29 July 2016

Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra City
ACT 2601

To the Commissioners

IAG welcomes the opportunity to make a submission to the Productivity Commission Inquiry into Data Availability and Use. At IAG we are in the process of building a customer-led and data-driven organisation. Data is fast becoming one of the most important assets for large companies like IAG, and our ability to use it to give customers what they need is a core part of our strategy.

Please find attached IAG's submission to the Inquiry. If you would like to discuss any aspect of this submission or require additional information please contact:

Gulshan Singh
Manager, Public Policy & Industry

Yours sincerely,

Peter Harmer
Chief Executive Officer
Insurance Australia Group

19 July 2016

PRODUCTIVITY COMMISSION INQUIRY INTO DATA AVAILABILITY & USE

Australia

New Zealand

Asia

Contents

Contents

Continued.

Executive summary

IAG welcomes the opportunity to contribute to the Productivity Commission Inquiry into Data Availability and Use. IAG in principle supports greater availability of both private and public sector data to stimulate innovation and elevate Australia's international competitiveness. IAG has a long history of advocating in the public interest for access to natural perils data held by government. Open government data will facilitate more accurate insurance coverage for a wider range of risks and enable better mitigation and risk management measures in the community. In the near future access to in-vehicle and infrastructure data will be critical to the advancement of autonomous vehicles and the ability to provide insurance cover.

IAG recognises there may be instances where increased accessibility and sharing of private sector data could benefit the public and supports government measures that eliminate barriers and incentivise voluntary sharing where appropriate. Data pooling across sectors already occurs through commercial and gratuitous arrangements and government can play a role in facilitating market solutions for more widespread data sharing. Guidelines and controls are needed to encourage the release of commercial proprietary data through mechanisms that create a level playing field and fair value exchange for private sector data access. Where there is a clear public interest benefit, government already have available mechanisms to compel the release of private sector data.

The benefits of open data need to be balanced with the numerous consumer risks posed by greater availability of data. Privacy can be protected to some extent by implementation of the Australian Privacy Principles and best practice data management. However privacy breaches are only one example of potential consumer detriment arising from data misuse. Transparency and ethical use of data are essential to ensure consumer benefit from data sharing. While regulation is incapable of addressing the wide array of constantly evolving opportunities for data misuse, there are strong market incentives exist to maintain consumer trust and handle data appropriately. Consumer protection can be further strengthened by government initiatives to educate citizens about the digital environment.

Security of data is an important consideration in an escalating and increasingly sophisticated cyber threat landscape. Increased connectivity, third party data storage, mobile workforces and cloud computing are increasing the vulnerability of organisations to cyber risks. Global and cross sector responses are needed to manage and limit the impacts of cyber threats. Organisations in both the public and private sectors need to better understand cyber risks and have stronger cyber defences.

As predictive analytics, virtual reality and artificial intelligence move into the mainstream, the implications (and capabilities) of data use will become even more urgent and complex. Data collection and use will become increasingly contextual and fluid according to the networks, services and devices we use, and the ways in which we use them. There are many uncertainties about how the impact of the scale of mass connectivity, new technologies and speed of change will affect the regulatory environment. Government intervention should be approached with caution and, where possible, regulation delayed until the market matures and the true implications of data usage are better understood.

Recommendations

1. Valuable public data should be shared via a reasonably standardized data portal infrastructure to allow easy access by the public and private sector.

2. Where appropriate the Productivity Commission should explore voluntary and collaborative options to unleash the value of private data for greater consumer and national benefit.

3. Regulation should be approached with caution and where possible delayed until new technologies are better understood.

4. Policy development to increase data availability and use should be accompanied by implementation of Australia's Cyber Security Strategy, together with public campaigns to increase cyber security skills and awareness in the community.

Public sector data

Public sector data sets can be used by the insurance sector to create value for the community in a number of ways. IAG uses natural hazard and census demographic information to improve its understanding of risk. This in turn allows IAG to provide premiums that accurately and fairly represent a customer's risk and enhance our response during major events. IAG also has specialised teams with advanced analytics capabilities who use census demographics to deliver market leading insights to enhance and constantly improve the customer experience. The combination of public data with IAG's internal enthnographic research and analytics can generate powerful insights to enable greater personalisation of insurance services and better meet the individual needs of our customers.

High value public sector data

1. Natural Perils

IAG uses natural hazard and weather information to get a clearer understanding of the impact of a major event such as a cyclone, bushfire or flood, before, during and after they strike. This allows IAG to scale its major event response rapidly to help affected customers recover from the event quickly, as well as notify our business partners, such as reinsurers, and the share market of the impact.

Insurers require raw data that can be analysed and uploaded into underwriting systems to facilitate risk assessment on an automatic and broad scale basis when residents seek a quote. The insurance industry provides in excess of 15,000 quotes for property insurance every working day across Australia. Insurers typically require GIS data for flood surfaces and extents for modelled events, as well as historical flood extents, levee details, and minimum floor levels. In New South Wales and Queensland, local councils are usually the primary source of this information.

IAG, individually and as a member of the Australian Business Roundtable, has an extensive history of advocating for greater public access to natural perils data. A key element of effective risk management by private individuals, businesses and Government is an understanding of the risks faced. Accurate information should be available to the public in a form which allows individuals to easily understand their level of risk. This level of transparency is essential to reduce confusion and encourage people to take steps to manage their risk (such as understanding the flood risk of a property they are buying and purchasing appropriate insurance cover).

Information is fundamental to natural hazards management. Ultimately, the goal is to ensure that communities, planners, emergency services, individuals, property owners and insurers understand the natural peril risks that they face, and that effective risk mitigation measures can be undertaken. Without access to critical data inputs and research findings, communities, business and government cannot make informed decisions on how to target these investments to achieve the greatest impact. Yet often councils and other authorities suggest that they are reluctant to provide specific information about risks such as flood or fire risk, to property owners or prospective purchasers. This reluctance arises from a fear of litigation that may arise if that information has adverse consequences, for example by reducing the market value of the affected property.

2. Mental Health

Increased availability of data has the potential to improve insurance access for people with mental health conditions. As community understanding and awareness of mental health conditions have increased over the past few years, there have been growing concerns about the suitability of existing insurance covers and definitions associated with mental illness. People experiencing mental illness have reported difficulty accessing and claiming insurance due to the broad definitions applied to mental illness.

