

# THE ALLENS HUB

## FOR TECHNOLOGY, LAW & INNOVATION

A joint initiative of

Allens > < Linklaters



UNSW  
SYDNEY



# World Legal Summit

*Informed Development for a Globally Sustainable Future*



Allens > < Linklaters

## **Event**

As part of the [World Legal Summit](#) 2019, an event was held on 1 August 2019 at Allens Sydney, co-sponsored by the Allens Hub for Technology, Law and Innovation, Allens, The Law Society of New South Wales, FLIP Stream, and UNSW Law. The goal was to bring multiple jurisdictions together in order to better understand and compare important issues in technology governance worldwide. It involved three panels on topics selected by the World Legal Summit (and taking place at multiple [locations](#) around the world) and a fourth panel on a topic of local interest. Details of these panels and invited panellists are below.

This document is a summary of some of the discussions at the Sydney event. Its headings are based on a template used to collate material internationally in order to provide a comparative evidence base.

## **Panels**

Panel One: Identity and Governance – Regulation of the construction and use of digital identities, including blockchain

- Dr Anton Didenko – Research Fellow, UNSW Faculty of Law
- Stephen Wilson – Managing Director, Lockstep Group
- Dr Katharine Kemp – Senior Lecturer, UNSW Faculty of Law
- Michael Morris – Partner at Allens

Panel Two: Autonomous Machines – Autonomous Transportation, changing rules for self-driving cars

- Dr Monika Zalnieriute – Research Fellow, Allens Hub for Technology Law and Innovation
- Evan Walker – Director, Smart Innovation Centre, Transport for NSW
- Nicole McDonald – Senior Policy Analyst, The National Transport Commission

Panel Three: Cyber Security and Personal Data – Legal frameworks to enhance cyber security and protect personal information

- Rachael Falk – CEO, Cyber Security Cooperative Research Centre
- Valeska Bloch – Allens Partner
- Paul Domoney – Head of Blackberry Services
- James Turner – Managing Director, CISO Lens

Panel Four: Regulation for AI Applications in the legal profession

- Thomas Chuang – Legal Product Expert, Luminance
- Dr Huon Curtis – Senior Research Analyst, University of Sydney Business School
- Dr Finnian Lattimore – Data Scientist, The Gradient Institute
- John McKenzie – Legal Services Commissioner, Office of the Legal Services Commissioner
- Felicity Bell – FLIP Stream Research fellow

## Highlights

- We are currently stuck in an echo chamber, and it is important to step back and identify the issue and pinpoint the problem that we are trying to solve – *Rachael Falk*
- Digital identity is a metaphor for a relationship that you have with a business or a service provider. Each one of these relationships has their own risk profile – *Stephen Wilson*
- We are trying to fit modern life and modern concerns into a Privacy Act that wasn't designed to deal with it today's digital environment. That's just a function of the fact that legislation will often struggle to keep pace with technological change and perhaps evolving societal norms in response to that change – *Michael Morris*
- One issue that is not spoken about as much is liability. First, questions of liability of governance structures in blockchain platforms are largely ignored. Second, liability of software developers is routinely disclaimed or otherwise avoided – *Anton Didenko*

Regulators need to address the acute information asymmetries and gross imbalances in bargaining power between digital platforms and consumers – *Katharine Kemp*

- Algorithms can't solve everything. There are some very simple problems like the "Halting Problem" in Computer Science for which we know there are no algorithmic solutions. The idea that a robot car can drive itself through any cityscape is incredibly optimistic. – *Stephen Wilson*

**Panel One: Identity and Governance – Regulation of the construction and use of digital identities, including blockchain**



**Top three proposed or recently enacted bodies of legislation. 1) list full title 2) list the main bodies involved by their full name - can include: government units, organizations, lobby groups, etc. 3) links to more information about each one.**

