International Professional Practice Partnership

ifip

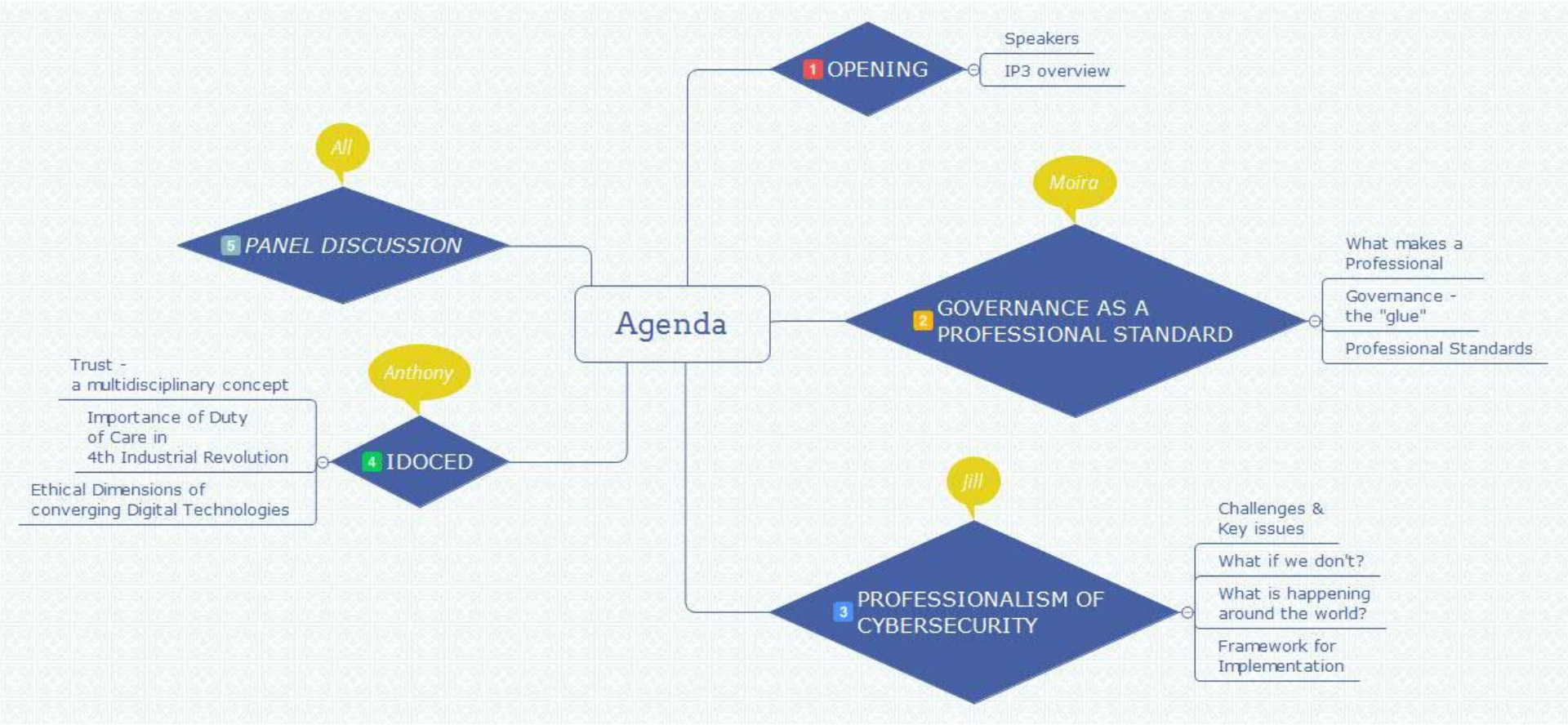
Good Governance: a Professional Standard

which builds Trust and Cybersecurity in the entire digital ecosystem

IGF Internet Governance Forum

International Professional Practice Partnership

Session agenda



International Professional Practice Partnership

Speakers

- Moira de Roche
  - Chair IFIP IP3
  - FIITPSA & PMIITPSA
  - Learning Specialist
  - Ethics evangelist
- Anthony Wong
  - ACS President
  - FACS CP
  - CEO AGW Consulting
  - International speaker on AI
- Dr Jill Slay
  - Professor of Cyber Security at UNSW Australia
  - Director of Cyber Resilience Initiatives for the Australian Computer Society (ACS)

International
Professional
Practice
Partnership

IP3 Overview

International Professional Practice Partnership

Transforming IT Professional Practice

ifip

Informing and Transforming IT Professional Practice

Partnering for Trust in Digital

- Global programme promoting professionalism
- IFIP led, independent & not for profit
- Defining and maintaining global standards for ICT
- Recognising & certifying professionalism

International Professional Practice Partnership

IFIP Community

- The leading multinational, apolitical organization in Information & Communications Technologies and Sciences
- Founded by UNESCO
- Recognized by United Nations and other world bodies
- Represents IT Societies
  - +- 56 countries/regions,
  - covering five continents
  - a total membership of over half a million
- Links more than 3500 scientists from Academia & Industry
- Over 100 Working Groups and 13 Technical Committees

International Professional Practice Partnership

Global Industry Council

- Global Industry Leaders
- Renowned Academics
- Advisory board to IFIP
- Provide advice & insights
- Skills 2020 Guide

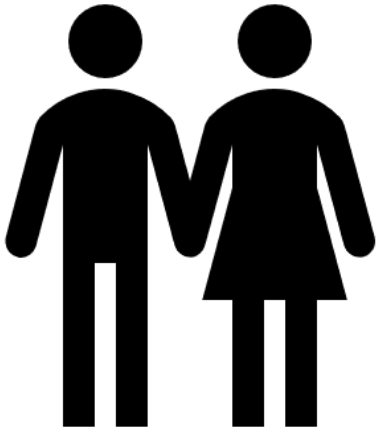
International
Professional
Practice
Partnership

What makes a Professional?

International Professional Practice Partnership

What is a Professional?

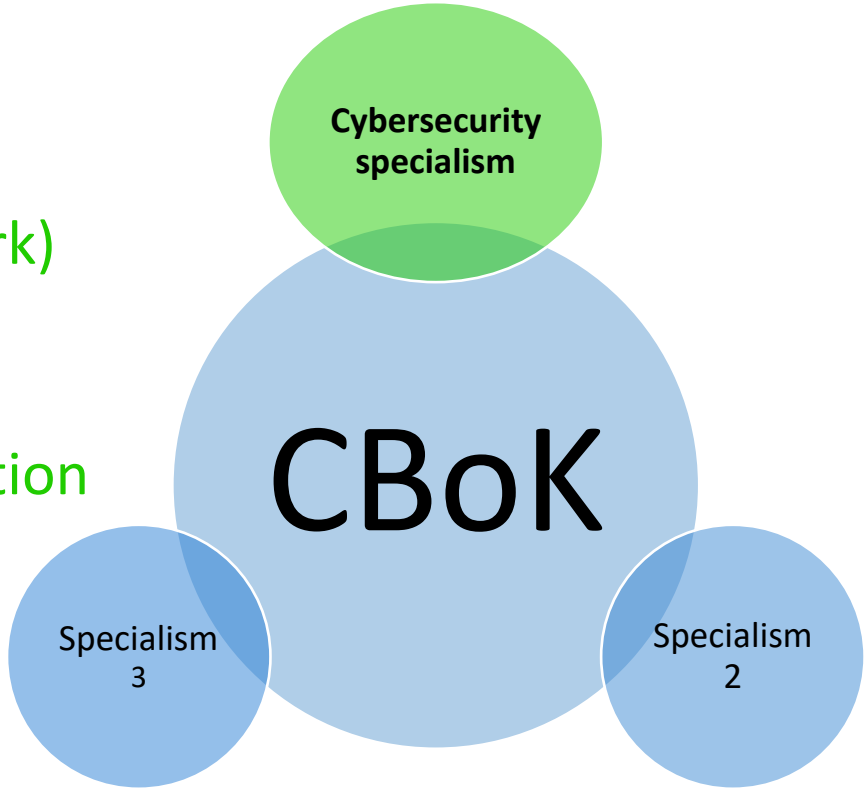
- Skills & Knowledge
- Service
- Trust
- Accountability
- Ethics
- Proud of Profession



International Professional Practice Partnership

IP3 certification

- IP3 Professional (IP3P)
  - Aspirational
  - Vendor neutral
  - SFIA Level 5 (Benchmark)
  - CBoK
  - Complete requirement for Professional Formation
  - Global recognition
- IP3 Technologist (IP3T)
  - SFIA Level 3



International Professional Practice Partnership

Gold Standard

- Quality Assurance
- Accountability
- Trust
- A world that works
- Equivalency

International Professional Practice Partnership

Governance – the “Glue”

International Professional Practice Partnership

Governance

- The need
  - Group or community
  - Achieve a goal or purpose
- Practice
  - Authority
  - Decision-making
  - Accountability

International Professional Practice Partnership

Governance

- Good or bad
- Effective or ineffective
- Not only compliance

International Professional Practice Partnership

Effective Governance

Effective governance is derived from **independent oversight** by **knowledgeable persons** with the **authority** to **ensure implementation of corrective action** and to **guide behaviour patterns** into the habit of **compliance**.