Pricing the risks associated with mental illness is challenging for underwriters due to the diversity in the prevalence and prognosis of various mental health conditions. The Diagnostic and Statistical Manual of Mental Disorders (DSM), the American Psychiatric Association's standard reference for psychiatry, includes over 450 different mental disorders. Each disorder can have varying impacts on individuals.

As a risk-based product, insurers' access to sophisticated data is critical to their ability to assess and price risk that is specific to an individual. Better availability of data would provide insurers with information they could use to more accurately assess the risk of providing cover for mental illness related claims. Access to mental health statistics would assist insurers to apply loadings and exclusions that are better aligned with the true risk of the illness by taking into account the type of illness, its severity and its prognosis. The Insurance Council of Australia is keen to work with the Government to identify data that would be useful for the purpose of general insurance underwriting.

In 2015 the Insurance Council of Australia wrote to the Minister for Health indicating that the industry would like to work with government to enhance the data available for underwriting purposes. It was suggested that while the existing data indicates the proportion of the population with a mental health condition, it does not provide an indication of the propensity of people with conditions to make a claim. While actuarial data would be ideal, statistical data that provides more granular information about specific illnesses and effect of treatment could be useful.

IAG, distributing under the CGU brand is one of the few insurers that offer travel insurance cover for mental health conditions. IAG has established a mental health working group that is exploring sources of available data to support our understanding of mental health and further refine our pricing and product offering.

3. Injury prevention and recovery

Better data on road trauma is another area with potentially wide ranging community benefits. There is currently no nationally consistent collection of data on serious injury road crashes. Quality data, particularly on serious injuries would facilitate evaluation of road safety measures.

The UN Global Plan for the Decade of Action for Road Safety 2011–20202 recommends establishing and supporting national and local data systems to measure and monitor road traffic deaths, injuries and crashes. In order to monitor the effectiveness of strategies to reduce injuries and accidents it is essential to develop a national database on injuries resulting from road accidents. Although some states have made progress towards better collection of information (eg.Western Australia's online crash reporting) ANCAP Australasia have advised that better injury data would improve the specificity of its vehicle safety ratings, and over time, could lower the injury rate. The Australian Trauma Registry has already led to the development of a functional model that has considerable potential for broader linkages as other models develop.

Collection and release of public data

The research set out in the Business Roundtable's commissioned Report (2014) 'Building an Open Platform for Natural Disaster Resilience Decisions' shows that a fresh approach to the collation, co-ordination and analysis of natural disaster information and research is fundamental to the prioritisation of mitigation decisions that will help strengthen and safeguard our communities. http://australianbusinessroundtable.com.au/our-papers/natural-disaster-data-report

As outlined in 'Building an Open Platform for Natural Disaster Resilience Decisions' the key set of inputs required by end-users consists of:

- **Foundational data**: data that provides the basic standard layers of locational information. This includes the characteristics of assets at risk, community demographics, topography and weather details, which are also used for other purposes
- **Hazard data**: hazard-specific information on the risks of different disaster types, providing contextual details about the history of events and the risk profile of Australian locations
- **Impact data**: data on the potential and actual impacts associated with natural disasters, including information on historical costs and damage, and the current and future value at risk

- **Research activities**: actions that draw on data and seek to answer specific questions across a range of areas. There is often also feedback from research to data, because research outputs build on the existing stock of data that is available.

The value of releasing data items into a reasonably standardized data portal infrastructure is that both public and private organizations can very easily access the data and experiment, at lower initial cost, in creating value from the data.

The National Map website for map-based access to Australian spatial data from government agencies has been a positive first step in this direction. The National Map is an initiative of the Australian Commonwealth Government's Department of Communications and the software has been developed by NICTA working closely with the Department of Communications, Geoscience Australia and other government agencies.

http://www.nationalmap.gov.au/

Private sector data

High value private sector data

IAG recognises the potential value of combining various disparate data sets for our business and the broader community. To create a data enabled economy and remain internationally competitive we accept that avenues are needed to unleash the innovative benefits of data sharing.

IAG uses the data it collects in the following ways:

- Pricing and issuing of policies
- Claims processing
- Fraud analytics
- Re-insurance
- Financial and insurance accounting
- Predictive modelling, analytics and insights
- Operational reporting
- Legal and compliance reporting
- Performance analysis and management
- Share data with partners (without compromising on customer's privacy) to provide value add services
- Risk management
- Data experimentations

There are a number of areas in which private insurance data can be used to create better outcomes for the community.

a) Land use planning

The understanding of natural peril risk at the government, business and community level has been undermined by a lack of national, comprehensive natural peril data and mapping. This has itself contributed to poor planning decisions leading to development in areas of unacceptable risk. Insurance data, when combined with other data sets has the potential improve the risk sensitivity of land use planning to ensure risk appropriate new development in high-risk areas and addressing legacy issues through a coherent, long-term strategy.

b) Mitigation investment

The budgetary impact of responding to and recovering from natural disasters could potentially be significantly reduced through carefully considered and directed investment in pre-disaster resilience. By making information on disaster risks and resilience options more accessible, decision making about preferred mitigation approaches and investment can be optimised to deliver additional savings to government and minimise the impact of disasters on the most exposed communities.

c) Infrastructure investment

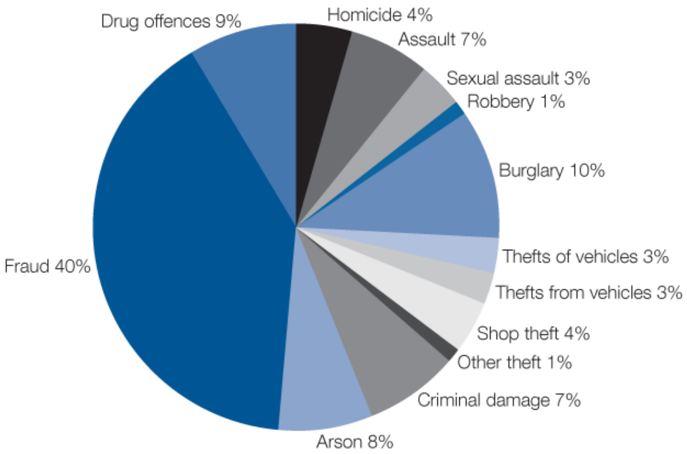
Ensuring areas with the highest levels of economic activity are protected from the risk of natural disasters by wise infrastructure investments will help to maintain economic growth. This requires government to understand the distribution of economic growth and the risk of natural disasters. Over laying the risk of natural disaster to economic and social data across Australia will help to highlight to all levels government where priority investments should be made.