- [Privacy Act 1988 \(Cth\)](#)
- [Regulation \(EU\) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data \('GDPR'\) \[2016\] OJ L 119/1, 1 - 88](#)
  - The GDPR is the regulation in the European Union on data protection and privacy for all individual citizens in the EU and affects businesses trading into the EU.
  - This law came into effect in 2016
  - Impact on Australian entities is significant.
- [Australian Competition Consumer Commissioner, Digital Platforms Inquiry Preliminary Report \(December 2018\)](#)
  - In 2017 the Australian Competition Consumer Commissioner ('ACCC') commenced an inquiry into the impact of digital platforms have on competition in media and advertisers and the implications for consumers.
  - The 23 recommendations in this report address the impact of market power of these platforms, in respect of media, advertising, consumer protection and privacy
  - The ACCC released a preliminary report on 10 December 2018

- The final report was made public on 26 July 2019
- [Australian Prudential Regulation Authority, Prudential Standard CPS 234 \('CPS 234'\) \(July 2019\)](#)
  - Australian Prudential Regulation Authority ('APRA') came into effect 1 July 2019
  - This Standard applies to all APRA regulated entities and is aimed at combating the threat of cyber attacks
- [My Health Record Act 2012 \(Cth\)](#)
- Commonwealth Government has proposed amendments to the [Privacy Act 1988 \(Cth\)](#) to include a Social Media Code of Conduct
- [Digital Identity Framework](#) of Digital Transformation Agency.

**What are the key elements of these bodies of legislation/regulations that your panelists believe to be the most promising? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful.**

- The expansive scope of GDPR enables information such as biometric data, locational data and volunteered statistical data to be protected sources of personal information – *Monika Zalneriute*
- CPS 234 sets out fairly prescriptive requirements for APRA regulated entities around information security. This reflects the proactive approach taken by regulators to the intersection of technological development and cybersecurity threats
- The Commonwealth Government had previously stated a desire for greater privacy regulation following even prior to the ACCC's recent scrutiny of social media platforms – Michael Morris
  - The Commonwealth Government had proposed to increase penalties from \$2.1 million to the greater of \$10 million, three times the value of any benefit that was gained by the company through misusing the personal information, or 10 per cent of a company's annual domestic turnover, and to grant the Office of Australian Information Commissioner ('OAIC') new powers to issue infringement notices for failure to cooperate with efforts to resolve minor breaches. – Michael Morris
- ACCC Final Report on the [Digital Platforms Inquiry 2019](#) includes 23 recommendations for the regulation of digital platforms, including major changes to Australia's privacy and consumer protection laws – *Katharine Kemp*
- Australian Privacy Principle 3 of the [Privacy Act 1988 \(Cth\)](#) prohibits the collection of personal information unless such information is "reasonably necessary" for (or, in the case of agencies, also directly related to) one or more of the entity's functions or activities – *Anton Didenko*