International
Professional
Practice
Partnership

Professional Standards

www.ipthree.org

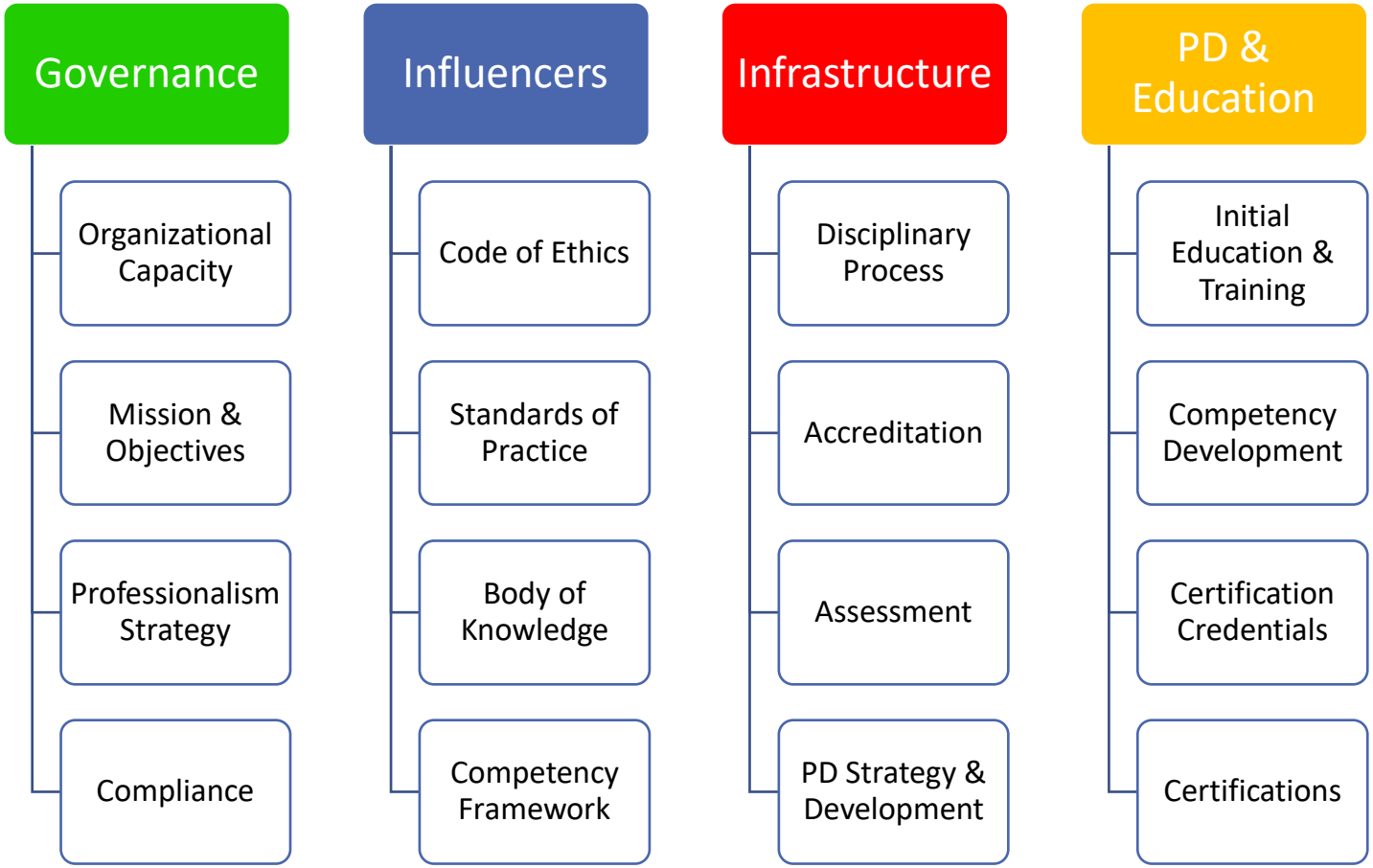
International Professional Practice Partnership

Definition

Professional standard of care. Ethical or legal duty of a professional to exercise the **level of care, diligence, and skill prescribed** in the **code of practice of his or her profession,** or as **other professionals in the same discipline would in the same or similar circumstances.**

International Professional Practice Partnership

Anatomy of a Profession



International Professional Practice Partnership

Governance Requirements in a Digital World

- Algorithm design
- M2M learning
- Autonomous transport devices
- Environmental impact
- Cryptocurrencies
- Cybercrime, personal and corporate vulnerability
- Access to networks - rights, responsibilities

International Professional Practice Partnership

Professional Standards

- Expertise and competence
- CBoK
- Lifelong learning
- Trustworthy computing
- Behaviour
  - Subscribes to and lives by Codes of Conduct & Ethics
- Apply to practitioners in all roles

International Professional Practice Partnership

Professional Standards for Governance

- Compliance Habit
- Active mitigation of risk
- Defence of Best Practice
- Whistle-blowing
- Ethics
- Leadership must ensure competence

www.ipthree.org

International
Professional
Practice
Partnership

Professionalism of Cybersecurity

Dr Jill Slay

International Professional Practice Partnership

- Definitions of ‘Cyber security’ still unclear.
- Strong demand for Cyber security practitioners but understanding of ‘professionalism’ not explicit.
- Pseudo Professional Standards.
- Australian Development of Professional Standards in Cyber Security

Overview

International Professional Practice Partnersh

Eight Vectors of Attack and Response*

Cyber security must address a range of political, social, legal, technical, management and personnel issues.

*Source: adapted from a Bell Labs graphic

What is Cyber Security?

International Professional Practice Partnership

- ‘Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.’
- Has implications from Government perspectives on
- Cyber Law
- Domestic Cyber Policy
- International Cyber Policy
- Communicating Cyber Security Issues
- Offensive Cyber Effects / warfare
- Cyber Economy- startups and commercialisation
- Cyber intelligence and forensics
-
- Estimation that we in Australia need 8000 more practitioners to meet status quo by 2025 and 10-11,000 to deal with growth - >1 million globally

‘Cyber Security’ for Governments?

International Professional Practice Partnership

- For Governments to develop cyber policy, legislation, technology, curricula and cyber industry growth we must
- Establish the minimum independent professional standard of competence for a cyber security practitioner – cf. engineering
- Provide a complete requirement for full professional formation of a a cyber security practitioner.
- Assure employer of the maintenance of competence through continuing professional development.
- Support by a disciplinary code with a process for public complaint and sanctions.
- Without Professional Standards we cannot ensure good governance, duty of care, validation and verification of results, efficiency, effectiveness, an appropriate future work force in a cyber context.

Why do we need Professional Standards

International Professional Practice Partnership

- Topics that are currently deemed to be the minimum of ‘cybersecurity’ content in an ICT degree are:
- Computer system security: CPU, Peripherals, OS. This includes data security.
- Physical security: The premises occupied by the ICT personnel and equipment.
- Operational security: Environment control, power equipment, operation activities.
- Procedural security: By IT, vendor, management personnel, as well as ordinary users.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.