d) Risk management

Meaningful insurance data linked to other sources of information can assist individuals to make decisions and better manage their personal risks. For example availability of information on exposure to natural perils of individual properties and the potential costs of premiums can help purchasers make more informed decisions about the risk they are prepared to take on when purchasing a property. Through the connectivity of the 'internet of things' there will be potential to provide insights on a range of ways to modify personal behaviours to reduce risk.

e) Fraud prevention

According to the Australian Institute of Criminology, fraud costs the Australian community up to $8.5 billion a year. It affects the private and public sectors alike, with many individuals perpetrating frauds against both. It is in all our interests to prevent fraud, and public authorities have a particular responsibility to ensure that taxpayers' money is not taken out of the system fraudulently.



http://www.aic.gov.au/crime_community/communitycrime/costs.html

In NSW the State Insurance Regulation Authority estimates fraudulent claims cost that state's motorists up to $400 million extra each year in CTP or "green slip" premiums. During a visit to Australia in June this year, the head of a recent British government insurance fraud taskforce David Hertzell suggested local insurers could do more to "break down silos" of information. He pointed to the success of Britain's industry-funded Insurance Fraud Bureau.

Existing data sharing initiatives

Many businesses have already identified the commercial benefits of data sharing and collaboration to increase innovation and improve services. IAG is already involved in a number of data sharing initiatives with the insurance industry, governments, academia, other businesses and with the general public.

a) Industry

National Flood Insurance Database (NFID) – the NFID is funded and managed by the general insurance industry. It combines all available government flood data into a format that is practical for insurers to use for underwriting flooding risks at address level. Where a local or state government has provided flood data of an appropriate standard, NFID provides participating insurers with estimations for the depth of flooding (if any) at each individual address for the one-in-20 year, one-in-50 year, one-in-100 year and Probable Maximum Flood (PMF) events. Where data has not been made available by government, insurers may not be able to offer premiums that reflect the precise nature of flooding for the location.

However the NFID is not complete for a variety for reasons including out-dated flood mapping, inconsistent approaches to the determination of flood risk, refusal of a number of councils to release mapping, lack of consideration being given to the effects of climate change or an absence of flood mapping being undertaken at all.

The ICA Property Resilience and Exposure Program (PREP) facilitates data sharing between local governments and the insurance industry. PREP centralises raw data in a consistent format that can then be used by all participating insurers. PREP has three levels or layers:

- Level 1 Exchange of relevant hazard data – Local government delivers all locally held hazard mapping. Information is processed by ICA into the National Flood Information Database (NFID) for use by participating insurers, in addition to the raw hazard data being made available through a centralised process on the ICA's DataGlobe.
- Level 2 Provision of building data – Local government provides address-specific building data that may assist insurers to understand building vulnerability to a greater degree (such as floor heights above modelled flooding)
- Level 3 Provision of resilience mapping – Joint identification between industry and local government regarding where buildings are exposed and vulnerable to local hazards, and may benefit from mitigation activity.

b) Academia

Most recently IAG and Suncorp have partnered with the Cyclone Testing Station at James Cook University (JCU) to study the impact of tropical cyclones on strata properties in North Queensland. The study is to help better understand the impact of wind-driven rain and water entry, which affects insurance costs for residents in strata properties, and is a major cause of damage to buildings. IAG and Suncorp will share data with JCU to use in its research, which will provide designers, builders and insurers with a better understanding of the common drivers of claims costs in strata properties during cyclones. The study will also provide recommendations to help mitigate against the impacts of cyclones for residents.

c) The community

i) Safer Homes

There has been a growing focus on insurance data and the 'information asymmetry' that exists between general insurance companies and their customers. Both the Financial System Inquiry and Productivity Commission Inquiry into National Disaster Funding highlighted the need for insurers to communicate natural perils risks to the public. In response to these recommendations, in October 2015 IAG created the Safer Homes website to educate customers on the key risks in their suburb. In May 2016 this tool was further refined to enable identification of the level of risk of flood and bushfire at an individual property level rated out of low, medium and high. This provides our customers with a deeper understanding of insurance and the risks they face within their local area.

SAFER HOMES
Find out how understanding your suburb can help you better protect your home.
Enter your suburb or postcode...

http://saferhomes.nrma.com.au/

ii) IAG Research Centre

IAG has an extensive history of sharing its data to improve road safety in the Australian community. The IAG Research Centre works with the automotive industry to carry out physical testing and data analysis to help reduce the impacts of motor vehicle accidents. The IAG Research Centre also advises consumers on car safety issues and provides technical information for the smash repair industry. https://iagresearch.com.au/index.php/car.html

d) Other businesses

IAG has collaborated with other businesses to combine data to support the activities of the Australian Business Roundtable. The member organisations of the Australian Business Roundtable formed in December 2012, the Australian Red Cross, IAG, Investa Property Group; Munich Re; Optus and Westpac have shared and pooled their data to produce four research reports to build an economic case for investment in building resilience to make our communities safer. This collaboration and sharing of information across industries has made a significant contribution to informing public policy to help government, business and communities better prepare for natural disasters.

e) Government

Govhack

As a sponsor of GovHack, IAG intends to provide digital access to a subset of our existing risk data sets at the GovHack2016 event to give GovHack participants access to high-quality, accurate risk datasets for use in innovation. No personally-identifiable or sensitive information will be included and the data will be made discoverable on a public open data portal. IAG hopes the release of risk data in this form will support innovation by start ups, entrepreneurs and government agencies and enable the development of new concepts to increase risk awareness.

