Black Economy Report - Privacy

Privacy

The Black Economy Final Report makes many suggestions on data sharing, suggesting a new Data Sharing Act as they say the current Privacy laws contain outdated secrecy provisions and a strong cultural bias against using data more intelligently. They make many suggestion that seem very intrusive- internet scraping, API access to social media sites, further consideration could be given to sharing de-identified data more broadly. (Beyond government agencies). Their suggestions seem intrusive, as they are calling for actions which override the current legal framework for privacy and may contravene the International Covenant on Civil and Political Rights, which Australia has signed.

International Covenant on Civil and Political Rights

http://www.austlii.edu.au/au/other/dfat/treaties/1980/23.html

Article 17

1. No one shall be subjected to **arbitrar**y or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to **the protection of the law against such interference** or attacks.

(Dictionary definition of arbitrary: (of power or a ruling body) unrestrained and autocratic in the use of authority.

based on random choice or personal whim, rather than any reason or system.

Some points they make about data (direct quotes)

- At the vanguard of the information revolution are a select group of firms, researchers andgovernment agencies. They recognise the potential for data, widely

defined, **to identify commercial opportunities** (**whether in finance** or understanding consumer behaviour)

- In a world awash with information, individuals, firms and indeed governments must learn how to harness it for their ends.
- Data is increasingly being seen as central to value creation rather than an add-on.
- In the information age, data must be seen in a fundamentally different way. As the Productivity Commission has pointed out, it is a powerful, yet underutilised, asset.
- **Privacy and other protections** can be 'engineered' into the way the ledger works. Any **data strategy, therefore, must not be set in stone.** In a few years, technological change may make it redundant. For that reason, the focus should be on priority concerns, specific, purpose-directed initiatives and cultural attitudes (No 'set in stone' legal data strategy for public ledgers??)
- The private sector has made large steps in this area and is probably 3-5 years ahead of the public sector. It is no exaggeration to say that we are witnessing a data revolution in business. **The same thing needs to happen in government.** … The ATO has significantly upgraded its data analytics capabilities in recent years, but remains behind the private sector leaders in this field
- Reforms in the area of individual and business identity, **moving people into the banking system** and contractor reporting will, if implemented, **significantly improve both the quality and range of data at the disposal**
- Indeed, the public assume data is exchanged between agencies already… It is no generalisation to say that the public see government as a single entity. They expect agencies to share data and insights as a matter of course (There are no references to research proving these statements are true??)

Cultural impediments (direct quotes)

- While government data, and in particular information provided by the public, should always be used lawfully and prudently, the traditional cultural attitude, at least in some cases, goes beyond this. Agencies collect more information than ever, but there is still **an instinctive reluctance to make use of it**, <u>even where the current law allows it</u>. **This mindset needs to change.**
- As the ProductivityCommission has pointed out, there is a cultural problem here, a mindset that data must be hidden away rather than seen as an asset.
- (They recommend that the proposed future **Data Sharing Act…)** would replace the current arrangements, which include a patchwork of specific data sharing agreements, **outdated secrecy provisions** and a **strong cultural bias against using data more intelligently.**

Legal Impediments (direct quotes)

- Potentially rich data sets are underutilised, in part because of outdated secrecy laws
- The primary legal impediment to more effective use of data is typically not the *Privacy Act*, but regulations and guidelines specific to the field in which the data is collected

- … much of this legislation is outdated, reflecting the concerns of a bygone age
- Government agencies' use of data is limited by a complex range of secrecy and other legislative restrictions.
- The ATO has significantly upgraded its dataanalytics capabilities in recent years, but remains behind the private sector leaders in this field.
- Why is this the case? After all, governments are spending more on information technology than everbefore. Agencies, for their part, have access to far more data. The two main reasons are **legislative impediments**, including **outdated privacy and secrecy laws**, and cultural attitudes.
- (They suggest) … revising the secrecy provisions applying to the ATO andother key Commonwealth agencies… Modernising the secrecy provisions of relevant agencies…. **Reform of the secrecy provisions** would allow increased data sharing
- (The proposed Data Sharing Act) The Act should, wherereasonable, **override existing secrecy provisions** that prevent agencies from gaining access toother agencies' data or providing their data to other agencies.
- Government collects a lot of data**, but current secrecy laws are complex and strongly restrict sharing of data** for the purpose of government administration and law enforcement.

