

# DirectorTech

Strategy + Risk + Governance



High-level advice on untangling business technology from the Centre for Internet Safety at the University of Canberra.

*Issue 003, April 2018*

# DirectorTech 003

|                                                 |  |    |
|-------------------------------------------------|--|----|
| 003.001                                         |  |    |
| Security leadership is the real skills shortage |  | 3  |
| 003.002                                         |  |    |
| Some thoughts on digital and data ethics        |  | 5  |
| 003.003                                         |  |    |
| Notifiable Data Breaches: What you need to know |  | 11 |
| 003.004                                         |  |    |
| What motivates the whistleblowers?              |  | 14 |
| 003.005                                         |  |    |
| Trusting our food: the blockchain solution      |  | 17 |
| 003.A1                                          |  |    |
| About the Contributors                          |  | 20 |
| 003.A2                                          |  |    |
| About DirectorTech                              |  | 22 |

# 003.001

## Security leadership is the real skills shortage

*Despite the constant messaging about Australia's lack of cybersecurity skills, **Nigel Phair** thinks it's not so much a skills shortage as a leadership shortage.*



Much has been made recently about the lack of cyber security skills in Australia. Indeed, a central part of the Australian government's **Cyber Security Strategy** is a commitment to "address[ing] the shortage of cyber security professionals".

The government will "work in partnership with the private sector and academic institutions to **improve cybersecurity education** at all levels of the education system." It will build on existing science, technology, engineering and mathematics (STEM) related initiatives, and help create what the government has called a "cyber-smart nation".

STEM graduates are important, but cybersecurity is a cross-cutting issue for all organisations. We need people from all academic disciplines to become involved, and use their unique skill sets to address this ongoing problem.

While there's a multitude of jobs being advertised for cybersecurity professionals, there's even more people applying for them, with many missing out.

I don't believe we have a skills shortage. What we have is a leadership shortage.

Australia is blessed with some amazing cybersecurity leaders across government and the private sector. They lead multi-disciplined teams, measure their performance, and provide advice to peers and the broader community.

However, Australia is home to three tiers of government (including over 500 local government bodies). We have more than two million actively trading business, according to the **latest statistics**, consisting of more than 2000 listed companies, and around 600,000 not-for-profits.

These organisations need cybersecurity leadership, but it's largely missing. There isn't enough understanding that cybersecurity isn't a technical problem, but one that requires an all-hazards approach.

## **Leadership starts with the board of directors.**

If the board isn't asking questions in an insightful way — and isn't skilled enough to know what answers to expect — then there's little incentive for an organisation's management to pay due attention.

Management need to realise that cybersecurity is about people and processes, with a limited amount of technology sprinkled in. While many vendors will give a different impression, there is no technical silver bullet.

Leadership requires managers to engage staff with a robust risk-management approach. It needs to incorporate physical security as well as digital, and it needs to including a system for rating the level of risk for each type of transaction undertaken by their organisation.

Once this is done, managers can set targets, and decide the level of controls and budget they'll need to achieve those targets.

Cybersecurity needs to be seen as a normal cost of doing business, just like salaries, office rental, and travel.

Too many organisations do things in isolation. They buy a new firewall without considering other network vulnerabilities. They encrypt their storage devices without looking at other data management issues. Or they invest in penetration tests without implementing their recommendations.

Organisations need to train staff not to fall prey to phishing attacks, stop holding personally identifying information any longer than necessary, and audit third-party suppliers and other outsourced arrangements. Most fundamental of all, they must back up their data, and develop and test a disaster recovery program.

A solid cybersecurity governance approach will foster cybersecurity leadership, both within an organisation and through the sector in which it operates. It will allow them to decide whether they want to be the gold standard in cybersecurity, or perhaps only the silver or bronze standard, based on the identification, measurement, and management of the risks they face.



# 003.002

## Some thoughts on digital and data ethics

*A smorgasbord of issues to think about when your organisation starts deploying big data based systems, from **Kate Carruthers**.*



*"We ask ethical questions whenever we think about how we should act. Being ethical is a part of what defines us as human beings."*

— The Ethics Centre, Sydney

Humans have been thinking about the moral principles that govern our behaviour or the way in which we conduct ourselves for aeons. We are moving at lightspeed towards a new and exciting future that is built on algorithms, data, and digital technologies. Ethics is an area of increasing importance since we are barrelling forward with the proliferation of data through digital and IoT, and there seems to be little opportunity to slow things down.