GovHack

empower. enable. connect.

https://www.govhack.org/

Local councils

IAG supported Rockhampton Regional Council’s efforts to improve community resilience by working with Council to explore the likely impact that reducing flood risk in the community could have on insurance premiums. By working with the technical experts in our Natural Perils Research Team and using insights from our industry leading flood risk analysis system, IAG was able to show the levee would potentially decrease the flood component of premiums for approximately 1,250 properties in Rockhampton, Port Curtis, Depot Hill and Allenstown. Our customers could see reductions to the flood component of their premium of between 11% and 76%, depending on the level of flood risk at the property and other factors such as sum insured and expected levels of damage. By sharing our expertise, we have been able to give the local community a better understanding of the benefits and costs involved in the levee.

Regulators

Government is currently already able to access private sector data when it is in the public interest. For example the Australian Prudential Regulation Authority (APRA) has powers to compel data collection, and a long-standing set of protocols and procedures to regulate release of the data items gathered. ASIC also possesses a range of compulsory information-gathering powers that can be used proactively to examine the industry environment or test a concern, issue or practice. This includes a Power to require the production of documents which includes electronic data and files.

Concerns of private sector data owners

Release of private sector data entails numerous business risks and government has a role to play in developing and implementing policies that mitigate business concerns.

a) Impacts of data release on competition

The private sector has legitimate concerns about mandated release of its valuable internal data. Companies such as IAG have invested considerably to collect data from various sources over a number of years and therefore would be reluctant to release that data freely or at no charge. For example, IAG has invested heavily in sourcing quality data and researching flood risk to accurately understand all the factors involved in flood risk. We have derived data from a large range of diverse and independent sources; and employ publicly available and off-the-shelf technology as well as our own programs to utilise this information. IAG opposes legislative or regulatory change that compels organisations to release data in which it has legitimate commercial interests in protecting, except in rare circumstances when release of data in the public interest is imperative.

b) Reduced incentives to invest in data

Organisations have made large investments to grow, analyse and maintain their datasets in order to achieve a competitive advantage. Businesses are also facing rapidly increasing costs of managing cyber security risks to protect their data. If businesses are required to release data to competitors at no cost they are unlikely invest in future collection of data.

c) Liability

When considering access to private sector data, personal and general data will require distinct and separate approaches. Clear guidelines will need to be established on the use of private sector data by another entity, and clarity on where the liability lies if that data is misused or subsequently determined to be inaccurate.

d) Practical challenges of data release

There are major challenges around linking data together, due to a lack of consistency in the content and assumptions behind each dataset. Commercially sensitive and complex enterprise data can be costly and time consuming to collect and process into a commercially de-sensitised, anonymised and consistent form suitable for public release.

Possible principles and protocols for sharing of private sector data

While the public sector is making some progress in identifying opportunities for bringing different datasets together, it is understandably more challenging for businesses in a competitive market to share valuable data with one another or with Government. There are a number of models overseas that can offer guidance for a solution in Australia. IAG supports private sector data sharing through a collaborative and co-operative approach that incentivises and facilitates the voluntary data sharing of proprietary and commercially sensitive information.

1.) Facilitate data 'trading' between organisations

Access to proprietary corporate data can not necessarily be expected without cost. Data sharing or 'trading' between businesses is a natural outcome of market forces as awareness of the commercial value of data grows. The market is already responding by creating data 'ecosystems' to create mutually commercially beneficial data sharing arrangements. In response to the threat of digital disruption and changing consumer preferences, incumbent industry leaders are joining together to form a co-operative of willing, aligned partners operating together to empower the customer through satisfying their whole of person needs.

Data processing services can be used to unify second party datasets, and extract commercially de-sensitised customer attribute records from complex enterprise data sets. As a result, customer attribute records generated by organisations can be combined with minimal effort to enable each individual organisation to infer deeper insights into their customers and create superior customer experiences.

Establishing mechanisms and guidelines for trading data may enable and encourage more widespread ecosystem style arrangements to share private sector data without impinging on proprietary rights. A vital component of creating markets in data will be the formation of trading hubs and exchanges where controlled access can be bought and sold and datasets appropriately curated. The ability to trade data in 'data markets' under rigorously specified conditions is therefore a necessary condition for gaining access to currently unavailable data held by private entities.

2.) Facilitate centralised data sharing with government

Sharing industry data with government rather than the general public is more acceptable to the private sector as it ensures a level playing field by removing the competitive disadvantage of volunteering data as an individual organisation. Canada and New Zealand for example have mandated private sector data to be open to their statistical offices. In Australia IAG submits that this outcome can be achieved through voluntary and industry led agreements rather regulation.

Industry led sharing of data can be facilitated by the creation of platforms to enable proprietary datasets to be released within a framework that promotes trust and practicality. In the rare situation that mandated data release appears to be indicated, the release should be preceded by public consultations to seek input on the case for and against the public release of the data in question and the acceptable format for that release.

3.) Facilitate data sharing with customers

The private sector will be more open to sharing its data with customers rather than its competitors. The Blue Button and Green Button initiatives in the United States and midata in the United Kingdom are voluntary programs the Government is undertaking with industry to give consumers increasing access to their personal data in a portable, electronic format. Individuals will then be able to use this data to gain insights into their own behaviour, make more informed choices about products and services, and manage their lives more efficiently.

4.) Provide greater certainty to encourage data sharing

Private sector organisations have rich data that they are unwilling or feel unable to share because the acceptable boundaries for sharing and reuse may be unclear. Development of standards or codes for private sector data usage may encourage greater voluntary release of private sector knowledge. Knowledge transfer between companies and countries, as well as sectors, about experiences and best practices of data sharing will facilitate more rapid implementation, and help ensure that the benefits are realised.

5.) Share data in forms other than raw data

The public may more likely benefit from increased availability and use of private sector data when it is processed into meaningful information. Raw data poses greater risks of becoming appropriated and used by competitors or offshore companies. Monetisation of data could involve selling critical insights and desensitised customer attribute records to third parties in a controlled manner. For consumers to benefit from accessing their own data, the data must be in a meaningful and useful form.

6.) Consultative approach to mandatory data sharing

In the complex connected environment of big data and associated emerging technologies, problem-solving strategies will necessarily rely on a mix of participants. Therefore where it is considered to be in the public interest to compel the release of private sector data, consultation and collaboration between industry, government, citizen or consumer stakeholders will be critical to the design of any regulatory or non-regulatory initiatives.