**What are the major gaps in these frameworks? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful.**

- There appears to be a growing consensus among Australian policy makers and regulators that Australia’s current privacy regulation is lagging behind the rest of the world – *Michael Morris*
  - o There is no specific law in Australia which regulates digital identity. Rather, the *Privacy Act 1988* (Cth) continues to be the main source of regulation despite probably not contemplating the issues surrounding the widespread use of digital identities when it was drafted – *Michael Morris*
    - As a result, personal data is only protected at a base level at law.
    - Unlike countries such as Estonia and Switzerland, Australia doesn’t have the “legislative appetite” to create a national digital identity legislative regime – *Stephen Wilson*
  - o The *Privacy Act* does not currently prevent companies from exploiting information asymmetries and imbalances in bargaining power in their dealings with consumers regarding data practices – *Katharine Kemp*
    - Consumers are generally unaware of the existing data ecosystem – the companies that “pervasively track” and profile consumers for profit – *Katharine Kemp*
    - Consumers do not currently have real choices about the data practices of the firms that collect and disclose their personal information – *Katharine Kemp*
  - o Organisations now need to comply with an increasingly complex web of data breach notification regimes, both within their own jurisdictions and globally. This causes practical difficulties because when it comes to data breach notification, the different notification thresholds, timeframes and recipients means that it will not always make sense (practically) to take a 'high watermark' approach – *Valeska Bloch*
  - o The GDPR does not allow organisations enough time to determine precisely what has happened in the event of a data breach, or the extent of the impact, before having to notify. In the PageUp example, this meant that it also notified its customers before having enough information to allow them to determine the most appropriate steps that they should be taking to minimise any harm in the circumstances. The Australian NDB scheme allows a more sensible timeframe for notification.
  - o Generally speaking, *CPS 234* is fairly prescriptive as to the information security capabilities that APRA regulated entities need to have. However the requirement that their capabilities, systems and processes are commensurate or proportionate to the threats faced by these entities means that undertaking a risk assessment is a critical first step – one that is implied but not expressly provided for in the Standard – *Valeska Bloch*
- Although Australia has data localisation restrictions, they are narrow and sector-specific. For example, s 77 of the [My Health Record Act 2012 \(Cth\)](#) prohibits holding and taking “outside Australia” records relating to the My Health Record system – *Anton Didenko*
- The GDPR ‘right to be forgotten’ does raise some issues for Australia's proposed use of data in the context of autonomous vehicles. Specifically, information may need to be retained to provide better support and services for such technology, and yet it is not clearly defined as to what could make this permissible in a legislative sense – *Monika Zalnieruite*

- A new regulatory regime under existing legislation is needed, consistent with the ACCC's recommendations from the [DPI report](#).

**What kind of feedback has it received in the public domain? Are there any major controversies around it? \*\*Please provide as much detail as possible, links to articles with major headlines are very helpful.**

- Digital identity strategists love to create new “trust frameworks” but in my view, we already have plenty of rule sets for dealing with people and their credentials in the real world. New frameworks are difficult to develop and establish. So I believe the best way to treat identity data is to use the regulatory regimes that we already have, such as the *Privacy Act 1988* and the *forthcoming Consumer Data Right – Stephen Wilson*
- ACCC DPI recommendations have been [“applauded by industry figures”](#)
  - o The ACCC’s recommendations to increase pecuniary penalties under the *Privacy Act* and to impose new pecuniary penalties for unfair contract terms would have a very broad impact, given that these recommendations are not restricted to digital platforms – *Katharine Kemp*

**Where can it be read about and accessed online, if at all? If not, then where and how is it accessed by those it applies to? (provide as many links here as possible)**

- These proposals can be read in the ACCC [Digital Platforms Inquiry 2019](#)
  - o Some of these proposals include:
    - Updating the definition of personal information under the *Privacy Act 1988* (Cth)
      - The definition needs to cover the new methods used to identify individuals, including IP addresses, location information and credit transactions etc.
    - Increased consent and notification obligations under the Privacy Act
      - Unbundling consents so that the individual can choose between different purposes of the use of information
      - Consent should be freely given.
    - Increased penalties under the Privacy Act to bring into line with the [Australian Consumer Law 2010](#), from a 2.2 million penalty to a maximum penalty of \$10 million, 10% of turnover or three times the benefit gained
    - Privacy respecting default setting
      - Companies are falling back on ‘pre-set’ location tracking and personalised advertising options. These boxes should be unticked (to enhance privacy settings automatically)
    - Pecuniary penalties for unfair contract terms under the ACL.
      - This would create a greater deterrent for companies that currently incorporate prejudicial terms in privacy policies

**What do technologists think about its basic tenets? Has there been pushback or positive reception? (e.g. are the laws understood as practical?)**

- Data held by a centralised entity poses too great a risk – *Anton Didenko*
  - o Some technologists propose blockchain as a decentralised alternative – *Anton Didenko*

- However, storing personal data on a distributed database may be risky (as long as the same information is shared among all nodes) – as a result, new digital ID solutions are reimagining the scope of blockchain implementation (e.g. by moving identity claim verification on blockchain but storing personal data locally) – *Anton Didenko*

**How can technologists and non-legal professionals contribute (if at all) to the transformation of this legislation or body of standards? (e.g. polls, roundtables, online communities?)**