Updating Current Concepts of ‘Security’ in Australia

International Professional Practice Partnership

- To provide recommendations on the establishment of a cyber security specialism certification. Thus creating Australian Professional Standards at request of Minister Tehan
- Identify all job roles and occupations aligned with cyber security.
- Establish a baseline of knowledge and skills criteria which represents the minimum expectations of cyber security technician and professional
- Provide recommendations of professional assessment techniques for determining whether an individual has the cyber security knowledge and skills to fulfil the identified baseline requirements.
- Ensure recommendations are aligned with international best practice and comply with appropriate national and international cyber security professional and technical standards.

Work of ACS Cyber Task Force

International Professional Practice Partnership

- The approach of contextualizing existing international frameworks identified as best practice by the Taskforce, for appropriate implementation in the domestic Australian market has been taken.

- We have asked ourselves:
- What should a Cyber skilling framework look like?
- What does International Best Practice look like?
- How can we ‘Australianise’ it?

Overarching Context

International Professional Practice Partnership

- Examine practise of a range of countries including US, UK and Singapore
- Determine types of tasks carried out by Technologists and Technical Managers of Cyber Security
- Map out competencies assessed by common certifications
- Take on board existing Australian government evaluator criteria

How to determine cyber skilling competencies?

International Professional Practice Partnership

- Department of Defense Directive 8570 provided guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions.
- These individuals are required to carry an approved certification for their particular job classification. GIAC certifications are among those required for Technical, Management, CND, and IASAE classifications.

US original policies: DoD 8570 (2005) and 'pseudo professional standards'

International Professional Practice Partnership

- The NICE Cybersecurity Workforce Framework (NCWF) is a national US resource that categorizes and describes cybersecurity work.
- It provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks and skills required to perform cybersecurity work.
- Standardizes how positions are managed and described by populating position descriptions with Tasks and KSAs from the Workforce Framework.
- Incorporate Tasks and KSAs into job advertisements to attract candidates who can perform needed job functions.
- Develop career paths that outline the Tasks and KSAs staff need to perform to progress to the next level.

National Initiative for Cybersecurity Education (NICE)

Technical Level 1 **CompTIA A+** **CompTIA Network+** **SSCP** **CCNA-Security**	**Technical Level II** **CompTIA Security+** **GSEC** **SSCP** **CCNA-Security**	**Technical Level III** **CASP** **CISA** **CISSP** **GCIH (or Associate)** **GCED**
Managerial Level I CompTIA Security+ CAP GSLC	Managerial Level II CASP CAP CGSLC CISSP (or Associate)	Managerial Level III GSLC CISM CISSP (or Associate)
Specialist Level I CASP CISSP (or Associate) CSSLP	Specialist Level II CASP CISSP (or Associate) CSSLP	Specialist Level III CISSP - ISSEP CISSP - ISSAP

Historically Identified IA roles and certs : DoD 8570

International Professional Practice Partnership

- We used a similar method and also SFIA, the Skills Framework for the Information Age, (which describes skills required by professionals in roles involving information and communications technology).
- It provides a common reference model in a two-dimensional framework consisting of skills on one axis and seven levels of responsibility on the other. And also describes professional skills at various levels of competence.
- We have mapped common cyber security certifications using SFIA to develop a potential cyber skilling framework

Mapping Common Cyber Security Certifications

International Professional Practice Partnership

- An environmental scan on global certifications held in high esteem has been undertaken via the taskforce and broader industry consultations. It is the Taskforce's view that those certifications with the greatest global acceptance provide an opportunity to expedite the introduction of an ACS Cyber Specialism.

Outcomes

International Professional Practice Partnership

- These have been identified for Certified Technologist (Cyber Security) as:
- Systems Security Certified Practitioner from ISC²
- Certified Information Systems Auditor from ISACA

- These have been identified for Certified Professional (Cyber Security) as:
- Certified Information Systems Security Professional from ISC²
- Certified Secure Software Lifecycle Professional from ISC²
- Certified Information Security Manager from ISACA

Outcomes

International Professional Practice Partnership

MACS CT Cyber
SSCP CISA
MACS CP Cyber
CISSP CSSLP CISM GIAC

Australian Cyber Professional Standards Framework

International Professional Practice Partnership

- A mapping exercise of the nominated ISC² and ISACA certifications have been mapped to SFIA and levels 3 and 5 as required through the ACS certifications.
- These are in many cases higher than the nominated SFIA levels. Reflecting the multi-disciplinary nature of Cyber Security, there is little overlap across these certifications. As a result, the taskforce is of the view that flexibility needs to be built into the specialism process.
- We have recommended three SFIA skills from a limited SFIA list of ten for Certified Technologist and four skills from ten for Certified Professional.

Outcomes

International Professional Practice Partnership

- Cyber security specialism assessment requirements are equivalent to existing ACS Certified Professional assessment criteria and pathways with the addition of demonstrating in-depth competence in 4 SFIA skills at SFIA level 5. SFIA skills must be from the following skills:

- IT Governance
- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Penetration Testing
- Security Administration
- Programming/Software Development
- Systems Software
- Testing
- Asset Management

Certified Professional - Cyber Security

International Professional Practice Partnership

Cyber security specialism assessment requirements are equivalent to existing ACS Certified Technologist assessment criteria and pathways with the addition of demonstrating in-depth competence in 3 SFIA skills at SFIA level 3. SFIA skills must be from the following skills:

- Information Management
- Information Security
- Information Assurance
- Business Risk Management
- Systems Development Management
- Asset Management
- Change Management
- Security Administration
- Incident Management
- Conformance Review

Certified Technologist - Cyber Security

International Professional Practice Partnership

- 1. At this stage, greater research is required to be undertaken on certifications provided by SANS and CREST and other global organisations but similar mappings will also be produced.
- 2. There is ongoing discussion with Defence contractors, vendors and the Big 4 with a view to mapping the learning outcomes of their training courses to those SFIA outcomes recommended above.
- 3. ACS will be developing a repository of open source resources for self-education and running, where necessary, specialized workshops to allow for the development of specific SFIA skills.
- 4. ACS will offer micro-credentialing to test for these SFIA skills.
- 5. ACS will work with government and industry to advise and support the implementation of these Professional Standards.

Further work

International Professional Practice Partnership

- Australian industry needs to profile cyber positions or clusters
- Individuals need to be certified for sake of individual career path
- Employers need to look at future work force issues
- Professional standards provide vehicle for these and also for board responsibilities such as governance, due diligence and duty of care

Implications

International
Professional
Practice
Partnership

iDOCED

Anthony Wong

International Professional Practice Partnership

TRUST =

"Firm belief in the reliability, truth, or ability of someone or something."

Oxford Dictionary

International Professional Practice Partnership

Trust in the Digital Economy

- Technology is pervasive – it impacts every aspect of our lives. It underpins and enables:
  - ❖Collaborations
  - ❖Communications
  - ❖Connectedness
  - ❖Interactions
  - ❖Infrastructure including Critical Infrastructure for Human Survival
  - ❖Information Sharing
  - ❖Products and Services
  - ❖Transactions

We can no longer live without it!!

International Professional Practice Partnership

The Fourth Industrial Revolution

Converging technologies are disrupting and reshaping our world including:

- Artificial Intelligence (AI)
- Automation & Machine Learning
- Autonomous Vehicles – drones, cars, trains etc
- Blockchain
- Robotics
- Internet of Things (IoT)
- The Cloud

International Professional Practice Partnership

Trust in the Digital Economy

- Trust is essential for people to embrace digital technology and feel confident in using it
- A lack of trust will limit potential benefits of the digital economy by:
  - ❖Reducing productivity gains
  - ❖Restricting economic growth
  - ❖Limiting access to new markets, products and services
  - ❖Discouraging interest in ICT careers, leading to critical skills shortages

Trust is a Multi-Disciplinary Concept

Trust requires certainty in the areas of:

- Security
- Privacy
- Usability
- Safety
- Reliability/Performance
- Access

A breach in *any one* of these areas will *diminish trust* and *discourage users from engaging* with systems/technology.