The International Transport Forum of the OECD recommends that mandatory private-public data sharing should be limited: ‘Only where clear benefits to all parties exist and public authorities have capacity to handle the data should they be considered. Public authorities can compel regulated entities to provide data. They should do so when mutual benefits exist – for example, establishing data sharing schemes in return for transport service licensing – or when data sharing is required to deliver on public policy objectives. Simply requiring regulated parties to provide data may not be sufficient for authorities to extract useable information from it. The skills to understand, format, clean, parse and analyse large data streams are not typically found in the public sector. ‘

(ITC http://www.itf-oecd.org/sites/default/files/docs/data-driven-transport-policy.pdf)

7.) Develop suitable platforms for voluntary data sharing and collection

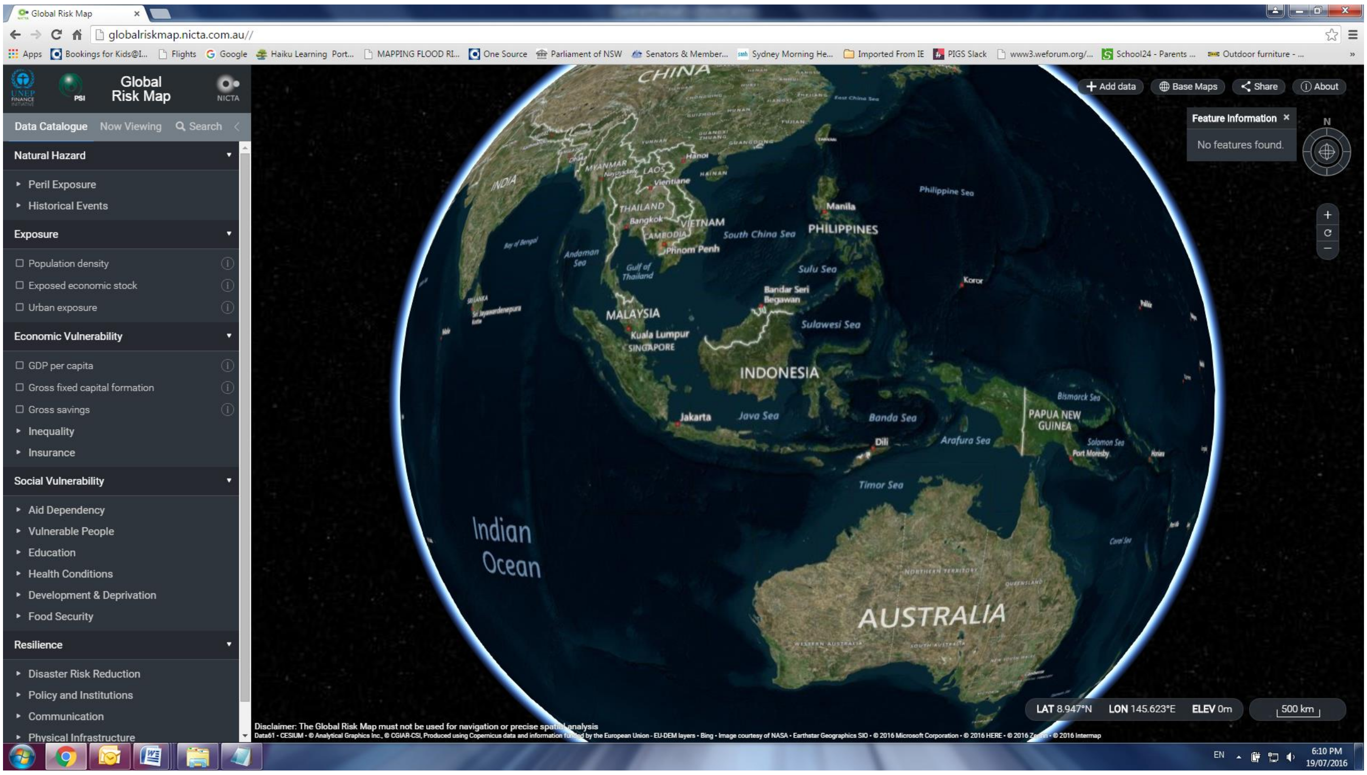
Secure data sharing platforms that deliver a clear public benefit are more likely to encourage voluntary data contributions from the private sector. For example, The Global Risk Map, the second phase of the PSI Global Resilience Project led by IAG uses Terria™ technology, built by the team at National ICT Australia (NICTA) that allows the user to benefit from the masses of datasets related to the project such as disaster response resources and insurance penetration and density. Terria™ maps allow users to search spatial data catalogues through all major web browsers. It is interoperable with a wide range of geographic information systems (GIS) back-end services and is Open Geospatial Consortium (OSG) compliant.

The Global Risk Map demonstrates the following data through an interactive tool:

- Exposure to cyclones, earthquakes, floods and related perils (geo-coded).
- Cyclone, earthquake, flood and related peril events since 1900 (country level).
- The economic and social impact of these events (county level).
- National-level vulnerability to each of these natural hazards.
- National-level resilience, covering vulnerability and coping capacity, including disaster risk reduction and insurance penetration and density (covering both general and life insurance).

Private sector data

Continued.



http://globalriskmap.nicta.com.au//

Consumer protection and data

The responsibilities that accompany personal data use are multilayered and extend beyond privacy and data security. Responsible data handling obligations are conferred on businesses through legislation, regulation, corporate values and customer and community expectations. Considering the pace and pervasiveness of data collection and technological developments, legislation will have limited ability to regulate all scenarios to protect consumers.

There will always need to be an element of self-regulation and self-imposed standards by organisations to maintain customer trust and the associated permission to collect and use customer data. IAG aspires to maximise the use of data, information and analytics to create world leading customer experiences. In order to access customer data in the future to achieve this objective, IAG and the rest of the business community will need to use data management frameworks that combine legal compliance with ethical treatment of data, transparency about use and close monitoring and responsiveness to community expectations.