- It is important for the community be moderate in our use of the vague and all-encompassing term ‘personal identity’
  - Identity is more about relationships than who we “really are” online, for that’s far from settled.
    - For example, a credit card number can be considered an “identity” but more precisely, we should view it as a token which symbolises the relationship and agreement that an individual has with a bank – *Stephen Wilson*
- We need to start having roundtable discussions about what type of regulation is needed for digital identity in all its forms, which acknowledges the difference between raw data which clearly identifies and relates to an individual on the one hand, and on the other hand the treatment of value-added and derived data sets which organisations create from that raw data to create insights, products and services that individuals often want and which benefit the broader economy – *Michael Morris*
- As a community we need more discussions about identity. It is important that we identify the issue that we are trying to resolve.
  - It is a complex and multifaceted conversation. – *Rachael Falk*

**Additional Information**

- The notion of ‘self-sovereign identity’ has gained traction as people try to reclaim disparate parts of the data they share – *Anton Didenko*

**Panel Two: Autonomous Machines – Autonomous Transportation – changing rules for self-driving cars**





**Top three proposed or recently enacted bodies of legislation. 1) list full title 2) list the main bodies involved by their full name - can include: government units, organizations, lobby groups, etc. 3) links to more information about each one.**

- Some state governments have passed legislation that allows automatic motor vehicles to be trialled
  - o [Motor Vehicles \(Trials of Automotive Technologies\) Amendment Act 2016 \(SA\).](#)
  - o [Road Safety Amendment \(Automated Vehicles\) Act 2018 \(Vic\).](#)
  - o [Road Transport Act 2013 \(NSW\)](#)
  - o [Transport Legislation Amendment \(Automated Vehicle Trials and Innovation\) Act 2017 \(NSW\) – complete.](#)
- National Transport Commission (‘NTC’) has also published guidelines for trialling of autonomous vehicles in Australia
  - o [NTC Guidelines for Trials of Automated Vehicles in Australia \(May 2017\).](#)
  - o Other reports on safety and privacy issues available [online](#). Recent reports include [Motor Accident Injury Insurance and Automated Vehicles](#) and [Regulating Government Access to C-ITS and Automated Vehicle Data.](#)

**What are the key elements of these bodies of legislation/regulations that your panelists believe to be the most promising? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful.**

- The goals of automated vehicles are ‘road safety, increased productivity, economic sustainability and an integrated customer experience’ – *Evan Walker*
- Australia’s policy approach to automated vehicles has to be made in the context of having a small local vehicle manufacturing and technology industry and Australia being a small global market for vehicle sales. Australia’s policy makers are examining international developments

and regulatory approaches in significant markets like Europe and the United States. – *Nicole McDonald*

**What are the major gaps in these frameworks? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful.**

- This is a complex and emerging body of law with overlaps in negligence, product liability, consumer protection law, insurance law, property damage and contract law – *Evan Walker*
- The NTC identified 716 provisions in state, territory and federal legislation that may act as barriers to deployment (public use) of autonomous vehicles.
  - o This includes provisions in state and territory road safety, traffic laws and commonwealth vehicle design rules.
- Another concern with this legislative framework is that it relates to the human experience and not to machines. As such, the current regulations implicitly assume that there is human control – *Evan Walker*
  - o Therefore, one of the biggest issues is how to change these regulations so it aptly applies in the relevant circumstances to a human and a machine
    - It is likely that we [will need significant legislative reform](#). The policy work to develop reform is underway.
- Another challenge with this emerging area of law is federalism
  - o Currently, there is no specific national law relating to automated vehicles – *Evan Walker*
  - o The Commonwealth is responsible for some parts of transport but states control road vehicle uses. We need to align these roles and establish cooperative federalism
    - A patchwork of legislation in this area is not going to be adequate for industry and consumers – *Evan Walker*
- Within the new sharing economy, there are still hurdles to overcome with regard to customer interaction
  - o For instance, the robo-taxi trials in Las Vegas, has highlighted that even though autonomous vehicles are capable of transporting individuals from hotel to airport, there are still limitations in regards to digitalised customer interface: how do they pay; how to ensure customer identity; and how to determine destination etc – *Evan Walker*
- The GDPR shows promise in that it clearly defines personal information. However, in practice this regime offers little protection for individuals and at the same time leaves loopholes that were prevalent in previous regimes’ – *Monika Zalnierute*