I've been thinking about digital and data ethics since I joined Steve Wilson, David Bray, John Taschek, and R "Ray" Wang on a x in 2016.



## 5 propositions about data

- **Data is not neutral.** All data is subject to bias.
- **There is no such thing as raw data.** Even the simple mechanism of selecting data, means you've exercised judgment as to which data to include or exclude.
- **The signal to noise ratio has changed.** We now have so much data that there is more noise than signal, and it gets difficult to ascertain which of it is the signal.
- **Data is not inherently smart.** Our interpretation of data is what adds value.
- **The more data we have, the less anonymity.** It's becomes increasingly difficult to avoid identification.

## Why this is important

There have been numerous examples of data breaches. The **Australian Red Cross** and the **nation of Sweden** are just two recent examples.

To understand the scale and scope of data breaches globally, it's worth spending a few minutes in the visualisation tool **World's Biggest Data Breaches**.

Every data breach is the result of some defect in the design, development, or deployment of the technology. These breaches could be prevented by including some ethical frameworks into the design, build, and deployment phases.

It is interesting to recall the ease with which Microsoft's artificial intelligence (AI) based Twitter chatbot Tay was trained to become very nasty very quickly. **Twitter users taught Tay to be a racist asshole in less than a day.**



Anyone deploying an artificial intelligence system needs to understand the training data they're using, and ponder the potential consequences of design and deployment decisions.

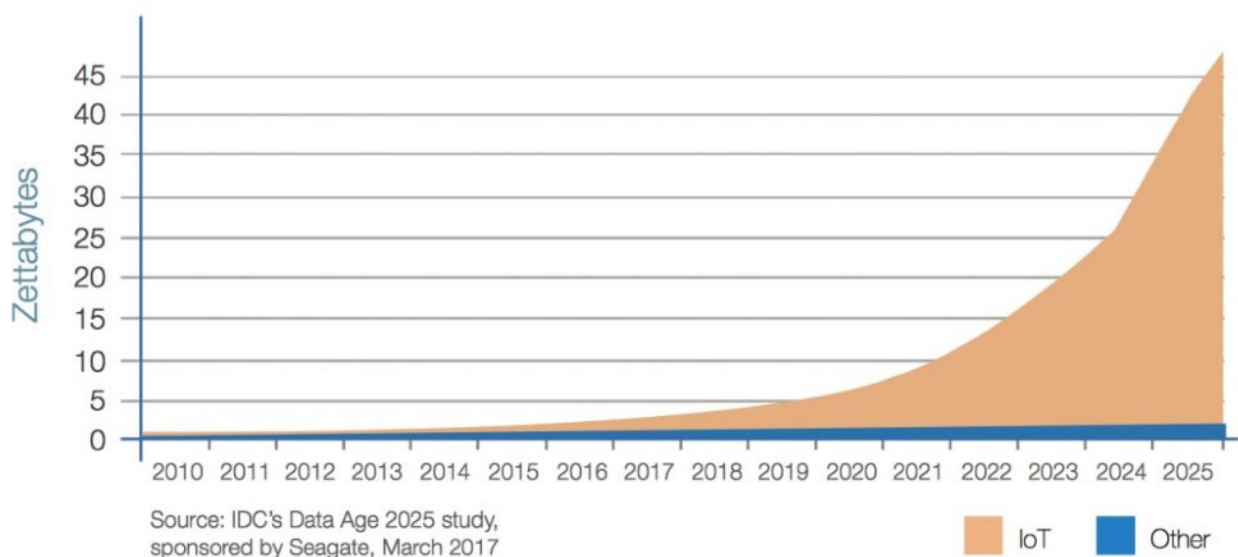
Then there was the recent example of **bathroom soap dispensers (video)** being designed to recognise white hands but not coloured ones.



This is obvious bias from the design and development team, and an example of why diversity in teams is critical. The average software developer is a white male, which means that it's likely that every design has default settings reflecting white male biases.

The issues of bias — both unconscious and conscious — are enormous.

The ocean of data is increasing at a vast rate, as shown by this chart from the **IDC Data Age 2025 study**. This means that we need to develop ethical frameworks to support the acquisition, management and analysis of large datasets.



## Some existing approaches

Universities have a long history of managing ethics, but even they are struggling with the implications of the complex data sets and algorithms they're dealing with.