International Professional Practice Partnership

When Trust is Broken …

DIESELGATE

- 99,672 diesel Volkswagens affected in Australia alone
- Australian Consumer and Competition Commission (ACCC) is *taking legal action* against Audi AG, Audi Australia Pty Ltd, and the German parent, Volkswagen AG over diesel emissions
- VW Australia is also *facing class actions* from affected Australian car owners

International Professional Practice Partnership

When Trust is Broken …

WannaCry Ransomware

- *400,000+ users* affected worldwide
- Major organisations crippled across Europe, Asia & US
- Exploited leaked NSA hacking tools
- 98% of victims using Windows 7
- Highlighted *dangers of using outdated software*

Some ethical dimensions of converging digital technologies in our digital ecosystem

AUSTRALIAN COMPUTER SOCIETY

International Professional Practice Partnership

Ethical dimensions of converging digital technologies in our digital ecosystem

- **The 'Intelligent' car**: what if an autonomous vehicle is programmed with an algorithm that would, in a crash situation, 'sacrifice' the life of a pedestrian over that of the vehicle's owner? **Could the car's designer, or the developer of the algorithm, or the owner of the car be charged with a crime?**

- If ethical parameters are programmed into AI, whose ethical and social values are they? What biases do we build in – intentionally or otherwise – that will affect the output? Each individual, sociocultural group and national geography can have different attitudes to ethics, morality and legality.

- A natural outcome of machine learning and the application of big data is that algorithms often become even more complex over time, to the point where even the developers don't fully understand what is going on.

International Professional Practice Partnership

Ethical dimensions of converging digital technologies in our digital ecosystem

- **Killer robots**

➢ Recently a proposal was put to the UN for a treaty to ban lethal autonomous weapons -- aka 'killer robots'. The open letter was signed by over 100 business and technology leaders from 24 countries including Elon Musk - Telsa, SpaceX; and Mustafa Suleyman, Head of Applied AI at Google's DeepMind.

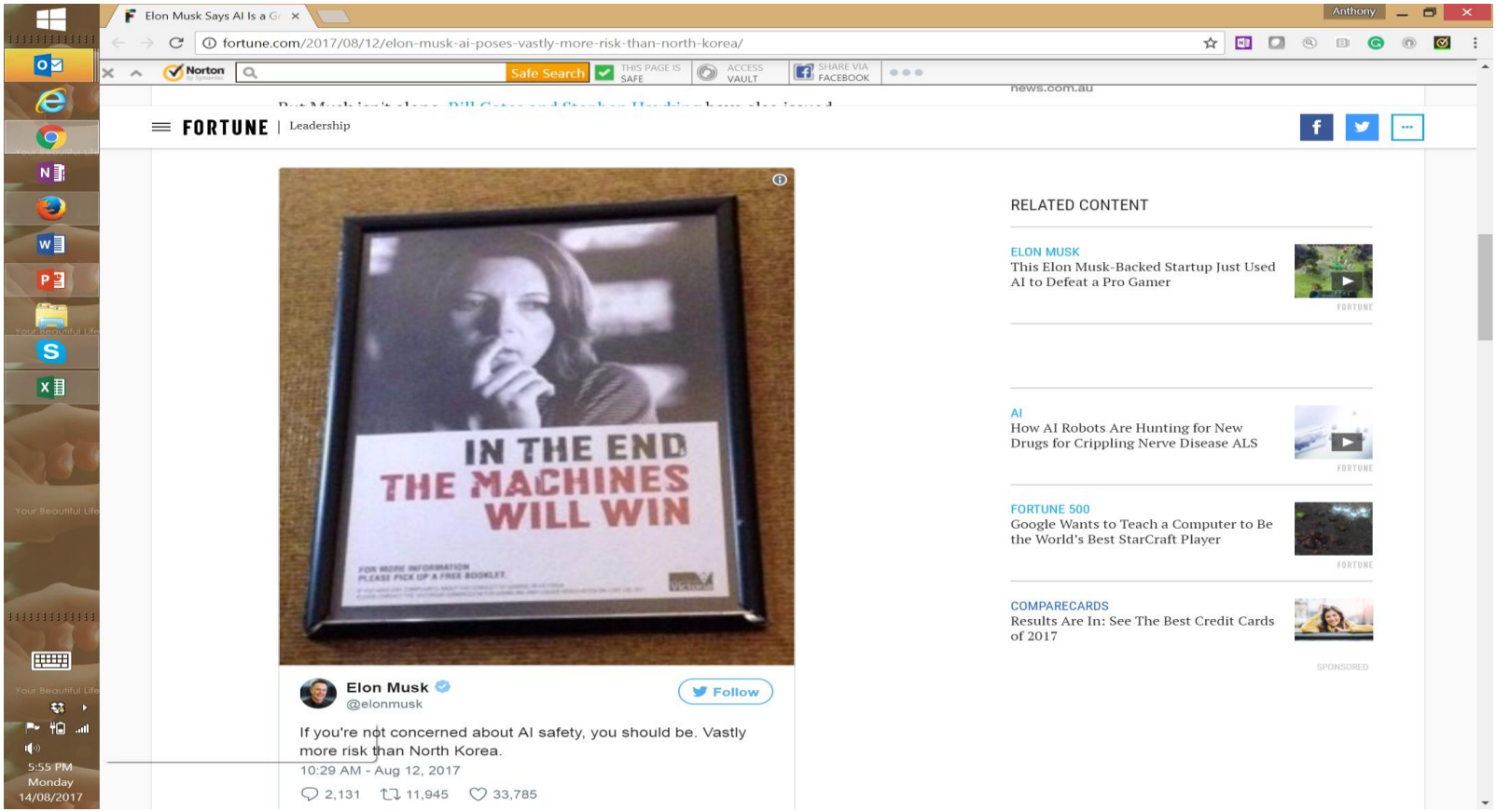
- **Influence**

➢ We are moving rapidly towards a world where robots and intelligent AI systems are connected to the mesh and influenced by Social Media, the internet of Things and Big Data. Clear boundaries and filters will be needed to prevent these systems from being influenced and corrupted by darker elements.

- The Singularity

➢ One fear is what's known as The Singularity, where an AI achieves a level where it can self-improve and enter a cycle of ever-accelerating, run-away self-improvement that results in a super intelligence far beyond our own capabilities, leading to potentially catastrophic changes for human civilisation.

Elon Musk: *AI Poses 'Vastly More Risk Than North Korea'*



International Professional Practice Partnership

Ethical dimensions of converging digital technologies in our digital ecosystem

- Autonomous cars being fooled by…
  - Kangaroos!
  - Graffiti and stickers on street signs.

- Microsoft Tay chatbot corrupted in 24 hrs
  - Taught racist, hate and abusive speech through social media.

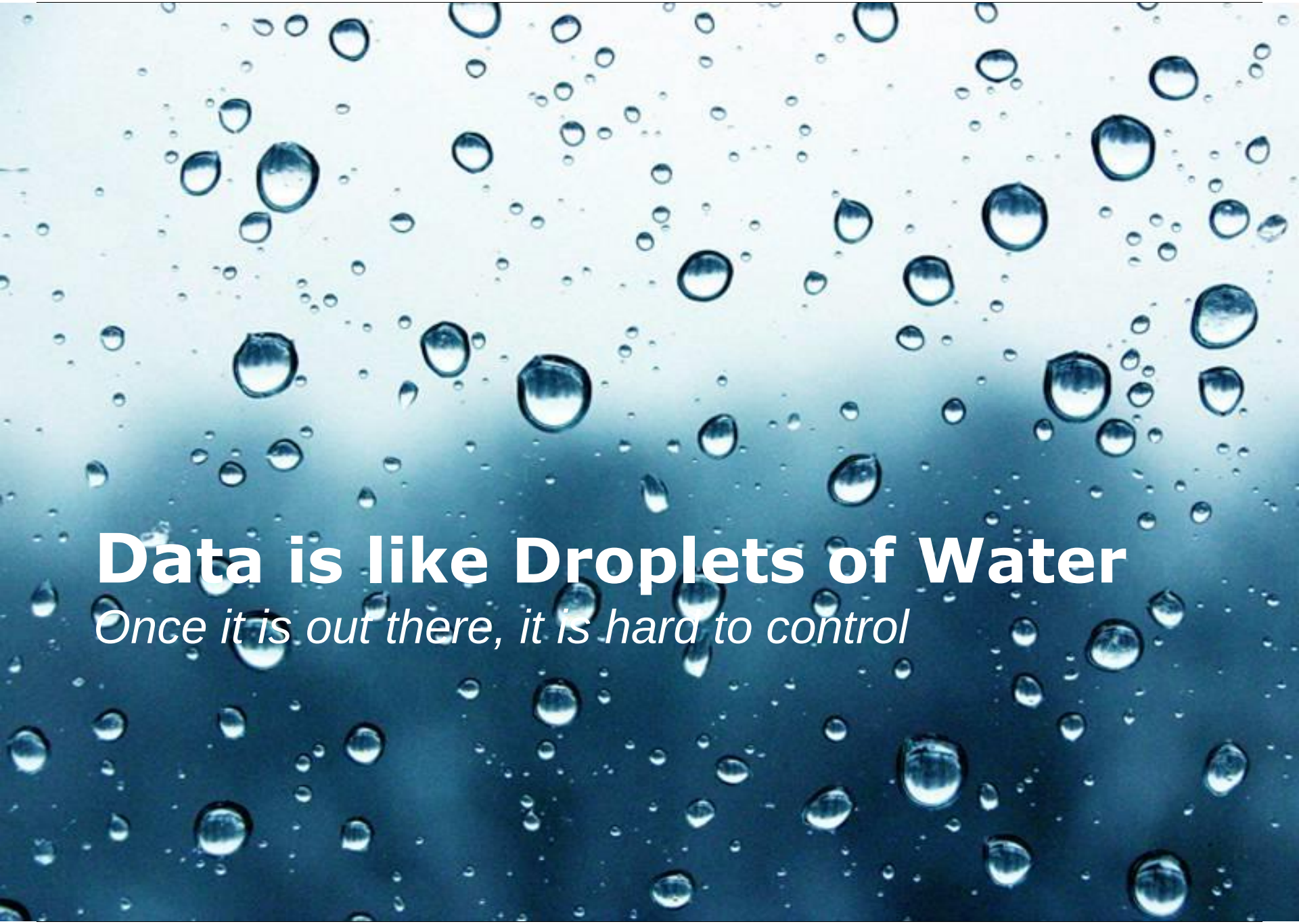
- Google's image search reveals limits
  - Google ***was forced to apologise*** after its artificial intelligence photo app labelled two black people as "gorillas".