**What kind of feedback has it received in the public domain? Are there any major controversies around it? \*\*Please provide as much detail as possible, links to articles with major headlines are very helpful.**

- This is controversial and in many ways uncomfortable area of law for the public to grapple with, as it involves placing our trust in a machine.

- One issue debated was whether autonomous vehicles are safer than human drivers
  - In 2018, there was around people [400 killed](#) on roads in NSW.
    - If autonomous vehicles are safer than what is on the market at the moment, we should not necessarily concern ourselves with ethical dilemmas – *Evan Walker*
    - However, there are statistical issues when comparing the safety of autonomous vehicles to human operated vehicles because the death rate is actually very low over millions of passenger kilometres. There is not enough statistically significant evidence to show that autonomous vehicles are safer – *Steve Wilson*
  
- There are debates about the ethics of autonomous vehicle decision making
  - This issue was highlighted in (German) Ethics Commission, Automated and Connected Driving (June 2017)
    - *Anton Didenko*
      - This report tackled the tram dilemma (i.e. a scenario where automated vehicles have the capability to choose the victim in an unavoidable accident) and proposed a number of corresponding rules – *Anton Didenko*
  - Some stakeholders advocate that ethics of automated vehicles should be a component that manufacturers must satisfy. However, as of yet, there is no national or international consensus about whether ethical considerations should be integrated into law – *Nicole McDonald*
    - Ethical considerations may be unnecessary as an exercise in the first instance because the clear priority and objective is to ensure that there is adherence to basic first principles of safety and reliability, with most decisions by algorithms not determinative but instead impressionistic, using snapshots of the limited data available in the moment. As such, the ethical scenarios, and a standalone ethical criteria is somewhat inchoate – *Nicole McDonald*
    - Some potential solutions to this ethical dilemma include – *Anton Didenko*
      - Technology designed so the machine does not have to choose between ‘two evils’
      - Programming to prioritise protection of human life over protection of property or animals
      - Programming to prevent distinction of potential victims based on personal features (including age or gender)
      - Programming to prevent injuries to parties not involved in generation of mobility risks
      - General programming to reduce number of injuries
  
- Issue of whether autonomous vehicle tech is proprietary and if so, how can regulators accurately assess it – *Jessica Selby (Managing Associate, Allens)*
  - Currently the focus is on creating a new legal entity - [Automated Driving System Entities \(‘ADSE’\)](#) who will be responsible for the safe operation of automated vehicles. Australia is focusing on converting broad policy principles to law at the moment, rather than proprietary tech at present – *Nicole McDonald*

- There is also issue of how liability will be attributed to drivers, manufacturers or tech companies. Alternatively, it may be attributed to registered 'ADSE' that purport to supply the vehicles to Australia – *Nicole McDonald*
- Australia will have to put more resources toward establishing a tech industry
  - o Currently we do not have the capability to produce the tech in Australia, and we have to make ourselves and our legislative frameworks attractive to manufacturers. – *Evan Walker*

**What do technologists think about its basic tenets? Has there been pushback or positive reception? (e.g. are the laws understood as practical?)**

- Generally, there is a consensus that more work needs to be done to ensure that automated vehicles protects valuable personal data – *Nicole McDonald*
- ADSE is a new legal entity in Australia and we need to put regulation on this group – *Evan Walker*
- The legislative framework is only a starting point. We will also need to establish the digital infrastructure to integrated automated industry in a way that adds value – *Evan Walker*

**Add any additional information that you and your local experts think we should highlight in the global publication:**

- The goal is to create end to end (from the point at which system are imported or manufactured through to operation and end of life of automation of vehicles) system that is a safe system of automation in Australia
- Currently there are five autonomous vehicle trials in NSW which will be observed and monitored.
  - o One such trial is an autonomous shuttle bus in a retirement village in Coffs Harbour, known as [Busbot](#). This service has been crucial in providing transport to those with mobility issues.