Over the years, the ICT industry has developed a number of codes of ethics, and codes for professional practice, yet many developers and data scientists are unaware of them.

Some examples of these codes of practice include:

- **IEEE CS/ACM Code of Ethics & Professional Practice**
- **ACM Code of Ethics**

But realistically, if developers haven't even heard of these codes, how can they possibly influence the design of solutions that avoid bias and other ethical issues?

## Some newer approaches

*"Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."*

— **Bruce Schneier**

The beginnings of new approaches are starting to emerge, such as the **Accenture: 12 guidelines for developing data ethics codes**. Recent initiatives such as the **OWASP Security by Design Principles** and **Privacy by Design** might well provide a good starting point for thinking about how we can embed good practice into the design and building of data sets and algorithms.

There is some good discussion of these issues in Luciano Floridi and Mariarosaria Taddeo's **What is Data Ethics?** (2016). As they note, we need to examine ethics in terms of these three categories:

- **Data**, including how we generate, record, and share data, including issues of consent and unintended uses of the data;
- **Algorithms**, or how we interpret data via artificial intelligence, machine learning and robots; and
- **Practices**, devising responsible innovation and professional codes to guide this emerging science.

There have been developments in the area of community based approaches to improving digital and data ethics, chiefly in the area of machine learning and AI.

Some of the groups working in this area:

- **IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems**
- **Fairness, Accountability, and Transparency in Machine Learning**
- **Algorithmic Justice League**

## Some new ways to think about digital and data ethics

*“Complexity is a defining feature of the digital era, and we are not adjusting our governance structures to manage it.”*

— **Kent Aitken**, Prime Minister’s Fellow, Public Policy Forum Canada, 2017

We need to be clear that technology has no ethics. It is people who demonstrate ethics. And technology inherits the biases of its makers. We need to develop ethical frameworks and governance practices that enable us to develop solutions that are better from an ethical perspective.

I believe that if we start from the principles of Privacy by Design and Security by Design, then we have a reasonably firm practical basis for the future.

One thing is certain, at an institutional level, information security, privacy, and data governance will need more work to form a solid foundation to enable better data ethics.

## References

- **Causeit Data Ethics**
- **Digital Ethics Lab - Oxford Internet Institute - University of Oxford**
- **Georgetown University, Kennedy Institute of Ethics, Ethics Lab**
- **The BIG Data Ethics Cheat Sheet**, Hackermoon
- **Guidelines on Ethical Research - British Sociological Association**
- What is data ethics? Luciano Floridi, Mariarosaria Taddeo. **Phil. Trans. R. Soc. A** 2016 374 20160360; DOI: 10.1098/rsta.2016.0360. Published 14 November 2016
- Digital Enlightenment Forum: Digital Ethics. Workshop Report. (2016, March 1). Retrieved August 16, 2017, from <https://digitalenlightenment.org/sites/default/files/users/14/Digital%20Ethics%20Workshop%20Report%20v2.pdf>
- A deep study on the concept of digital ethics. Maggiolini, Piercarlo. (2014). Revista de Administração de Empresas, 54(5), 585-591. <https://dx.doi.org/10.1590/S0034-759020140511>

- Digital Ethics. Capurro, R. (2009, December 1). Retrieved August 18, 2017, from <http://www.capurro.de/korea.html>
- The Eternal Value of Privacy. Schneier, B. (2006, May 18). Retrieved August 18, 2017, from [https://www.schneier.com/essays/archives/2006/05/the\\_eternal\\_value\\_of.html](https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html)
- Governance in the digital age. Aitken, K. (2017, May 23). Public Policy Forum. Retrieved August 18, 2017, from <https://medium.com/@PPForum/governance-in-the-digital-age-a7edce03637d>

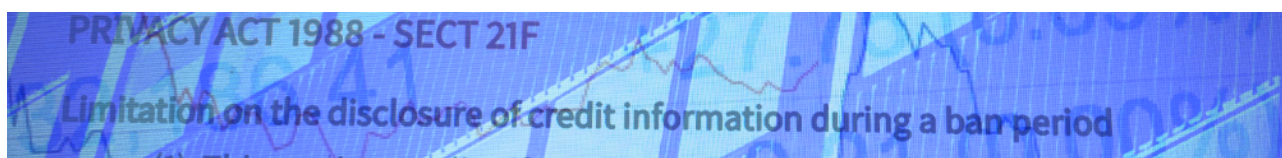


# 003.003

## Notifiable Data Breaches: What you need to know

Australia's mandatory data breach notification obligations came into force on 23 February 2018. Your organisation may no longer have the option to conceal serious cybersecurity breaches.