International Professional Practice Partnership

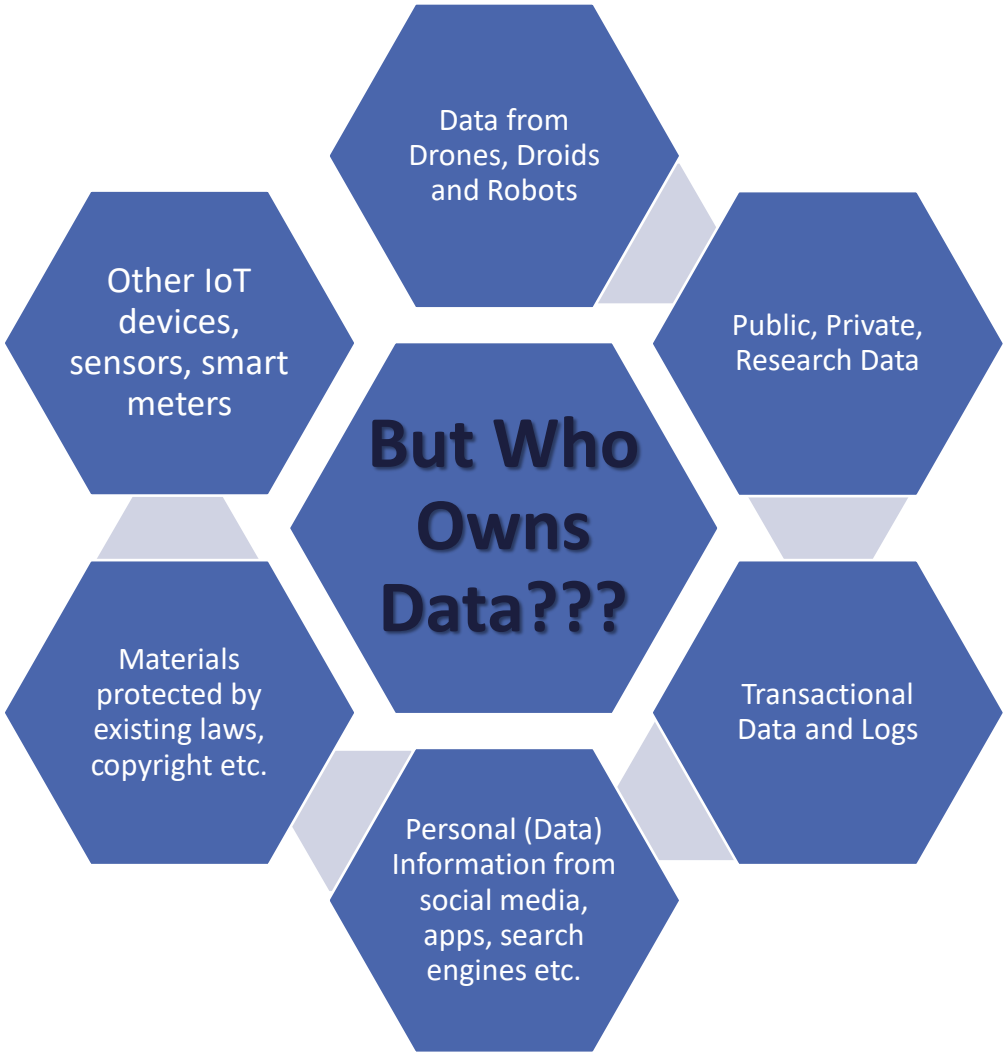
Internet of Things (IoT)

- **IoT concept thought to date back to the early 1980s**.
  - A vending machine selling beverages at the Carnegie Mellon University was connected to the Internet so its inventory could be accessed online to determine when new stock was needed.
- **Term covering a multitude of devices and technologies**.
  - Can be viewed as a collection of devices with low processing power and network communication capabilities.
- **Increasing number of IoT devices**.
  - In 2017, IoT reached 8.3 billion devices and is expected to reach 20.4 billion in 2020.

Source: Presentation by Professor Jill Slay, Australian Centre for Cyber Security UNSW Canberra 2017


Data is like Droplets of Water
Once it is out there, it is hard to control

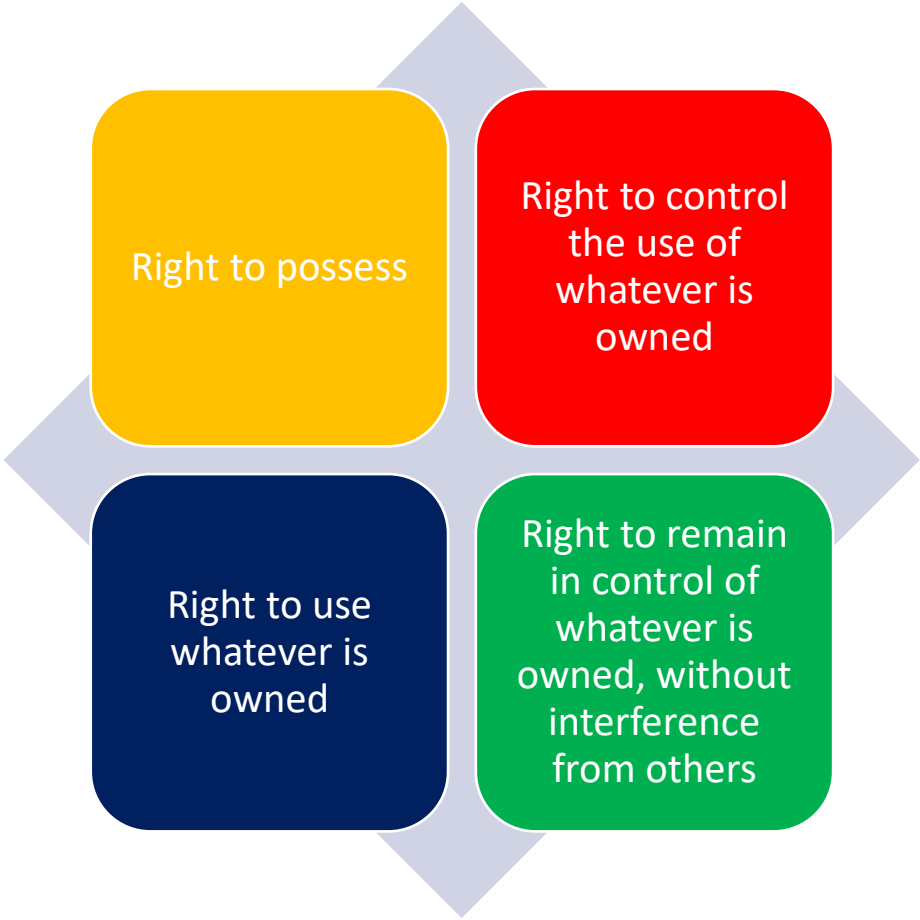
International Professional Practice Partnership



Data sources (including from IoT) as varied as the types and colours of flowers

Concepts of Ownership

Ownership includes:



Source: Honoré, A. M. (1961) "Ownership" in A. Guest (ed) Oxford Essays in Jurisprudence, OUP

International Professional Practice Partnership

The Challenges We Face

- As yet there is no consensus on how to secure IoT devices and no comprehensive solutions have appeared to date.
- IoT device vulnerabilities will expand the attack surface – drones, wearables, medical devices, home security.
- Looking futuristically, we see large scale acceleration of use of IoT sensors, an excitement about their use and some development of security standards, but no obvious engagement with potential disruption.