Consumer trust correlates highly with a business' ability to expand the data it can access and use and the opportunities it can subsequently pursue. The growing focus on privacy arising from high profile data breaches internationally and in Australia may influence customers to withhold their personal data even where it is legally permissible for organisations to collect and store it. Privacy research regularly reveals that consumers will often volunteer more data and expect it to be exploited for their benefit when a business has been transparent about what it is intending to do with information, and puts unconditional control in the hands of the Data Subject, i.e. providing differing levels of service dependent on the permissions granted, not taking an 'all or nothing' approach.

Privacy is only one of many consumer protection considerations associated with increased data availability and use. Increasingly, companies are using machine algorithms instead of humans in developing their analytical capabilities. Machine algorithms do not have a fundamental understanding of data context, sensitivity or appropriate usage. This means that the analysis should consider the benefits and risks to the individual, for society as a whole, and for the parties conducting big data discovery and application. Moreover, data protection requires a full understanding of the potential impact of big data on the full range of human rights, not just those related to privacy.

The Australian Communications and Media Authority's occasional paper on the 'Internet of Things' identified an opportunity in this innovative environment to also focus on the development of the necessary skills and confidence of citizens and consumers so that they can operate productively in shaping their connections and information exchange for Internet of Things applications. Digitally empowered and aware consumers are likely to be a necessary adjunct to minimise risk of data misuse.

Privacy

IAG supports minimum standards of best practice data usage by all organisations using customer data including 'privacy by design', privacy impact assessments and de-identification as outlined in the Office of the Australian Information Commissioner's Privacy Management Framework. The Office of the Australian Information Commissioner has also developed the draft Guide to Big Data and the Australian Privacy Principles to facilitate big data activities while protecting personal information. In response to the Government's consultation on draft legislation, the Privacy Amendment (Notification of Serious Data Breaches) Exposure Draft Bill 2015, IAG and the Insurance Council support the introduction of a pragmatic mandatory breach notification regime.

However regulation is unlikely to be able to address the entire spectrum of data privacy issues. Data de-identification techniques, and in particular techniques for de-identifying location and trajectory data, is continuously evolving. Confidence in anonymisation is increasing challenging given the growing sophistication of re-identification and inference-based attacks on de-identified location and trajectory data.Ultimately it will depend on an organisation having a clearly defined value proposition and a set of principles that govern behaviour and are encoded into practice to protect and manage customer privacy from an ethical, social, legal and regulatory perspective.

IAG's approach to data

In addition to the practices outlined above, IAG uses three types of privacy lenses to identify risks and make informed decisions before it delivers any of its data products or data services for consumption by its customers, partners and third parties. The goal of this approach is to develop a capacity to incorporate ethical inquiry into IAG's normal course of doing business.

At IAG, we are promoting a 'privacy by design' culture by ensuring privacy and ethics are considered throughout the lifecycle of data (from collection to retention/destruction) for any data driven initiatives from a privacy impact and risk management perspective.

This culture is about getting the organisation think about privacy of the customers during planning stages of any initiative by applying the following lenses when dealing with customer's personal information and their privacy and managing the risks through informed decisions throughout the lifecycle of the initiative:

- Community/social expectations
- Ethical and moral obligations, and
- Legal and regulatory requirements

Data security

Cyber security and privacy are two distinct but related concepts. Open data policies must be cognisant of the escalating and increasingly sophisticated cyber threat landscape. If poor cyber security erodes trust and confidence in cyberspace, the potential social and economic benefits of big data may not be realised. In addition to the risk of privacy breaches, cyber risk also poses a physical threat. The convergence of the digital and physical worlds via increased connectivity of the "Internet of Things" devices makes it increasingly possible for cyber attackers to digitally originate cyber attacks against physical assets causing harm to people, loss of life as well as large economic losses. With the trends of cloud computing, mobile workforce and off-shoring of business processes, we have seen a dramatic shift in the way information is stored, where it can be accessed, and by whom. It is now much easier and cost effective to store information in shared data centres (i.e. Cloud Computing). These data centres are likely to be in other jurisdictions (e.g. USA, UK, China, Singapore, India) that have their own unique legislative requirements and constraints.

The launch of Australia's Cyber Security Strategy in April 2016 which sets out Strategy sets out a national approach to meeting the challenges of the digital age is a positive step in addressing cyber risk. The strategy recognises that 'much of Australia's digital infrastructure is owned by the private sector, so securing Australia's cyberspace must also be a shared responsibility. It will be important that businesses and the research community work with governments and other stakeholders to improve our cyber defences and create solutions to shared problems'. CERT Australia is the main point of contact for cybersecurity issues affecting major Australian businesses. It provides major businesses with the best cybersecurity advice and support possible, as soon as possible. The Strategy will increase the capacity of CERT Australia to work with Australian businesses.

IAG considers there are four key areas of focus for organisations to effectively manage cyber risk:

i) Preventative measures

The National Institute of Standards and Technology and Cyber security Framework (NIST) is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cyber security risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cyber security management communications among both internal and external organizational stakeholders (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.).