**Timothy Webb** and **Sumer Dayal** from Clayton Utz explain what you need to know.



As 2017 in particular demonstrated, even high-profile companies like **Equifax**, **Uber** and **Verizon** are vulnerable to serious incidents that can compromise personal information on a large scale.

Understanding the new Notifiable Data Breaches (**NDB**) Scheme and creating a response framework should therefore be a key consideration for 2018 to avoid serious reputational risks and civil penalties.

### Origins of the NDB Scheme

The scheme came into force through amendments to the **Privacy Act 1988 (Cth)** (**Privacy Act**) by the **Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)** (**Amendments**).

### Who does it apply to?

The NDB Scheme applies to agencies and organisations that are required to take steps to secure certain categories of personal information under the Privacy Act. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of \$3 million or more, credit reporting bodies, and health service providers.

### When do the notification obligations arise?

Where there are reasonable grounds to **believe** that an “eligible data breach” has occurred — exceptions to this are discussed below — or an organisation is directed to do so by the Office of the Australian Information Commissioner (**OAIC**).

An **eligible data breach** is one where a reasonable person would conclude that there is a likely risk of serious harm to the individuals to whom the information relates as a result of

the unauthorised access or disclosure. This covers both intentional and unintentional acts, from a malicious hacker penetrating the organisation's network to an employee inadvertently leaving an unsecured laptop on public transport.

However, an eligible data breach does not include circumstances where:

- the organisation has taken remedial action before any serious harm occurred. The action must be such that a reasonable person would conclude that the access or disclosure of information would not likely result in serious harm to affected individuals; and
- an organisation only has reasonable grounds to **suspect** that an eligible data breach has occurred. Organisations will be required to complete a "reasonable and expeditious" assessment into the relevant circumstances within 30 days, ensuring that wilful ignorance will not avoid the requirements of the Privacy Act.

Organisations must promptly notify the OAIC and any potentially affected individuals of the eligible data breach. This involves:

- preparing and providing a statement to the OAIC containing information prescribed by the Amendments about the data breach (including recommendations that individuals should take in response); and
- taking steps to notify affected individuals of the contents of the statement. This may involve sending the statement to the individual via normal means of communication or, if this is not practicable, publishing the statement on the organisation's website.

## When is there "serious harm"?

**Serious harm**, while undefined, is likely to include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation. Serious harm will be "likely" if such harm is "more probable than not" having regard to relevant matters including:

- the kind of information;
- the sensitivity of the information;
- whether the information is protected by security measures (such as encryption) and how easily those security measures could be overcome; and
- the nature of the harm.

## Exceptions

Organisations may be exempt from the notification obligations in the following circumstances:

- the requirements to issue statements or contact individuals regarding eligible data breaches will not attach to eligible data breaches of other entities;
- if the CEO of an enforcement body believes that compliance would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, the enforcement body;
- where notification would be inconsistent with secrecy laws that prohibit or regulate the use or disclosure of information (to the extent of that inconsistency); and
- where the Commissioner makes a declaration that some or all of the obligations do not apply.

## What should you do next?

To ensure compliance, organisations should:

- review the OAIC's **comprehensive guide** to complying with the NDB scheme now available on its website;
- audit their current information security processes and procedures to ensure they are adequate; and
- prepare a data breach response plan (or update the current plan) to enable organisations to respond quickly, efficiently and lawfully to an actual or suspected data breach.

Compliance with these new laws will be much easier for organisations that are prepared for data breaches and have the ability to detect and take action before any serious harm occurs.

Organisations would be wise to have in place detailed policies and procedures which outline the steps to be taken in response to a serious data breach, regardless of whether that breach has occurred inadvertently by the organisation or following a coordinated attack by hackers.

After all, prevention is better than a cure.



# 003.004

## What motivates the whistleblowers?

New laws currently before the Senate look set to increase protections for whistleblowers, and extend them to the private sector. Amendments are due to be released on 1 July 2018. **Andrew McLeish** explains what motivates whistleblowers, and what the changes will mean.