Extracts: Presentation by Professor Jill Slay, Australian Centre for Cyber Security UNSW Canberra 2017

International Professional Practice Partnership

Challenges in our complex cyber environment

- The embedded OS(s) will have security vulnerabilities
- The embedded hardware may have security vulnerabilities
- These devices may run for decades
- They will be built to price, with time-to-market a major consideration (security?)
- They may be covered by stringent regulation and testing (eg. Medical devices), or very little at all
- The people who “own” them may not even be aware they’re present, and if they are, how to upgrade them
- Yet they will possess network connectivity and the required operating system and hardware environment to support that
- These are major challenges

Source: Presentation by Professor Jill Slay, Australian Centre for Cyber Security UNSW Canberra 2017

Legal solution from US

S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017

- .. issue guidelines for each executive agency to require the following clauses in any contract, except as provided in paragraph (2), for the acquisition of Internet-connected devices:

- *(A) Verification required.--*

  (i) In general.--A clause that requires the contractor providing the Internet-connected device to provide written certification that the device

  …

  (ii), does not contain, at the time of submitting the proposal, any hardware,

  - *software, or firmware component with any known security vulnerabilities or*
- *defects listed in*

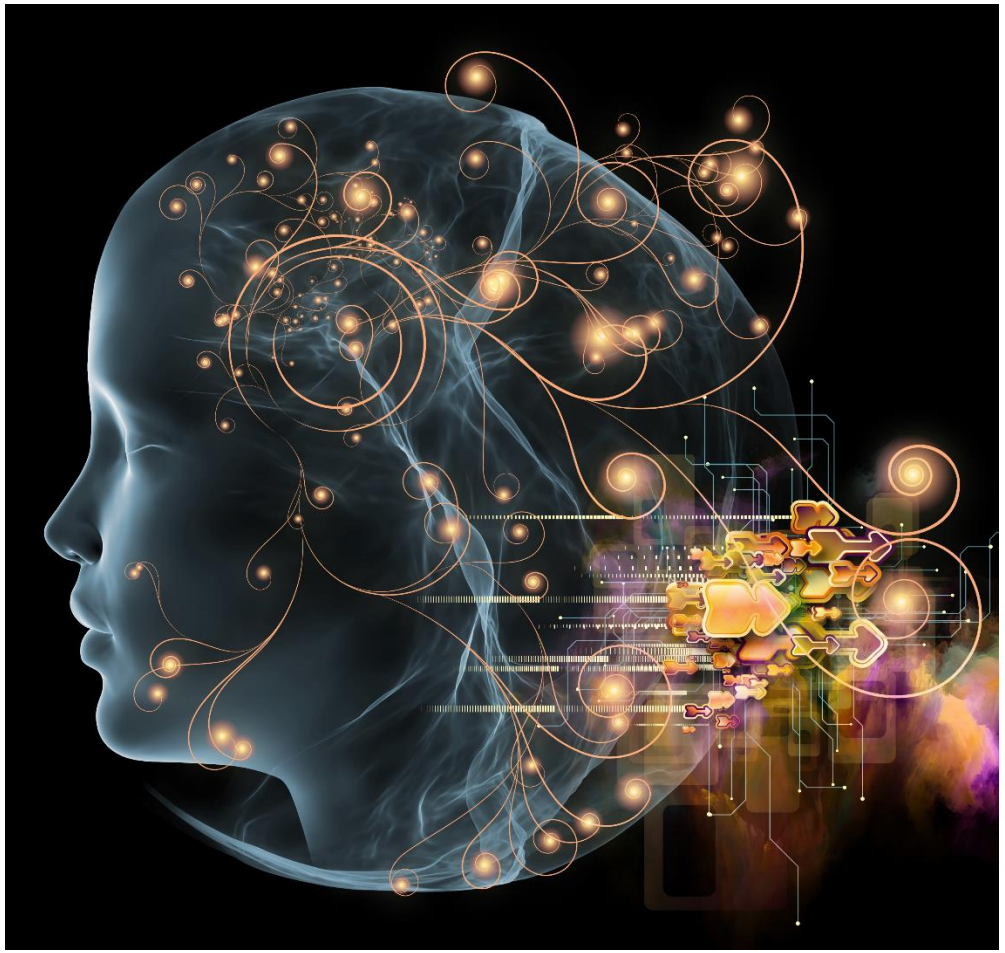
***Source: Presentation by Professor Jill Slay, Australian Centre for Cyber Security UNSW Canberra 2017**

International Professional Practice Partnership

Impact of Automation – Robots, AI and You

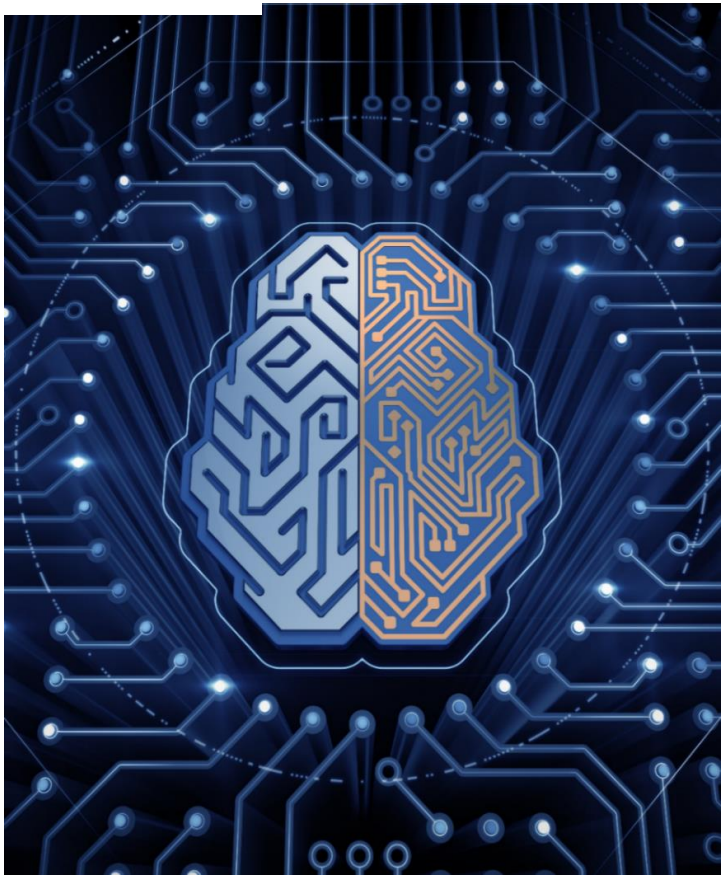
- Why Robots?
  - Work 24/7
  - Don't get paid
  - Don't complain
  - Don't need breaks
  - Increased production rate
  - Reliable repeatable results

- Why AI?
  - Work 24/7
  - Don't get paid
  - Don't complain
  - Don't need breaks
  - Faster, more accurate results
  - Better at processing volumes of data
  - Entirely new possibilities arise