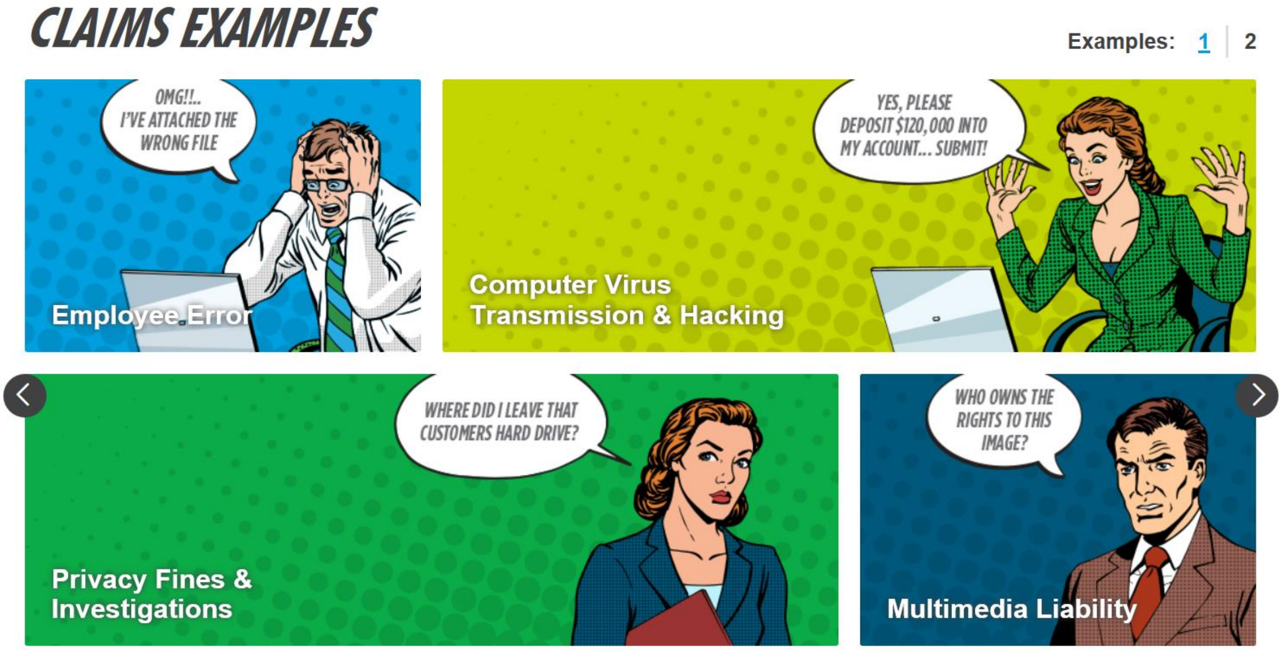
ii) Mitigation of cyber risk events

An organisation’s resistance to cyber threats derives not only from measures taken to resist attacks but also from the steps taken following an incident to mitigate the financial exposure to itself and parties affected by any lost data. Regardless of the preventative methods taken, no company can eradicate the risk of cyber threats entirely. A company’s remedial action taken (through forensic investigations) to identify and correct the breach and the protection of affected customers though a dedicated response team and identity theft monitoring services.

iii) Cyber risk insurance

The global capacity for the Cyber Insurance market is still growing. As such, there are very few underwriters that are capable of underwriting policies with liability coverage for larger enterprises. Most General Insurers are currently capping liability at $5-$10USD Million (focussing on SMB market opportunities). Actuarial data to develop insurance products is limited. Most insurers are heavily relying on a small set of data from providers such as Cyber Security Solution Vendors and a small pool of research organisations (often sponsored by security vendors – for example Ponemon Institute research into costs of Privacy Breach was sponsored by IBM). The quality and availability of information about the impact and frequency of cyber breaches is an on-going challenge. There is still a general unwillingness of affected parties to disclose information about financial losses and recovery costs after a cyber incident.

With cybercrime one of the leading risks for businesses in Australia, CGU has launched a new Cyber Defence product to protect against attacks that damage and undermine businesses. Developed for both SME’s and mid-market customers, CGU Cyber Defence helps to protect businesses from cyber incidents such as privacy breach, system damage, extortion, computer virus, crime and hacking. CGU’s Cyber Defence product includes a wide range of features including free cyber consultation to assess risk mitigation strategies, 24/7 incident response team, advancement of defence costs and a breach coach who can help businesses understand what they need to do to minimise their risk and protect their businesses.


CLAIMS EXAMPLES
Examples: 1 2
OMG!!.. I'VE ATTACHED THE WRONG FILE
Employee Error
YES, PLEASE DEPOSIT $120,000 INTO MY ACCOUNT... SUBMIT!
Computer Virus Transmission & Hacking
WHERE DID I LEAVE THAT CUSTOMERS HARD DRIVE?
Privacy Fines & Investigations
WHO OWNS THE RIGHTS TO THIS IMAGE?
Multimedia Liability

http://www.cgu.com.au/insurance/cyber

iv) Build cyber resilience through cross sector and cross border collaboration

Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to operate during, and to adapt and recover, from such an event. Enterprises operate in a global environment, often with conflicting or competing international data protection legislative requirements and constraints. The global connection of things, people and data underscores the importance of international frameworks to the development of any national regulatory arrangements. Participation in international standards making bodies can develop a more certain operating environment. Another aspect of national and global harmonisation relies on the sharing knowledge and experience with and between other regulators, law enforcement and industry groups to build cooperative mechanisms and identify best-practice approaches that may include non-regulatory as well as regulatory responses.

IAG and cybersecurity

IAG's Chief Information Security Officer (CISO) is an active participant in high-profile think tanks on Cyber Security. One is known as the CISO Lens - a forum for the Chief Information Security Officers (CISOs) of Australian private sector organisations. The purpose of CISO Lens is to empower and enable CISOs and, thereby, support the cyber resilience of the Australian private sector by ensuring that better practices are shared between leading CISOs. A key driver for the creation of CISO Lens was the recognition that information security is an issue for all organisations, and an area that can be most effectively addressed through collaboration. The other is sponsored by Stone & Chalk to encourage general collaboration as well as growth in the Cyber Security start up industry. We have also joined a number of forums related to sharing of security intelligence including CERT Australia, ASIO's Business Liaison Unit and similar groups in NZ. IAG has recently joined the Financial Services Information Sharing and Analysis Center (FS – ISAC) - the only industry forum for collaboration on critical security threats facing the global financial services sector. When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the Financial Services Information Sharing and Analysis Center (FS-ISAC) worldwide receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats.

Case study: autonomous vehicles

Autonomous vehicles

Driverless car technology provides an example that clearly illustrates the numerous challenges surrounding data access, ownership and protection outlined in this submission. The advent of autonomous vehicles provides policy makers within an opportunity to put in place best practice data sharing measures *before* the data is collected, and without being encumbered by legacy data investment considerations.

Public interest benefit

Advocates predict that autonomous vehicles will provide significant user convenience, safety, congestion reductions, fuel savings, and pollution reduction benefits. IAG considers it important for Australia's economic future to ensure the regulatory settings are right to harness the fiscal, road safety and environmental benefits of this technology. Australia has the professional, technical and trades orientated skill base, large geographical area for testing, the technological capability and much of the ITC infrastructure in place to leverage this as an alternative source of income generation.

