. Where a CSO applies to a broader community who benefits from the regulated services, then passing the costs onto consumers via a levy on the regulated entities can be more efficient and fair. If industry, rather than taxpayers bear the cost of the CSO, they have an incentive to ensure that it is delivered as efficiently as possible.

Testing the incentives created by the proposed cost sharing arrangements — to gold plate (or skimp) on compliance activities or the delivery of the CSO — should be an essential element in developing cost-sharing arrangements. This should occur alongside consideration of administration costs and the simple practicality of enforcing payment. The Commission’s inquiry into Marine Fisheries recommended that seafood processors across all jurisdictions pay licence and accreditation fees that reflect the efficiently incurred costs of regulating their facilities (PC 2016c). The recent Commission’s inquiry into Telecommunication Universal Service Obligations (PC 2017c), recommended that consumer subsidies to meet affordability and accessibility are best funded through general revenue. However, given the wide user base, availability gaps in areas other than remote areas experiencing disadvantage should be funded by industry levies. Broader application of these principles could improve the operation of some markets where CSOs are imposed.

## **Facilitating improvements in cyber security**

One of the challenges for governments in managing the new data-centred economy is cyber security. Australia was ranked equal 3<sup>rd</sup> (with Oman and Malaysia) behind Canada and the United States in the 2014 Global Cyber Security index and dropped to 7<sup>th</sup> in the 2017, overtaken by Singapore, Malaysia, Oman, Estonia and Mauritius (ITU 2017).

The global cyber security index is built on five pillars: legal, technical, organisational, capacity building and cooperation. In the 2017 rankings Australia ranked well on legal and technical elements, but is conspicuously behind the other nations in the top 10 on a range of other measures (including bilateral and multilateral agreements, international participation, public-private partnerships, and interagency partnerships) (ITU 2017).

Australia does not rank well in the areas where coordination is required — locally, globally, and across the public and private sectors. Yet coordination is necessary in order to take a system-wide approach, and prevent knee-jerk responses to security violations. Clarity is also needed about how to provide protection against cyber-attack (including what regulations can help to manage risks) in order to provide a secure platform for innovative activity. For example, security concerns could quickly undermine the development of the IoT in Australia.

Half of all IoT things coming into the home are going to be produced by companies that are less than 3 years old. They are going to have access to your Wi-Fi, data and devices. Now, do you think those companies are seriously considering security? The answer is most probably, no. (Cisco’s Kevin Bloch cited in KPMG 2016, p. 8)

Much of the benefit of improving access to data also hinges on being able to manage the cyber security risks. This will be critical in sharing data, to ensure that data integrity is

---

maintained, and to prevent its release to any parties other than those intended by the person exercising their comprehensive right. The banks have raised concerns about cybersecurity in their resistance to sharing data. For example, open APIs help people to change bank services, keeping their account numbers and/or making the change to digital-only payments seamless. Their widespread rollout would help address the problem raised by McCullough (brief sub. 37) when moving home loans between banks, but is resisted by some banks on the grounds of cyber security. Such number portability is highly desirable, but can also offer opportunities for scammers.<sup>8</sup> The Commission's Data Inquiry recommended that sector-accredited release authorities be tasked with ensuring that governance standards (include cyber security) are up to the task.

The global cyber-attack in May 2017, which affected more than 200 000 computers across 150 countries, including hospitals in the United Kingdom, illustrates the importance of vigilance. In early 2017 the Australian Cyber Security Growth Network was set up with \$31.9 million in funding over four years to 'bring together businesses and researchers to develop the next generation of products and services that are needed to live and work securely in our increasingly connected world' (DIIS 2017). A recent review of the first year of the strategy concluded that progress had been 'undermined by the ad hoc nature of government's communications and insufficient expectation management with industry partners' (Hawkins and Nevill 2017, p. 3). This review made a number of recommendations including better communication with the private sector, a more 'flexible and adaptive' approach with easurable and time bound annual plans, and better baseline research.