When it comes to reporting misconduct, Australia has seen cultural shift. In the past it was commonly referred to as “dobbing”, or telling on someone. But as the number of news reports shows, people have changed their view.

Employees don’t like to see or hear others being dishonest, or treating team members badly.

As attitudes have changed, so has the law. That means organisations need to change too.

When the first whistleblower legislation was introduced in 2001, the Whistleblower Protection Act 2001 (Vic), the aim of the Act was to afford a person the ultimate protection against reprisal by giving that person anonymity.

There were limitations, however, and in early 2013 this legislation was updated with the introduction of the Protected Disclosure Act 2012 (Vic). This new legislation broadened the scope of the original Act, and made significant changes to the management of disclosures. Public bodies now needed a framework to handle reportable offences under that Act, including fraud and misconduct, and that signified more accountability.

Between 2001 and 2012, the awareness of fraud and corruption in the public and private sector rose rapidly.

In 2016, the Association of Certified Fraud Examiners (ACFE) surveyed companies from across the world to identify the cost of fraud. The resulting report, **“Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Survey”**, identified several key ways in which fraud was identified, including whistleblowing.

*“In cases detected by tip at organisations with formal fraud reporting mechanisms, telephone hotlines were the most commonly used method (39.5%). However, tips submitted via email (34.1%) and web-based or online form (23.5%) combined to make reporting more common through the internet than by telephone.”*

It's hardly surprising that many public and private organisations, including not-for-profit businesses, are now starting to implement formal reporting processes, such as an integrity line, or whistleblower hotline.

So what are the motivators for reporting fraud in the work place?

The real reason lies within the individual and their beliefs. There are many examples of individuals who report workplace incidents or misconduct not for the recognition, but because they're fed up with others doing the wrong thing. Having said that, many people don't come forward because they fear reprisal from their employers and from their colleagues.

A **recent study** (PDF) by the Transnational Research Institute on Corruption at the Australian National University found that in Victoria, the general public has a strong feeling that corruption is increasing, but roughly half of them don't know where to report it.

So how do we change people's perception of reporting workplace misconduct? How do we protect the whistleblower?

The latest legislation is the **Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2017**, currently before the Senate. It proposes significant changes in the protection of whistleblowers and the reporting of misconduct. The most significant alteration will be to cover the private sector, and ensure consistency by bringing all private sector legislation into a single Act.

**FIX: This new legislation has been tabled for release on or about the 1 March 2018, and the complete list of recommendations has not been confirmed at the time of writing this article.**

Having said that, here is a list of some of the recommendations put forward by companies and individuals:

- Broaden the private sector definition of disclosable conduct to a breach of any Commonwealth, state or territory law;
- Provide protections for both former and current staff that could make a disclosure, or are suspected of making a disclosure;
- Provide appropriate protection for recipients of disclosure and those required to take action in relation to disclosures;
- Adopt a tiered approach comprising:
  - (i) internal disclosure;
  - (ii) regulatory disclosure; and
  - (iii) external disclosure (in appropriate circumstances);

- Protect internal disclosure in the private sector, including in registered organisations;
- Align thresholds for protection across the public and private sectors;
- Allow for anonymous disclosure across the public and private sectors;
- Protect the confidentiality of the disclosures and the whistleblower's identity;
- An appropriate body to set and promote standards for internal disclosure procedures in the private sector;
- Align the public and private sector with the protections, remedies and sanctions for reprisals in the Fair Work Registered Organisations Act 2009.

## Next Steps

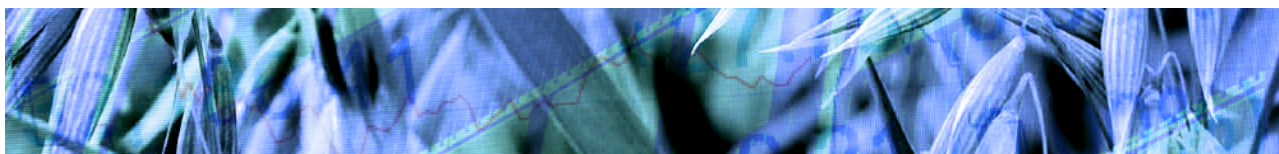
Make sure your company aligns itself with the impending changes to the new legislation:

- Ensure your policies and procedures are up to date and are aligned with the changes in the legislation;
- Ensure that your employees and other stakeholders are aware of the whistleblower service and how matters can be reported — internal awareness training and promotional material;
- Ensure you have adequate protection for anonymity — these may include data protection policies or document management systems to align with the new legislation;
- Have your policies and procedures reviewed — in some cases it is worthwhile having these documents reviewed by legal counsel.