Their suggestions (direct quotes):

- The government should have API access to use data held by social media providers. API are a set of functions and procedures allowing the creation of applications that access the features or data of **an operating system, application, or other service.**
- Agencies should be allowed to share data and information with other government agencies. Further consideration could be given to sharing **de-identified data more broadly**
- These costs will fall disproportionally on the agencies that collect large volumes of data and are required to share it... Government may consider **some sort of compensation mechanism** for agencies that share large volumes of data (banks?)
- Consideration should also be given to the relative costs and benefits of agencies developing these tools in-house **compared to using or adapting solutions developed** internationally or **in the private sector.** (So they would data mining tools that social media and banks, like google already have)
- The Government should also keep a continual look out for other opportunities to **access and makeuse of data held by third-parties.**
- Web scraping, which hasn't been tested in Australian law yet to see if it contravenes copyright or human rights laws
- We recommend the creation of a ***Data Sharing Act (the Act)*.** This would create a **positive obligation** on officials to share data

- Further consideration could be given to **sharing de-identified data more broadly,** as per the Productivity Commission's proposed '*Data Sharingand Release Act*' (see below). (Sharing with private companies like banks? Or sharing health data with insurance companies like the UK did)
- These features of distributed ledgers make it an ideal candidate to **host a single record of an entity's records across federal, state and local government agencies**. (This makes them a honeypot for hackers)

Black Economy Final Report

Source of direct quotes

P107 Potentially rich data sets are underutilised, **in part because of outdated secrecy laws... Indeed, the public assume data is exchanged between agencies already**… As the ProductivityCommission has pointed out, there is a cultural problem here, **a mindset that data must be hidden away rather than seen as an asset.**

P107 The private sector has made large steps in this area and is probably 3-5 years ahead of the public sector. It is no exaggeration to say that we are witnessing a data revolution in business. The samething needs to happen in government. Two reform priorities stand out. **First, there needs to be far more data sharing and collaboration across agencies, mirroring what we have seen in national security since 9/11.** Second, data analytics need to be brought up to 21st century standards, in linewith the data revolution we are seeing outside government.

P107 As a result of the 9/11 Commission recommendations, the USA set up the Information SharingEnvironment (ISE) which facilitates the sharing and safeguarding of terrorism-related information.This brings together federal, state, local and private sector partners.

The Northwest Joint Analytical Center/ Washington Joint Analytical Center (NWJAC/WAJAC) whichwas set up as part of the ISE uses an 'all-crimes approach'. This includes collecting and **analysing both criminal and non-criminal information** to improve the depth, speed and coordination of analysingterrorism and other threats.

P108 An individual, firm or government department **can have access to all thepowers and resources it may desire,** but will be singularly **ineffective if it is deprived of data**, unableto make sense of it, or unable to translate it into action. Data matching across agencies, when donewell, promises to exponentially increase our capacity to pinpoint risks and vulnerabilities, but also tobetter tailor services. The data agenda also requires more standardisation of data, the collection andstorage of data in usable ways and better data analytics.

P108 **It is no generalisation to say that the public see government as a single entity. They expect agenciesto share data and insights as a matter of course.** This is particularly the case for cross-cutting policyand regulatory problems. It is true that in

some areas, including counter terrorism, agencies are‘talking to each other’ more than ever before. With some exceptions, however, this has not been thecase for the black economy. Whether it is phoenixing, visa or welfare abuse, sham contracting or theperennial problems of undeclared takings or wages, existing data sets, if intelligently used, canpinpoint risks and vulnerabilities.
P108 The internet, an exponential increase in computing power and acceleration in scientific and commercial innovation are underpinning this. We are only starting to appreciate howthis revolution will change our lives. There is no doubt that it promises lasting benefits, but it alsopresents challenges. In a world awash with information, **individuals, firms and indeed governments must learn how to harness it for their ends.** In this decentralised eco-system, misinformationbecomes a greater threat.
P108 At the vanguard of the information revolution are a select group of firms, researchers andgovernment agencies. They recognise the potential for data, widely defined, to identify commercial opportunities (whether in finance or understanding consumer behaviour), achieve medical breakthroughs or fight terrorism (in the case of our intelligence agencies). In our Interim Report we highlighted the use of internet scraping technology by German authorities. During our consultations,we saw evidence of **how social media resources can be used by investigators** to identify links among a large number of individuals, piecing together networks that otherwise would be hard to detect.
P109 Leading edge organisations are developing an impressive range of analytical tools including specialised algorithms to deal with big data which enables predictive modelling and undertakes arange of other functions. They recognise that data is not just about hardware. Data scientists arebeing appointed. **Data is increasingly being seen as central to value creation rather than an add-on.**Organisational cultures are being examined from this perspective.
P109 The ATO has significantly upgraded its dataanalytics capabilities in recent years, but remains behind the private sector leaders in this field.
Why is this the case? After all, governments are spending more on information technology than everbefore. Agencies, for their part, have access to far more data. The two main reasons are **legislative impediments, including outdated privacy and secrecy laws, and cultural attitudes.**
P109 ‘Legislation restricting access to data was formulated up to a century ago, and much of it is no longerfit for purpose. **The primary legal impediment to more effective use of data** is typically not the *Privacy Act*, but regulations and guidelines specific to the field in which the data is collected’.
- Productivity Commission Inquiry into Data Availability and Use, 2017
P109 **Government agencies’ use of data is limited by a complex range of secrecy and other legislativerestrictions.** These are set out each agency’s enabling legislation, the multiple laws governing the programs and policies they administer and other provisions. As the Productivity Commission hasobserved,1 much of this legislation is outdated, **reflecting the concerns of a bygone age**, and not more restrictive than the

Privacy Act, which should be the main guarantor of this privacy. A holisticrenewal is required.