Following the finding of a lack of cybersecurity preparedness in two of three major data handling departments (ANAO 2017), and recommendations following the 2017 Census events, the 2017-18 Budget included \$10.6 million for the DTA to build a cyber security governance capability, overseeing management of cyber security in the public service. The Digital Investment Management Office in the DTA has responsibility to ensure that all large Australian government technology projects will provide value for money by providing a much greater focus on costs and risks. These projects include developing the systems for GovPass and a 'tell us once' capability to share data across Commonwealth agencies.

One of the reactions to concern about cyber security has been to require that data be stored locally. This is the case in Australia, with the electronic health record data. Other countries have introduced more restrictive laws, not just for security reasons, but because of the misplaced view that restricting the flow of data across borders will provide commercial advantage to local firms. Such 'data mercantilism' policies can be costly, as they prevent firms and individuals taking advantage of lower cost data storage and restrict the parties can offer to add value to data. For example, recent estimates put the cost of the United

---

<sup>8</sup> Mobile phone number portability has been exploited by scammers who have used it to steal identity and redirect banking verification codes (Winterford 2011).

---

States' restrictions at between 0.1 and 0.36 per cent of GDP. The cost of cloud services in Brazil and the EU have also increased by 10 to 54 per cent following the introduction of data localisation policies (Corey 2017).

Governments need to provide leadership to coordinate cybersecurity responses, but this must include testing proposed regulatory action to manage risks with the industry players and ensuring that the costs as well as benefits are considered.

#### CONCLUSION 13.12

Leadership across all areas of cyber security is needed. It will be important that 'knee jerk' reactions, such as restricting the cross border flow of data, are not imposed as the costs may well exceed the benefits. Harnessing local and international expertise to be prepared to respond as challenges arise would be a sensible investment.

## Market development — do regulators have a role to play?

There is a live and valid debate about the role that regulators can or should play in market development. Clearly, poor regulation and regulator behaviour hampers market development, but whether regulators should be proactive in promoting market development is a different question. This supporting paper has argued that there can be circumstances when regulators can be tasked with some aspects of market development. These include:

- keeping up with technological changes and designing regulations and regulatory systems that take a risk-based and education-based approach. This includes adopting an outcomes-focused approach to regulation — what firms have to achieve to be compliant — rather than specifying how they must be compliant (although offering explicit 'how to comply' guides can be of considerable value to small firms, so a differentiated approach can assist in encouraging new entry)
- recasting regulations into machine readable form, and designing compliance requirements so that they can take advantage of the opportunities offered by new technologies
- providing benchmarking services to their regulated entities to help them assess their performance. And more generally, providing information back to the regulated industry or firms so that they can see how the information they provide works to deliver on the objectives of the regulation — be it levelling the playing field to improve competition or consumer, worker and investor protection
- compelling the provision of information to consumers in standardised forms
- improving complaints systems and the effectiveness of redress, to build the confidence of consumers in the relevant market and help the industry quickly identify and manage risks that could otherwise attract heavy-handed regulation

- 
- developing national plans to guide investment in infrastructure, notably to support the IoT and develop cyber security systems
  - coordinating industry to develop common standards, including the adoption of international standards and using powers to compel where industry cannot self-organise
  - adopting the recommendations of the Data Inquiry, including compelling firms to transfer client data at the client's request, as well as improving access to public sector data
  - adopting the recommendations of the IP Inquiry, not least changing copyright law from 'fair dealing' to 'fair use'.

Whether governments should go beyond setting and enforcing the rules depends on how much they could add to market development, and how much this would conflict with their regulatory responsibilities. In some cases, these responsibilities will align, but in other cases there will be tension between the roles, and regulatory capture is a real possibility. In asking whether governments should go beyond what is largely a risk management role (to provide information and manage market power, as well as setting allowable risk levels) to take on a market development mantle, they should be guided by the answers to the following questions:

- Can industry work together to resolve the problem? If they can, then government's job is to set the parameters they must achieve, not to intervene. An example is the Data Inquiry's recommendation that industry achieve at least 40 per cent credit history sharing by a specified date to avoid a mandate. This is a good example of how to focus the minds of industry to co-operate to resolve these issues.
- What is the risk of regulatory capture? Co-design of regulations with industry can help shift the regulatory attitude from a 'No, but' to a 'Yes, if' approach, as industry will be better than regulators at understanding the risks that can arise and what parameters will work to mitigate these risks. This requires an alignment of objectives, in particular through most of the industry benefitting from the risks being well-managed. This is the case where it is industry reputation, rather than firm reputation, that matters most for consumer confidence in the products. For example, a single adverse event relating to one airline can affect the demand for aviation services generally.
- Which markets are being held back by current regulation and regulator behaviour? Industries where technology is moving rapidly and introducing new risks and opportunities, such as biotechnology and Fintech, could find themselves hamstrung by regulatory regimes that were designed for a very different world. Regulators may well struggle to keep up, and their legislation may prevent them from adapting to the changing industry they regulate. Co-design has risks of capture, but the alternative is to either strangle nascent industry to the detriment of the economy, or to let activity that may well need to be regulated (to create a healthy long-term market) go ahead unchecked. Co-design of regulations and the compliance regime is needed for timely action, but good governance is critical to avoid regulatory capture. This must include transparency about the co-design process (who, what, when and how). Checks and

---

balances to ensure that the regulations maintain a level playing field must be built into the co-design process. This includes release of exposure drafts of regulation.

**CONCLUSION 13.13**

Governments should be cautious when being proactive about market development. But there can be situations, such as in establishing some standards, where governments need to act to provide coordination that is lacking.

Ensuring that consumers, workers and investors have adequate protection, that regulations impose only necessary distortions to markets, and that regulators engage with regulated entities and take a risk-based approach to compliance and enforcement, remains the best way that governments can support productivity growth.

---

# References

- Ackermann, K., Angus, S. and Raschky, P. 2017, *The Internet as Quantitative Social Science Platform: insights from a trillion observations*.
- ACMA (Australian Communications and Media Authority) 2015, *Reconnecting the customer - Estimation of benefits*, November.
- ANAO (Australian National Audit Office) 2017, *Cybersecurity Follow-up Audit*, 15 March.
- Australian Financial Centre Forum 2009, *Australia as a Financial Centre: Building on our Strengths*.
- Australian FinTech 2016, *Fintech Market Growth to Add A\$1 Billion New Value to Australian Economy by 2020*, 15 April, [www.australianfintech.com.au/fintech-market-growth-to-add-a1-billion-new-value-to-australian-economy-by-2020/](http://www.australianfintech.com.au/fintech-market-growth-to-add-a1-billion-new-value-to-australian-economy-by-2020/) (accessed 12 May 2017).
- Australian Government 2016, *Fit for the Future: A Capability Review of the Australian Securities and Investment Commission*.
- 2017a, *Australia's FinTech advantages*, [www.fintech.treasury.gov.au/australias-fintech-advantages/](http://www.fintech.treasury.gov.au/australias-fintech-advantages/) (accessed 9 May 2017).
- 2017b, *Budget 2017-18 - Budget Paper No. 1*, May.
- 2017c, *Budget 2017-18 - Budget Paper No. 2*, May.
- Australian Treasury 2017, *Backing Australian FinTech*.
- Bajkowski, J. 2017a, *Digital identity: Australia Post and Digital Transformation Office finally hook-up together*, The Mandarin, [www.themandarin.com.au/79218-australia-post-joins-dta/](http://www.themandarin.com.au/79218-australia-post-joins-dta/) (accessed 22 May 2017).
- 2017b, *Real Time Government? NSW Reveals its New Digital Government Strategy*, The Mandarin, [www.themandarin.com.au/79420-real-time-government-nsw-reveals-new-digital-strategy/](http://www.themandarin.com.au/79420-real-time-government-nsw-reveals-new-digital-strategy/) (accessed 23 June 2017).
- Bowen, C. and Sherry, N. 2010, *Government Responds to Australia as a Financial Services Centre Report*, Media Release, 14 September.
- Brynjolfsson, E., McAfee, A. and Spence, M. 2014, 'New World Order: Labor, Capital, and Ideas in the Power Law Economy', *Foreign Affairs*, vol. 93, no. 4.
- Corey, N. 2017, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, 1 May.
- Cowan, P. 2014, *Victoria Jumps on Board with myGov*, iTnews, [www.itnews.com.au/news/victoria-jumps-on-board-with-mygov-385974](http://www.itnews.com.au/news/victoria-jumps-on-board-with-mygov-385974) (accessed 12 May 2017).