○

### Panel Three: Cyber Security and Personal Data – Legal frameworks to enhance cyber security and protect personal information



**Top three proposed or recently enacted bodies of legislation. 1) list full title 2) list the main bodies involved by their full name - can include: government units, organizations, lobby groups, etc. 3) links to more information about each one.**

- In 2018 there was a proliferation of Mandatory Notification Regimes – *Valeska Bloch*
  - These are regimes of transparency and accountability, allowing consumers and individuals’ opportunity to mitigate personally the harms caused by data breaches. The Notifiable Data Breach Scheme is in [Privacy Act Part IIIC](#). There is also an [OAIC guide](#).
  - Some of the ‘transparency oriented regimes’ include:
    - [Australian Competition Consumer Commissioner, Digital Platforms Inquiry Preliminary Report \(December 2018\)](#)
    - [Australian Prudential Regulation Authority, Prudential Standard CPS 234 \(‘CPS 234’\) \(July 2019\)](#)
    - ACCC [Digital Platforms Inquiry 2019](#)

In addition, other relevant laws include

- [Security of Critical Infrastructure Act 2018](#) includes cyber security as a security issue.
- There are cyber crime provisions in Part 10.7 of the [Commonwealth Criminal Code](#).

**What are the key elements of these bodies of legislation/regulations that your panelists believe to be the most promising? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful.**

- We cannot take a ‘one size fits all’ approach to cyber security and personal data. It is also important to not only focus on the protection of *personal* information, but also on the protection of other critical information and systems – *Valeska Bloch*

**What are the major gaps in these frameworks? \*\*Please provide as much detail as possible, links to additional resources (e.g. papers, articles, research), and any information that you think will be helpful**

- Technology in the corporate world is beset by risk. This includes ransomware, which can be an existential threat to companies without proper protocols – *Paul Domoney*
  - o There is also the issue of operational risk where information can be comprised through third party affiliates, or volunteered in an improper fashion - see the “bipolar” My Health Record [scandal](#) – *Paul Domoney*
  - o Liability regimes need to be accessible by individuals. Suggestion that corporations pay \$10 per person affected by data breach in order to provide financial incentive for good cyber security practices – *Rachael Falk*.

**What kind of feedback has it received in the public domain? Are there any major controversies around it? \*\*Please provide as much detail as possible, links to articles with major headlines are very helpful.**

- Cyber security is increasingly being seen as a critical part of corporate governance, with increased emphasis on board and executive level accountability – *Valeska Bloch*

**What do technologists think about its basic tenets? Has there been pushback or positive reception? (e.g. are the laws understood as practical?)**

- Organisations are trying to grapple with the pace of complexity in regulatory change and in many ways this increased volume of regulation has created difficulty for organisations – *Rachel Falk*
  - o For instance, the emphasis on mandatory notification schemes to allow individuals to mitigate personal harm and in data breach scenarios, this mandatory notification schemes this creates overlapping and illogical requirements
  - o There is also an increased number of regulators.
- Being compliant with the regulatory frameworks and being secure are not the same thing – *Paul Domoney*

**How Can Technologists and Non-Legal Professionals Contribute to Transformation of Legislation?**

- Corporations need to improve their technological literacy, focusing on educating individuals within the company to understand and articulate these latent harms – *Rachel Falk*
  - o Companies should ask “what are the risks here” and “what actions do we need to take to address these issues” – *Rachel Falk*
  - o Companies should not be driven by reputational risks but see cyber security as core– *Rachael Falk*
- We must develop dimensional critical thinking and facilitate understanding about technology
  - o Technology is moving fast, and the law is slow to evolve, but society is even slower – *Rachael Falk*

- It is not about meeting the baseline of compliance. We need to actually understand what is actually understood at the baseline level.