Private and public sector data sharing

New vehicles have increasing capability to record, store and send data back data to the manufacturer which can allow ongoing updates on the health status of the car system, and also on the usage profile and driving behaviour of the owner/driver. The nature of connected cars and the interdependency that is at the heart of their operation means that data is required to be passed on to a range of other parties to create significant potential revenue streams and manufacturer and customer benefits. More information about the use and operation of vehicles can improve customer satisfaction; allow for predictive maintenance; enable more personalised insurance products; make more effective use of road space and improve safety.

The significant historical investment to collect, collate, store, format, present and analyse the data associated with existing private data sets will not be as great a concern for newly generated data from emerging technologies such as autonomous vehicles.

Access to in-vehicle data will assist with protecting consumers, vehicle owners, road users and more broadly the community. This should involve collaboration between all stakeholders including enforcement authorities, manufacturers, government and insurers. For example, European Union has mandated that all auto makers implement emergency calling technology (eCall) in new cars by 2018. When there is a collision or other incident, an eCall device in each car will automatically alert authorities and send data about the impact.

For insurance companies to make a fair assessment of risk and provide competitive insurance products, insurers will need:

a. Accident information

If an automated vehicle does have a crash it is very important that the insurance industry (and other stakeholders including the police) are aware of who is liable. Ready access to crash information is critical to apportion liability and to make the claims process as efficient as possible for consumers. This should be made available to key stakeholders in an agreed format, and in an efficient, low cost manner.

b. Safety related test data

Data in general is essential for insurers to understand the risks they underwrite. It is even more important when dealing with new risks, for which there is no, or little, historical data. Access to in-vehicle data is therefore essential if insurers are to carry on providing the protection required for users of connected and highly automated vehicles as well as, in the near future, users of fully autonomous vehicles.

c. Repair and diagnostic data

Case study: autonomous vehicles

With sophisticated electronics controlling vehicle behaviour, integrated with active and passive safety systems and an increasing emphasis on emission control systems, accurate technical and diagnostic information will become increasingly critical to vehicle parts manufacturing, service and repairs. Effective flow of the data produced by vehicles will be critical to maintain fair and open competition in the automative industry and its supply chain.

At an international level, insurers have compiled a list of data that is considered essential in order to address liability and insurance issues:

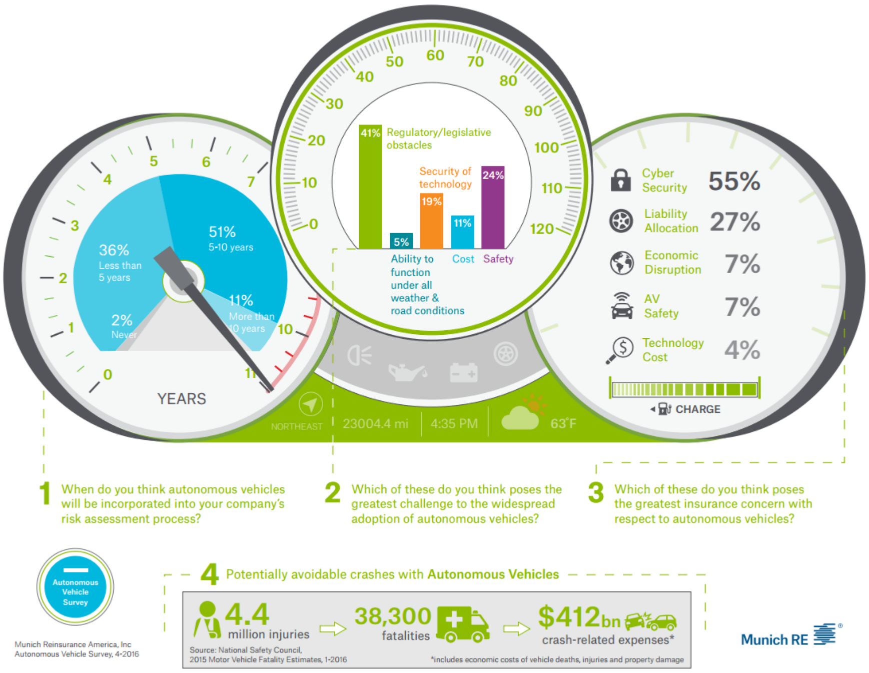
2. GPS-time
3. GPS-Location
4. ACSF Status
5. Automotive Corrective Steering Function Mode e.g. Parking or Driving
6. Automotive Corrective Steering Function Transition time stamp
7. Record of Driver Take over
8. Driver Seat Occupancy
9. Driver Belt Latch

Privacy

Connected vehicles will bring significant new legal responsibilities for vehicle manufacturers, distributors, providers of connected services, and software providers. Every organisation in the chain needs a clear understanding that the handling of personal data raises legal issues such as: who owns the data; who is entitled to access and use it; what are the terms for sharing it; what security measures need to be adopted to keep it safe?

Cybersecurity

The growing importance of network-based information and other connected services in transport obviously poses increased cyber-security risks, especially when networked-based systems interact directly or indirectly with primary control systems of vehicles. Reinsurer Munich Re found that 55 percent of corporate risk managers surveyed named cybersecurity as their top concern about self-driving cars. Cybersecurity included the potential hacking of an automated car's data systems as well as the failure of smart road infrastructure.



https://www.munichre.com/us/property-casualty/business-solutions/innovation/solutions/mobility/autonomous-vehicles/index.html

About IAG

IAG is a general insurance company whose purpose is to help make your world a safer place, whether you are a customer, partner, employee, shareholder or part of the communities IAG serves across Australia, New Zealand and Asia.

Our businesses have helped people recover from natural disasters, accidents and loss since 1851. We employ more than 15,000 people in our operations in Australia, New Zealand, Thailand and Vietnam, providing insurance under many leading brands, including NRMA Insurance, CGU, SGIO, SGIC, Swann, WFI and Lumley Insurance (Australia); NZI, State, AMI and Lumley Insurance (New Zealand); Safety and NZI (Thailand); and AAA Assurance (Vietnam). We also have interests in general insurance joint ventures in Malaysia, India and China.

Last year, we insured $2,012 billion worth of assets on behalf of millions of customers, and we paid $8,736m million in claims.

Increasingly, we see our role extending beyond paying claims to increasing awareness of risk, and helping communities reduce and prevent risk. We believe it is our responsibility as an industry leader to use our influence and role as a major investor, purchaser and employer for the good of everyone.

For further information please visit www.iag.com.au.