- 
- 2017, *Australia will No Longer Get a Single Government Website*, iTnews, [www.itnews.com.au/news/australia-will-no-longer-get-a-single-government-website-447255](http://www.itnews.com.au/news/australia-will-no-longer-get-a-single-government-website-447255) (accessed 12 May 2017).
- Coyne, A. 2016, *Australia Gets an Industry Body for IoT*, iTnews, [www.itnews.com.au/news/australia-gets-an-industry-body-for-iot-431057](http://www.itnews.com.au/news/australia-gets-an-industry-body-for-iot-431057) (accessed 3 April 2017).
- Department of Communications and the Arts 2015, *Updating Australia's Copyright Laws*, [www.communications.gov.au/have-your-say/updates/australias-copyright-laws](http://www.communications.gov.au/have-your-say/updates/australias-copyright-laws) (accessed 24 July 2017).
- DIIS (Department of Industry Innovation and Science) 2017, *Cyber Security Growth Centre*, [www.industry.gov.au/industry/Industry-Growth-Centres/Pages/Cyber-Security-Growth-Centre.aspx](http://www.industry.gov.au/industry/Industry-Growth-Centres/Pages/Cyber-Security-Growth-Centre.aspx) (accessed 23 June 2017).
- Donaldson, D. 2017, *Service Victoria: Not Delayed, Just Slower than Anticipated*, The Mandarin, [www.themandarin.com.au/79453-service-victoria-not-delayed-just-slower-anticipated/](http://www.themandarin.com.au/79453-service-victoria-not-delayed-just-slower-anticipated/) (accessed 13 June 2017).
- EY (Ernst and Young and FinTech Australia) 2016, *EY FinTech Australian Census 2016: Profiling and Defining the Fintech Sector*.
- Eyers, J. 2016, 'Banks call for data-sharing governance standards', *The Australian Financial Review*, 28 November.
- 2017, 'Start-ups form regtech industry association', *Financial Review*, 2 April.
- Fifield, M. 2017, *Improving Access to Copyright Material*, 22 March.
- Gordon, R. 2015, 'Secular stagnation on the supply side: US productivity growth in the long run', *Digiworld Economic Journal*, vol. 100, no. 4, pp. 19–45.
- Harper, I., Anderson, P., McCluskey, S. and O'Bryan, M. 2015, *Competition Policy Review*, Final Report, March, Australian Government.
- Hawkins, Z. and Nevill, L. 2017, *Australia's Cyber Security Strategy: Execution & Evolution*, Australian Strategic Policy Institute, [www.aspi.org.au/publications/australias-cyber-security-strategy-execution-and-evolution](http://www.aspi.org.au/publications/australias-cyber-security-strategy-execution-and-evolution) (accessed 25 June 2017).
- Head, B. 2017, *ASIC Plays in RegTech Sandbox*, [www.innovationaus.com/2017/02/ASIC-plays-in-RegTech-sandbox/](http://www.innovationaus.com/2017/02/ASIC-plays-in-RegTech-sandbox/) (accessed 12 May 2017).
- HM Treasury 2013, *Bank Account Switching Service set to Launch*, [www.gov.uk/government/news/bank-account-switching-service-set-to-launch](http://www.gov.uk/government/news/bank-account-switching-service-set-to-launch) (accessed 3 April 2017).
- Houghton, J. 2011, *Costs and Benefits of Data Provision*, Report to the Australian National Data Service, September, Centre for Strategic Economic Studies, Victoria University.