P110 We should not ignore the cultural barriers to data sharing. If legal reform took place, these wouldcontinue to frustrate efforts to better connect government. **Within the public service, data has traditionally been viewed as a potential risk, a resource to be hidden away and protected, allowingonly the selected few to see and study**. While government data, and in particular informationprovided by the public, should always be used lawfully and prudently, the traditional culturalattitude, at least in some cases, goes beyond this. Agencies collect more information than ever, butthere is still an instinctive reluctance to make use of it, even where the current law allows it. Thismindset needs to change.

P110 In the information age, **data must be seen in a fundamentally different way.** As the ProductivityCommission has pointed out, it is a powerful, yet underutilised, asset. Making better use of it within government is not incompatible with fundamental privacy concerns. While we are advocating forbetter data sharing, and the legal and cultural change required to enable it, we are not advocatingblanket access to data within government. There should be tiered levels of access across and withingovernment agencies. For instance, all or near all data should be available for sharing to agencies fornational security purposes, most data should be available for sharing to agencies for lawenforcement purposes, and less data should be available for sharing for administrative purposes.Staff access to data within each agency should be tailored to suit the needs of their job. Some usersmay need access to classified data whereas others may not need access at all.

P111 Other short-term actions should include **revising the secrecy provisions applying to the ATO andother key Commonwealth agencies** (to eliminate outdated restrictions), developing a central registerof data holdings by agencies, and pursuit of a data sharing agenda with the states and territories(discussed in Chapter 15). In the longer-term consideration should be given i**ncluding a single *DataSharing Act*** to promote this within government, but also to include necessary protections against abuse.

Distributed ledger technology, while still at an early stage, offers enormous potential for data sharing. An early example of this is the National Criminal Database. **With a distributed ledger, data can be shared instantaneously among a large population of users.** There is no need for a central register or database doing away with the risk, inefficiency and costs that this entails. **Privacy andother protections can be 'engineered' into the way the ledger works.** Any data strategy, therefore,must not be set in stone. In a few years, technological change may make it redundant. For that reason, **the focus should be on priority concerns, specific, purpose-directed initiatives and cultural attitudes.**

Our data strategy forms part of our wider suite of recommendations. **Reforms in the area of individual and business identity, moving people into the banking system** and contractor reporting will, if implemented, significantly improve both the quality and range

of data at the disposal of agencies.
Public support for greater data sharing within government will be greatest if the focus is on better enforcement of existing laws. Progress on this front pays an immediate revenue dividend, restoresconfidence in government administration and improves fairness. But data can also be used to makegovernment more efficient, responsive and also to lower red-tape burdens.

P113 The Government should implement a black economy data strategy which includes:
In the short-term:

- **Modernising the secrecy provisions of relevant agencies**

In the medium-term:
4. Improving data and information sharing between states and territories and the Commonwealth.
In the long-term:

- Introducing a whole-of-government *Data Sharing Act*.
- **Consider migrating government records** onto blockchain technology as the technology matures.
- **Reform of the secrecy provisions** would allow increased data sharing with state and territorygovernment agencies, such as state revenue offices and workers' compensation authorities.

P115 **We recommend the creation of a *Data Sharing Act (the Act)*.** This would create a **positive obligation on officials to share data**, subject to protections, where this might help in administering or enforcingthe law. It would replace the current arrangements, which include a patchwork of specific datasharing agreements, **outdated secrecy provisions and a strong cultural bias against using data more intelligently.** We recommend that the following features are factored into the design of the Act:
When can data be shared: The Act should empower the agency that holds the data to sharedata if it believes that the data or information is likely to assist the receiving agency to administer or enforce Commonwealth, state or territory laws. The Act should, wherereasonable, **override existing secrecy provisions** that prevent agencies from gaining access toother agencies' data or providing their data to other agencies.
Data should not be provided to an agency if the data is unlikely to assist it to administer orenforce a law. For example, this principle in the Act should disallow the disclosure of anindividual's sensitive personal health records to an agency that administers business grants.