## Trusting our food: the blockchain solution

Agricultural supply chains are complex networks that span the globe, yet in Australia agriculture is one of the least digitised industries. **Emma Weston** looks at the challenges, and explains how blockchain technology might be part of the solution following trials by AgriDigital.



Australia has long enjoyed a clean and green reputation for the food we grow. Our farm produce and processed foods now travel further than ever before, so we need to reassure our customers, and quickly identify and fix problems.

Digitisation and the exploration of blockchain technology have gained incredible traction in other industries over the past few years. It could do the same in agriculture.

### Three key agri-supply chain challenges

#### ***1. Farmers don't get paid for what they deliver when they deliver it***

Historically, growers worldwide have carried the burden of counter-party risk, and the lack of payment security, when making a delivery to a buyer or storage site. Grower and grower-representative groups want greater security over the title to produce for the grower, and want to explore ways to eliminate counter-party risk entirely by matching the transfer of title to payment.

#### ***2. Buyers can't get the financing they need to pay the seller on delivery***

The lack of accurate real-time data prevents financial institutions from managing the risk of lending to the agricultural sector. Buyers don't have accurate data on the farmers' position and the potential inventory they could deliver. Financial institutions don't have access to live industry-wide data for comparison.

The lack of real-time data and event-driven finance also means that many buyers and storage operations must be paid on terms, rather than immediately.

The settlement latency compounds the counter-party risk the sellers face, and compounds the affect of limited liquidity on business growth.

### 3. Consumers don't know where their food comes from

Consumers are demanding the information they need to make informed purchasing decisions. Providing that information is becoming an integral part of a proactive brand strategy.

They want direct knowledge of how and where their food is grown — whether it's produced organically, for example — and they want confidence that the information they're being given is true.

Consumers are now aware of issues such as provenance, counterfeit products, and food security.

### Blockchain as a solution

Blockchain technology, including smart contracts, can provide an immutable record of key transaction data, and link that data with each transaction as goods pass through the supply chain.

A blockchain, as Wikipedia describes it, is a **continuously growing list of records**, called *blocks*, which are linked and secured using cryptography. Its original use was to secure transactions in digital currencies, that is to say, as a ledger, but it can be used for any application that involved a sequence of records that much be kept free from tampering.

The key features of a blockchain ledger:

- All participants have access to the ledger, allowing direct peer-to-peer transactions, rather than relying on an intermediary to facilitate them.
- Information is generally distributed across the network of participants, rather than being stored in a central database. It has no centralised control point or governing entity. A blockchain is often therefore called a “distributed ledger”.
- Data is cryptographically protected against tampering.
- Adding transactions to the ledger requires consensus among the participants who hold a copy of the blockchain.

All this is done automatically by the software platform used by the participants.

Smart contracts use a blockchain to store the agreements and transactions amongst the participants. In supply chains applications, workflows can execute automatically, tracing payments and the title to goods as they pass along the chains .

## Blockchain applications in agriculture

In an August 2017 pilot by **AgriDigital**, digital title for a delivery of oats was generated on a private blockchain network and held in the grower's "digital wallet". Seven days later, settlement occurred in an atomic transaction — meaning that payment was made from the buyer to the grower, and simultaneously title transferred from the grower to the buyer. For the period up until payment, the grower had clear ownership of the digital title token that represented the physical grain delivery, and therefore security over their asset.

The grower delivery was received at the buyer's site using the AgriDigital platform, where information about the quantity and quality of the commodity was captured. That resulted in the generation of a digital title token on the blockchain. The token was then held and flagged for payment in seven business days. Payments were recorded in "AgriCoin", a digital currency used on the platform, equivalent in value to an Australian Dollar (AUD).

Smart contracts were used to auto-execute payment on the blockchain, which was also processed using traditional banking method, to ensure the grower received payment in regular currency. At that point the AgriCoin token was destroyed. Conceptually, that was a currency transfer from AgriCoin to AUD.

Paper-based systems or spreadsheets provide little to no recourse for growers when payment is disputed or fails. The immutable and accessible record on the blockchain, however, means that both growers and all sellers can match title transfer to payment.