International Professional Practice Partnership

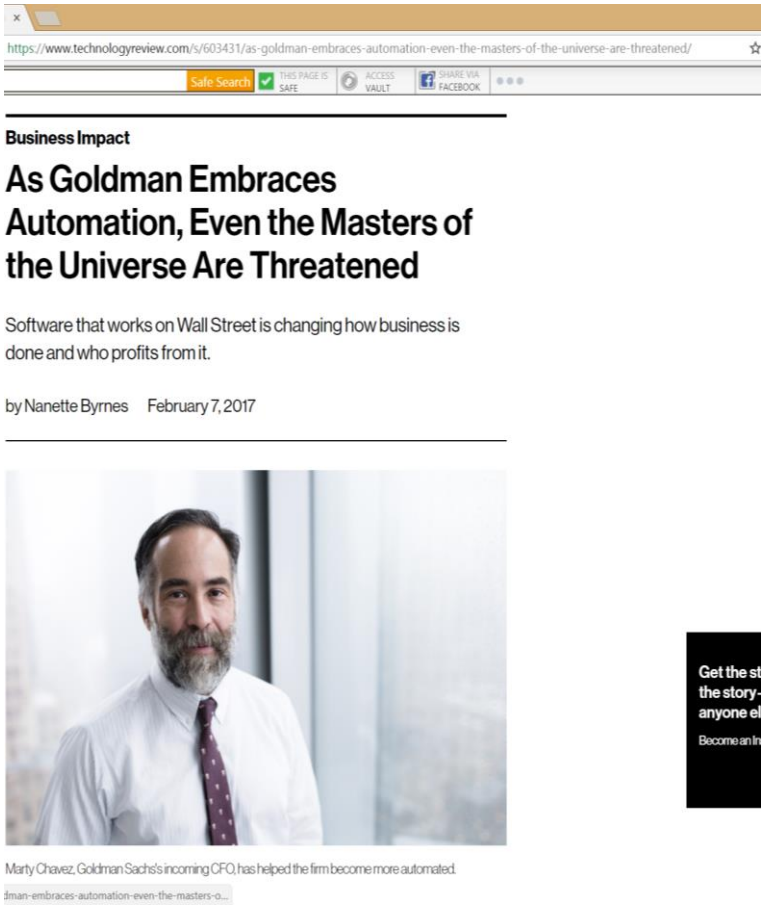
Impact of Automation - Example



- *"In the realm of …algorithms, the action unfolds at a pace that would be incomprehensible to the fastest human trader…*
- *At the turn of the 21st Century, Wall Street firms employed nearly 150,000 financial workers in New York City; by 2013, the number was barely more than 100,000 –*
- *even as both the volume of transactions and the industry's profits soared"*

ɔact of Automation – an Example

- Goldman Sachs employed 600 equity traders in 2000. Today, there only two.
- Automated trading programs have taken over the work – supported by 200 computer engineers.
- *"…four traders can be replaced by one computer engineer. Some 9,000 people, about one-third of Goldman's staff, are computer engineers."**



https://www.technologyreview.com/s/603431/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/

Business Impact

As Goldman Embraces Automation, Even the Masters of the Universe Are Threatened

Software that works on Wall Street is changing how business is done and who profits from it.

by Nanette Byrnes February 7, 2017

Marty Chavez, Goldman Sachs's incoming CFO, has helped the firm become more automated.

https://www.technologyreview.com/s/603431/as-goldman-embraces-automation-even-the-masters-of-the-universe-are-threatened/

What drives Duty of Care?

When does Duty Arise?

AUSTRALIAN COMPUTER SOCIETY

International Professional Practice Partnership

Example 1 – Security of Critical Infrastructure Bill 2017 (Australia)

- Australian sabotage laws will be modernised to cover all major critical infrastructure including utilities
- "The Bill will regulate approximately 100 assets in the highest-risk sectors of ports, electricity and water. If any of these assets were disrupted, they would have a significant impact on Australia's economic interests and services for large populations.
- Part 1, Division 2 – Definitions outlines the thresholds for determining which assets will be classed as 'critical infrastructure' and who constitutes a reporting entity or an operator, upon whom the obligations under the Bill will fall."
- This Bill will impose reporting requirements on two sets of entities: direct interest holders and responsible entities.
- Direct interest holders of a critical infrastructure asset will be required to provide interest and control information in respect of the asset. Responsible entities for a critical infrastructure asset (effectively the main licensed body) will be required to provide operational information, such as system access abilities and operator and outsourcing arrangements.
- These entities will have six months to report the required information from the commencement of the legislation.

***Source: Presentation by Professor Jill Slay, Australian Centre for Cyber Security UNSW Canberra 2017**

Example 2 – EU General Data Protection Regulation (GDPR)

- Access to data and its use has become a hot topic.
- At the rate of technological transformation, the debate is unlikely to abate anytime soon.
- The EU leads the world in legislating to protect and provide access to personal data with its EU General Data Protection Regulation (GDPR).
- Replacing the 1995 Data Protection Directive when it comes into operation in May 25, 2018.

Who is caught by the GDPR?

- Businesses with an establishment in the EU or that offer goods and services in the EU, or that monitor the behaviour of individuals in the EU may need to comply.

International Professional Practice Partnership

Some Key Considerations – EU General Data Protection Regulation (GDPR)

- Require businesses to take appropriate technical and organisational security measures, including effective cyber security measures.
- Accountability and governance - Accountability principle in GDPR Article 5(2) requires demonstration of compliance with the principles.
- Enhanced measures including:
  - Data minimisation;
  - Pseudonymisation;
  - Transparency;
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis.
- Use of Privacy Impact Assessments (PIA) where appropriate.
- Records of processing activities (documentation).
- Obligation to provide comprehensive, clear and transparent privacy policies.
- In many circumstances, controllers and processors will need to appoint Data Protection Officers (DPOs).

International Professional Practice Partnership

EU General Data Protection Regulation (GDPR) provides the following rights (Duty?):

- ✓The right to be informed
- ✓The right of access
- ✓The right to rectification
- ✓The right to erasure (right to be forgotten)
- ✓The right to restrict processing
- ✓The right to data portability
- ✓The right to object
- ✓Rights in relation to automated decision making and profiling

EU General Data Protection Regulation (GDPR) – Breach Notification

- Duty to report certain types of data breach to the relevant authority and to the individuals affected.
- *What breaches do I need to notify the relevant supervisory authority about? W*here risk to the rights and freedoms of individuals are likely.
- *When do individuals have to be notified?* Where there is high risk to the rights and freedoms of individuals.
- *How do I notify a breach?* Report to the relevant supervisory authority within 72 hours (of becoming aware).
- If the breach is sufficiently serious, you must do so without undue delay.
- Failing to notify a breach => fine up to 10 million Euros or two per cent of global turnover.

International Professional Practice Partnership

Trend Micro 2018 Predictions

- Many companies will only act after the first high profile lawsuit is filed:
  - 57% of C-level executives shun the responsibility of complying with GDPR.
  - 66% of companies appear dismissive of GDPR fines.
  - 42% of businesses aren't aware that email marketing databases contain Personally Identifiable Information (PII).
  - Only 34% of businesses have invested in technology to identify intruders.

Example 3 – Cybercrime & Security Framework

There is no "International" 'Law of Cyberspace' - however, in Australia, there are a number of regulatory and policy landscapes that may be applicable including (not exhaustive):

- *Privacy Act 1988 including the* new Australian Data Breach Notification provisions - *Privacy Amendment (Notifiable Data Breaches) Act 2016* which will commence 22nd February 2018
- *Cybercrime Act 2001*
- *Spam Act 2003*
- *Telecommunications (Interception and Access) Act 1979*
- *Electronic Transactions Acts*
- *Copyright Act 1968* - intellectual property

International Professional Practice Partnership

Cybercrime & Security Framework

- There are many legislations which have some relevance to cybercrime.
- Legislation is not uniform, either in offence provision or in penalties.
- Offences apply within each jurisdiction and offences target unlawful access to computers and data, and offences committed using a telecommunications service or carrier.
- Examples of Australian legislation include *Cybercrime Act 2001* (Federal) and *Crimes Act 1900* (NSW).

International Professional Practice Partnership

Cybercrime & Security Framework

- Generally, the Australian provisions make it an offence for a person to do or attempt to do the following:
  - unauthorised access to a computer system
  - unauthorised access or modification of data
  - impairment of electronic data and communication
  - impeding access to computers; and
  - possession of data with intent to commit serious offence

An example of an Cybercrime offence – WannaCry?