What should this Act apply to: The Act should apply to both data and information. The Actshould also apply to connected datasets which may consist of datasets from multiple

agencies.
Who should be able to receive this data: Agencies should be allowed to share data and information with other government agencies. **Further consideration could be given to sharing de-identified data more broadly, as per the Productivity Commission's proposed '*Data Sharingand Release Act*' (see below).**
Privacy would need to be maintained. We are not recommending that there be wholesale sharing ofinformation for the sake of it. As noted above, sharing would only be within government, to assist inadministering and enforcing laws. The Act would not alter the application of the current secrecy orprivacy provisions as far as they relate to releasing information outside of government. Thosestringent protections of privacy would be maintained.
P115 As distributed ledger technology matures the Governments should be alert to the potential it offers for record storage and data sharing. The Chief Government Scientist of the UK describes distributed ledgers as a **'database that can securely record financial, physical or electronic assets for sharingacross a network through entirely transparent updates of information**'.5
P115 In contrast to centralised registry functions, distributed ledgers are very efficient because there is **noneed for a central authority to authorise changes to a record. The ledger could be programmed so that everyone can make changes to the ledger as long as they stick to a mutually agreed set of algorithmic protocols.** Alternatively, the ledger could also be programmed so that only one personcan make changes to records. Regardless of who makes changes to records on a ledger, all updatesto records can then be broadcast to the other entities on the ledger in real-time.
P116 The ability for distributed ledgers to maintain a consensus of replicated, shared, and synchronizeddigital data geographically spread across multiple sites allows for a single unique record of a state ofaffairs relating to an entity.
These features of distributed ledgers make it an ideal candidate to **host a single record of an entity's records across federal, state and local government agencies**. The entity could choose to share theirdetails with trusted government agencies so that they do not have to provide the same informationrepeatedly. This reduces the current inefficiencies associated with the cost of maintaining multipledatabases across various agencies.
Distributed ledger technology also offers the entity enhanced control and privacy over their data.The ledger could be programmed so that the entity can choose to share certain aspects of its recordswith trusted entities. For instance, the individual may authorise only the health-related state andfederal agencies to view its health records.
The Government's data sharing strategy should therefore remain flexible such that where and whenpossible, the Government can adopt such technology.
P117 Government collects a lot of data**, but current secrecy laws are complex and strongly restrict sharing of data** for the purpose of government administration and law enforcement. This is inefficient,reduces the information available to comprehensively address the black economy, and is contrary tothe community's expectations about

efficient data and information sharing.
P117 The Act should include a number of protections against the misuse of data, violation of privacy rightsand the risk of inappropriate access. At present, these protections are scattered across multiple lawsand regulations, with overlaps and duplication. Many of these laws are outmoded.
Given the development of a *Data Sharing Act* may take considerable time, **action also needs to betaken in the short-term by modernising the secrecy provisions of select agencies** which are likely tohave large amounts of relevant black economy data.
P117 *Productivity Commission's 'Data Sharing and Release Act'*
This proposal focuses primarily on providing researchers, private sector and governmentdepartments with access to data for the purpose of evidence based policy and service design. Itwould support the provision of de-identified data for this purpose. Our proposed Act, in contrast,would promote data sharing within government. It would allow for identified data to be shared,subject to the protections against abuse it would build in.
P118 **These costs will fall disproportionally on the agencies that collect large volumes of data and arerequired to share it for the benefit of other agencies. Government may consider some sort ofcompensation mechanism for agencies that share large volumes of data.**
P121 In addition to the upfront investment required to deliver improvements in data analytics capabilityacross government agencies, improvements in intra-government data analytics capability willrequire consideration of the *Australian Privacy Principles.* **Consideration should also be given to the relative costs and benefits of agencies developing thesetools in-house compared to using or adapting solutions developed internationally or in theprivate sector.**
P122 Internet scraping should be explored as a tool to identify black economy activities on the internetand social media platforms. Scraping could be used to better monitor transactions and identifyindividuals that are offering products or services to the public on a repeated basis, for example aperson that has been selling many items on eBay or Gumtree over an extended period (including thesale of contraband such as drugs) and may therefore be conducting a business which generatestaxable income rather than hobby. We also have heard examples of international students sellingparticular items, like infant formula and vitamins, back in their home countries through onlinemarketplaces. This information could be matched with tax returns and income reported to DHS tocheck whether income has been reported to authorities. Web scraping is used by a number ofcountries on a systematic basis already, including by German and Dutch tax authorities. **The provision of API access** to allow regulators to use data held by social media providers to identifyblack economy activities would also be desirable.
P122 The Government should also keep a continual **look out for other opportunities to access and makeuse of data held by third-parties.** As technology changes and new systems are adopted by businessesand consumers, tax and other regulatory authorities

may be able to tap into them, where appropriate, to ensure that information is reported where the transactions are considered high-riskfor the black economy