This pilot also proved traceability from farm gate to a retailer's distribution point of several loads of organic oats. Data points such as where and how the oats were grown, the transportation from farm to mill, and their processing, packaging and readiness for distribution, were captured. Each representing an event or claim that was critical to maintaining the oats' status as organic.

One challenge is that a blockchain is an immutable record, so it's critical to ensure both the data and the actor making an assertion are correctly identified at the time of record on the blockchain. Manual, human data input continues to act as a threat to data integrity.

## Looking to the Future

Transparent supply chains, and creating a blockchain-based protocol for the global trade in agri-commodities is, I believe, central to this vision.

It's an exciting time to be a part of the agriculture industry and agtech in Australia. Watch this space



# 003.A1

## About the Contributors

*Meet this issue's writers.*



**Andrew McLeish** @stoplineptyltd

Andrew is Managing Director at Stopline Pty Ltd, Australia's leading specialist provider of whistleblower programs and related hotline services. We assist some of Australia's largest public and private sector organisations in meeting their governance requirements and duty to their staff and stakeholders by providing simple, effective and cost efficient services. We also provide fraud and corruption investigation, cyber threat assessment, eDiscovery and forensic IT services to our public and private sector clients. [stopline.com.au](http://stopline.com.au)



**Emma Weston** @emmaweston

Emma is CEO of AgriDigital, which she co-founded in 2015 after a diverse career as a lawyer, agribusiness executive, start-up mentor, and executive coach. She holds an MBA from AGSM and LLB (Hons), BA from University of Melbourne, and is a graduate of the Australian Institute of Company Directors. [www.agridigital.io](http://www.agridigital.io)



**Kate Carruthers** @kcarruthers

Kate is Chief Data Officer for UNSW Sydney, and an Adjunct Senior Lecturer in the School of Computer Science & Engineering at UNSW Sydney. She is a member of the Telstra Industry Advisory Board and the NSW Government's Data Analytics Centre Advisory

Board. She has extensive experience in senior executive roles for diverse organisations including Citibank, General Electric, AMP, Westfield (now Scentre Group), and NSW Treasury. [katecarruthers.com](http://katecarruthers.com)



### **Sumer Dayal**

Sumer Dayal is a lawyer in Clayton Utz's IP & Technology team, specialising in patents, trade marks and copyright disputes as well as technology, media and telecommunications agreements. He has acted for clients in both large-scale IP cases before the Federal Court of Australia and inter-party contract negotiations. His particular interests include cybersecurity and developing technologies. [www.claytonutz.com](http://www.claytonutz.com)



### **Tim Webb**

Tim Webb is a partner in Clayton Utz's IP & Technology team. He has an extensive advisory practice and as an experienced commercial litigator helps clients resolve disputes. Tim advises across the spectrum of intellectual property, including copyright, trade marks, patents, designs, advertising, confidential information and domain names, in both contentious and non-contentious matters. His clients come from a range of industries, although Tim is well recognised for his expertise in the technology, media and telecommunications sectors. He also has extensive experience working with public sector clients. [www.claytonutz.com](http://www.claytonutz.com)



# 003.A2

## About DirectorTech

*Who we are, and how to find us.*

DirectorTech is a regular advisory aimed at company directors of government entities, listed companies, private organisations and not-for-profits. The content for each advisory is researched, analysed and written by a diverse range of international contributors, each expert in their field. Advisories include written content specifically tailored for company directors and individual interactive webinars which focus on identified organisational issues.



**Nigel Phair, Managing Editor and Publisher @nphair**

Nigel is an Adjunct Professor at the Centre for Internet Safety at the University of Canberra, and is an influential analyst on the intersection of technology, crime and society. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.



DirectorTech is an initiative of the **Centre for Internet Safety** at the University of Canberra.

Web: [directortech.com.au](http://directortech.com.au)

Email: [admin@directortech.com.au](mailto:admin@directortech.com.au)

Phone: +61 408 437 056

Twitter: [@director\\_tech](https://twitter.com/director_tech)

Centre for Internet Safety  
University of Canberra ACT 2617  
Australia

ABN 28 150 165 343

DirectorTech is ©2018 Centre for Internet Safety. All rights reserved. Copyright in individual contributions is retained by the authors. Cover and internal digital illustrations ©2018 Stilgherrian.