Section 308I of the *Crimes Act* 1900 (NSW) states:

A person:

a) *who causes any unauthorised impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means, and*

b) *who knows that the impairment is unauthorised, and*

c) *who intends to cause that impairment, is guilty of an offence.*

Example 4 – Privacy Regulatory Framework in Australia

- Legislation e.g. the *Privacy Act 1988 (Cth)* including the new Australian Data Breach Notification provisions - *Privacy Amendment (Notifiable Data Breaches) Act 2016* which will commence 22nd February 2018
- Mandatory reporting of incidents where:
  - there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
  - the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates
- Equitable and common law duties regarding confidential information
- State privacy legislation (State laws) and health privacy laws
- Security and Information Management Standards and Practices
- Other Codes of Conduct, Industry Standards and Guidelines

IFIP Duty of Care in Everything Digital (iDOCED)

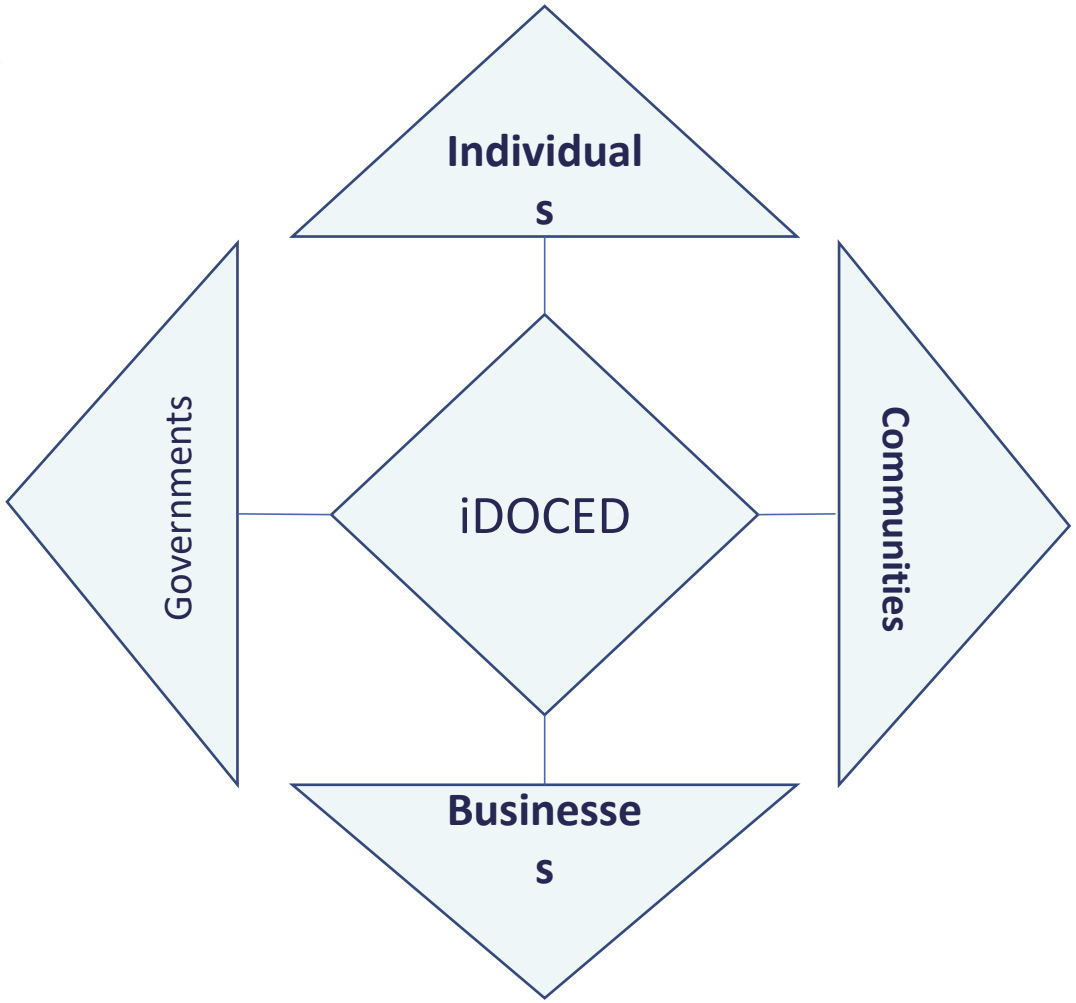
iDOCED was developed in response to numerous instances of:

- Poor ethical behaviour by companies
- Low quality/underperforming products
- Lack of care by consumers in how they access and use social media and other technologies

IFIP Duty of Care in Everything Digital (iDOCED)

iDOCED is designed to remind and support both *providers and consumers* of digital products and services that they have a *duty of care* in ensuring that they *act responsibly* in relation to the digital world.

iDOCED – Duties of Care for …



Duty of Care for Businesses

- ✓Responsibility of the board of directors and officers to fulfil their Duty of Care
- ✓What are the questions that they should ask about their businesses' cyber readiness and awareness?
- ✓What are the roles of directors and officers? - oversight
- ✓Who is responsible for cybersecurity in the business?
- ✓The roles and accountabilities in the chain of relationships in the business – interactions with customers, suppliers and 3rd parties

International Professional Practice Partnership

Duty of Care – Businesses – Privacy and Security

- Businesses are ultimately responsible for the protection of data/information that is stored and/or processed — even in the Cloud.
- Management must maintain assurance that the security of their ICT infrastructure, including the cloud service provider, is adequate for their purpose.
- An example:
  - *Privacy Act 1988 Australian Privacy Principle 11 — security of personal information*
  - *11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:*
    (a) from misuse, interference and loss; and
    (b) from unauthorised access, modification or disclosure

Duty of Care for Individuals

ICT Professionals must take responsibility for ensuring that ICT systems are Trustworthy.

"Ensuring cyber security and cyber resilience is also a *duty of care* of the individual *ICT professional*, in all stages of a system life cycle (design, development and operation). This means that most, if not all, types of *ICT functions and jobs must contribute to cyber security and cyber resilience*."

Leon Strous, Immediate Past President, IFIP

Duty of Care for Individuals

- ✓*Duty of care applies to ICT professionals*, in all stages of a system life cycle (design, development and operation)
- ✓Be aware and intentional in how you use technology
- ✓Ask questions about the tools you use
- ✓Become informed
- ✓Make demands of your legislators
- ✓Check the qualifications and credentials of your providers
- ✓Put your trust in demonstrated competence and ethics
- ✓Use passwords
- ✓Protect yourself

International Professional Practice Partnership

Duty of Care for Communities

- ✓Develop Information Security awareness
- ✓Establish collaborative models
- ✓Submit actions for scrutiny
- ✓Educate individuals – give them more power
- ✓Support and recommend trustworthy companies
- ✓Exercise governance
- ✓Address resource shortages

International Professional Practice Partnership

Duty of Care for Governments

- ✓Work with international organisations on:
  - ✓Regulations
  - ✓Standards
  - ✓Mandatory professional standards & accreditations
  - ✓Develop partnership agreements with other countries
- ✓Legislate for mandatory reporting of cyber attacks
- ✓Engage in trusted threat intelligence sharing
  - ✓State-sponsored attacks

ACS
Cyber Security Specialis

- Developed in Australia by the ACS.
- Designed to provide a level of Assurance, Trust and to address the growing shortage of cyber security expertise.
- Launched by Australian Minister Assisting the Prime Minister for Cyber Security, the Hon Dan Tehan in Canberra in Sept 2017.
- Adopted by IFIP IP3 as a new specialism certification for member societies around the world.
- ACS support for the implementation of the Australian International Cyber Engagement Strategy announced by the Hon Julie Bishop MP, Minister for Foreign Affairs in October 2017.
- Raise professional standards for cyber security specialists.
- Highlight the Duty of Care for cyber security professionals.

Thank you

anthony.wong@acs.org.au

Anthony Wong, President ACS

IFIP Councillor, A technologist and a lawyer

AUSTRALIAN COMPUTER SOCIETY

International
Professional
Practice
Partnership

Panel Discussion

All

International Professional Practice Partnership

Closing

- Any last comments?
- Actions going forward
- Let's not forget ……