- 
- IA (Infrastructure Australia) 2016, *Australian Infrastructure Plan Priorities and Reforms for Our Nation's Future*, February.
- IP Australia 2016, *Australian Intellectual Property Report 2016*.
- ITS Aus (Intelligent Transport Systems Australia) 2012, *Australia a Leader in Linked Tolling Technology*, [www.its-australia.com.au/2012/06/australia-a-leader-in-linked-tolling-technology/](http://www.its-australia.com.au/2012/06/australia-a-leader-in-linked-tolling-technology/) (accessed 15 May 2017).
- ITU (International Telecommunication Union) 2017, *Global Cybersecurity Index (GCI) 2017*.
- Klein, A. and Knight, B. 2017, *How Fintech Can Take Off Without Getting Hampered by Regulations*, Brookings Institute, [www.brookings.edu/opinions/how-fintech-can-take-off-without-getting-hampered-by-regulations/](http://www.brookings.edu/opinions/how-fintech-can-take-off-without-getting-hampered-by-regulations/) (accessed 9 May 2017).
- Kleiner, M. 2015, *Reforming Occupational Licensing Policies*, 28 January, Hamilton Project Policy Brief, Brookings Institute.
- KPMG 2016, *Creating Connections: IoT Foundations for Smart Cities*.
- Lawrence, M. and Pollard, C. 2015, *A Year on Australia's Health Star Food Labelling System is Showing Cracks*, The Conversation, [www.theconversation.com/a-year-on-australias-health-star-food-rating-system-is-showing-cracks-42911](http://www.theconversation.com/a-year-on-australias-health-star-food-rating-system-is-showing-cracks-42911) (accessed 16 February 2017).
- Lim, M. 2017, *NZ Gets Real About IoT Future*, [www.innovationaus.com/2017/04/Nz-gets-real-about-iot-future/](http://www.innovationaus.com/2017/04/Nz-gets-real-about-iot-future/) (accessed 4 April 2017).
- Lim, N. and Perrin, B. 2014, 'Standard Business Reporting in Australia: Past, Present, and Future', *Australasian Journal of Information Systems*, vol. 18, no. 3.
- Maggiore, J.B. 2007, 'Remote management of real-time airplane data - Boeing', *Aeromagazine*, vol. Q307, article 4.
- Morrison, S. 2016a, *Address to the Fintech Australia Summit, Melbourne*, Speech, 4 November, FinTech Australia Collab/Collide.
- 2016b, *Launch of an Innovative Regulatory Sandbox for Fintech*, Media Release, 15 December, [www.sjm.ministers.treasury.gov.au/media-release/133-2016/](http://www.sjm.ministers.treasury.gov.au/media-release/133-2016/) (accessed 21 July 2017).
- Murray, D. 2014, *Financial System Inquiry Final Report*, 7 December, Australian Government.
- New, J. and Castro, D. 2015, *Why Countries Need National Strategies for the Internet of Things*, Center for Data Innovation, [www.datainnovation.org/2015/12/why-countries-need-national-strategies-for-the-internet-of-things/](http://www.datainnovation.org/2015/12/why-countries-need-national-strategies-for-the-internet-of-things/) (accessed 3 April 2017).

- 
- Nicholls, R. 2017, *If Scandals Don't Make us Switch Banks, Financial Technology Might, The Conversation*, [www.theconversation.com/if-scandals-dont-make-us-switch-banks-financial-technology-might-72361](http://www.theconversation.com/if-scandals-dont-make-us-switch-banks-financial-technology-might-72361) (accessed 9 May 2017).
- Payments UK 2017, *Current Account Switch Service*, [www.paymentsuk.org.uk/projects/current-account-switch-service](http://www.paymentsuk.org.uk/projects/current-account-switch-service) (accessed 12 May 2017).
- PC (Productivity Commission) 2011, *Identifying and Evaluating Regulation Reforms*, Research Report.
- 2012, *Impacts of COAG Reforms: Business Regulation and VET*, Research Report, Volume 3.
- 2014, *Access to Justice Arrangements*, Inquiry Report.
- 2015a, *Business Set-up, Transfer and Closure*, Inquiry Report.
- 2015b, *Mutual Recognition Schemes*, Research Report.
- 2016a, *Digital Disruption: What do governments need to do?*, Research Paper.
- 2016b, *Intellectual Property Arrangements*, Draft Inquiry Report.
- 2016c, *Marine Fisheries and Aquaculture*, Inquiry Report.
- 2016d, *Regulation of Australian Agriculture*, Inquiry Report.
- 2017a, *Consumer Law Enforcement and Administration*, Research Report.
- 2017b, *Data Availability and Use*, Inquiry Report.
- 2017c, *Telecommunications Universal Service Obligation*, Inquiry Report.
- Riley, J. 2017, *Local, State, Fed digital delivery*, InnovationsAus.com.
- Sadler, D. 2017a, *FinTechs Unhappy on Crowdfunding*, [www.innovationaus.com/2017/06/FinTechs-not-happy-on-crowdfunding/](http://www.innovationaus.com/2017/06/FinTechs-not-happy-on-crowdfunding/) (accessed 13 June 2017).
- 2017b, *IP Changes an Act of 'Cowardice'*, [www.innovationaus.com/2017/03/Ip-changes-an-act-of-cowardice/](http://www.innovationaus.com/2017/03/Ip-changes-an-act-of-cowardice/) (accessed 23 June 2017).
- 2017c, *Nobody Playing in Govt Sandbox*, [www.innovationaus.com/2017/05/Nobody-playing-in-govt-sandbox/](http://www.innovationaus.com/2017/05/Nobody-playing-in-govt-sandbox/) (accessed 30 May 2017).
- Sallet, J. 2017, *The Internet of (Economic) Things*, Brookings Institute, [www.brookings.edu/blog/techtank/2017/04/12/the-internet-of-economic-things/](http://www.brookings.edu/blog/techtank/2017/04/12/the-internet-of-economic-things/) (accessed 18 April 2017).
- Schwab, K. 2016, *The Fourth Industrial Revolution*, World Economic Forum, Geneva.
- Shillito, M. and Stokes, R. 2015, *Governments Want to Regulate Bitcoin – Is That Even Possible?*, [The Conversation](http://www.theconversation.com),

- 
- [www.theconversation.com/governments-want-to-regulate-bitcoin-is-that-even-possible-39266](http://www.theconversation.com/governments-want-to-regulate-bitcoin-is-that-even-possible-39266) (accessed 9 May 2017).
- Smith, D. and Poologasundram, V. 2014, *Coalition's FOFA 'streamlining' will destroy protections*, UNSW Newsroom, [www.newsroom.unsw.edu.au/news/business-law/coalitions-fofa-streamlining-will-destroy-protections](http://www.newsroom.unsw.edu.au/news/business-law/coalitions-fofa-streamlining-will-destroy-protections) (accessed 23 June 2017).
- Stratix 2015, *Internet of Things in the Netherlands: Applications, Trends and Potential Impact on Radio Spectrum*, September, Commissioned by the Ministry of Economic Affairs, Hilversum.
- The Network and Information Technology Research and Development Program 2014, *Smart and Connected Communities Framework*.
- Thierer, A. 2014, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, Mercatus Center George Mason University.
- , Hobson, A., Koopman, C. and Kuiper, C. 2015, *How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the 'Lemons Problem'*, Working Paper, 26 May, Mercatus Center George Mason University.
- Towell, N. 2017, 'How the Turnbull government killed off its big website dream', *The Canberra Times*, 12 January.
- UK Government 2017, *Digital Service Standard - Service Manual*, [www.gov.uk/service-manual/service-standard](http://www.gov.uk/service-manual/service-standard) (accessed 4 July 2017).
- West, D.M. 2016, *Securing the future of driverless cars*, Brookings Institute, [www.brookings.edu/research/securing-the-future-of-driverless-cars/](http://www.brookings.edu/research/securing-the-future-of-driverless-cars/) (accessed 4 July 2017).
- Winterford, B. 2011, *\$45k Stolen in Phone Porting Scam*, iTnews, [www.itnews.com.au/news/45k-stolen-in-phone-porting-scam-282310](http://www.itnews.com.au/news/45k-stolen-in-phone-porting-scam-282310) (accessed 17 May 2017).