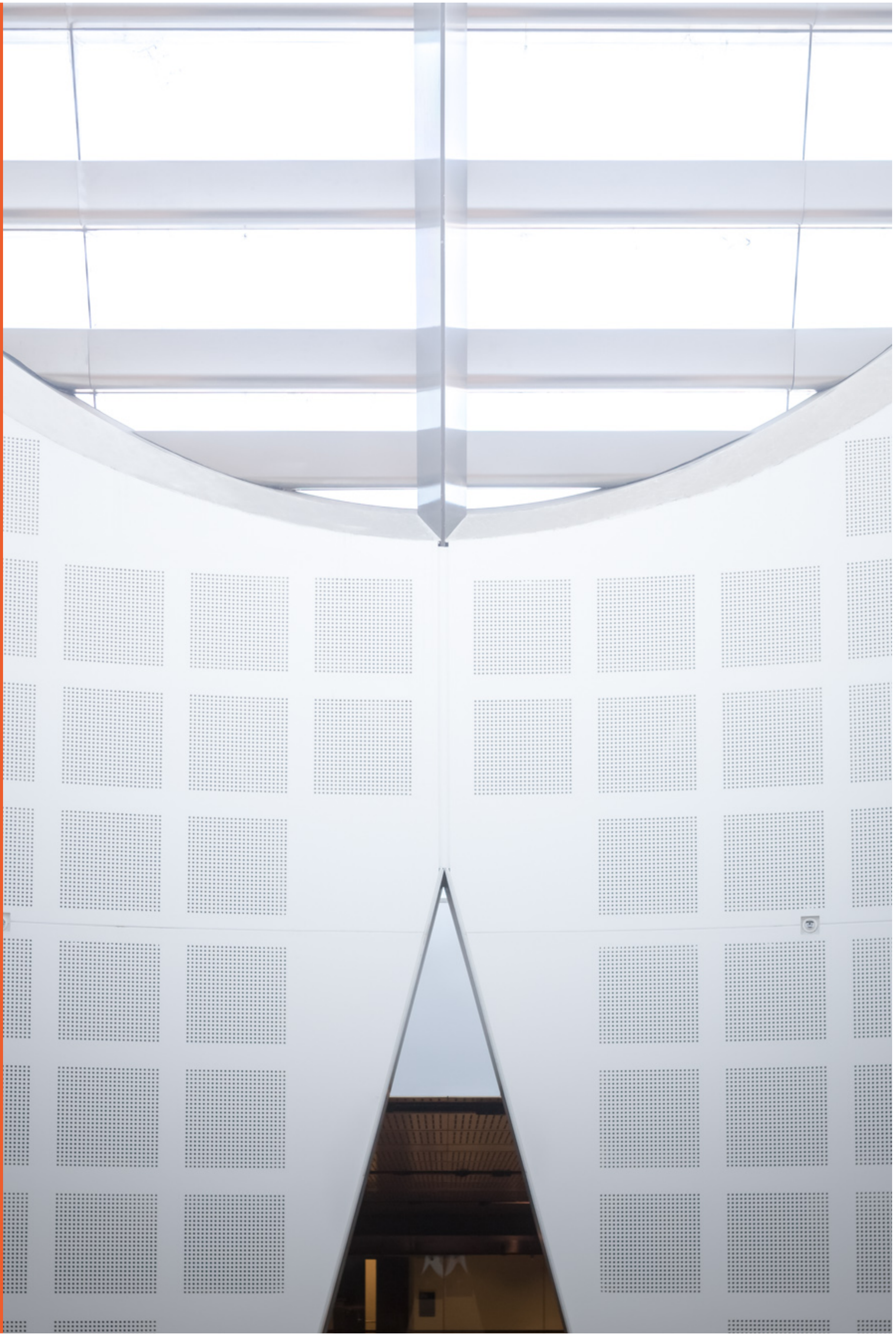
INFO2222

Security Management, Legal & Ethics

Presented by

Luke Anderson

THE UNIVERSITY OF SYDNEY



Overview

- Security management
  - Policy
  - Procedures
  - Risk Analysis

- Operational planning and execution

- Legal issues & ethics

Security management

IT security policy

- High-level management needs to set the framework in which operational decisions can be made.

- It is important for this framework to be explicit and documented.

- An organizational security policy provides this
  - IT Security Policy may be one part of a wider organizational security policy

What's in a policy

- Audiences
- Purpose
  - Explicitly order or trade-off
- Assets
- Nature of the protection
- Responsibility

Audiences

- Stakeholders
  - Users
  - Operators
  - Owners
  - Beneficiaries

- They should all be able to examine the security policy
  - See how it reflects their security goals
  - See how their interests are balanced with other stakeholders
  - See what their main rights and responsibilities are, in interacting with the IT system

Purpose

- Policy should state the purpose(s) of security functions, reflecting the balance between stakeholders' goals

- Security purpose should be related to the overall goal or nature of the organization

- A small number of major objectives (3-5 is common)

Examples:

- *Ensure that sales can be made, quickly and when the customer wants.*
- *Build reputation among customers for caring about them.*

Purpose

Very common example: comply with laws and regulations.

Note: be aware of tension between purposes.

“ease of use” versus “keep competitors from getting information about our plans”

The core of the policy

- What sorts of assets
  - Hardware
  - Software
  - Information
- What sort of protection
  - Who can access the system
  - What can they do
- Who is responsible for security
  - Who decides on the details
  - Who authorizes budgets
  - Who carries out the operations
  - Who checks that it is done

Examples

- Central computing services will be responsible for the installation and service of all computing systems used to store information of value.

- Data we collect about a partner company will be treated as confidential, and not released to other partners.

- Corporate computers are not to be accessed except by authorized employees.

- For each type of data stored about employees, the HR Manager will make a determination of the privacy level of this information.

Evaluation of policy

- Policy needs to be written at a high, business-focused level.

- So it can be read and understood by all stakeholders.

- It is all too easy to produce a poor security policy, that does not really guide day-to-day security decisions.
  - This can lead to chaotic security, where different aspects work against one another, and competing interests can't resolve their differences

- One should look at a security policy, and check that it is useful as a guide to decision-making on the ground.
  - Note: this is not the same as judging whether one agrees with the policy

Characteristics of good policy

Coverage

- Policy should apply, or explicitly be excluded from applying
- Policy should provide guidance when faced with all security-related decisions
- Don't leave lower-level managers or operators to guess whether they are allowed to do something, or how to balance between stakeholders

Durability

- Policy should continue to be meaningful through change
- Don't rewrite policy just because a new virus emerges, or because the company opens a new branch
- This means policy can't deal in specific technologies
- Policy changes only because corporate direction changes, or because of a deep lasting shift in social concerns

Characteristics of good policy

Realism

- It must be possible to implement the policy with existing technology, in reasonable amounts of time and cost
- This means that policy shouldn't be decided without technical input
- Policy shouldn't be for absolute perfection

Clarity

- Succinct
- Direct
- Plain English/Avoid jargon

Security procedures

- The day-to-day operation of the organization requires many security activities to be done.
- It is important for this to be explicit and documented.

- Examples:
  - How accounts are (supposed to be) created.
  - How passwords are (supposed to be) assigned and changed.
  - How a computer is (supposed to be) connected to the network.

Comparison

Policy

- High-level, expressed in business terms
- Set by senior management (board level)
- Widely read, publicly available
- Should change only rarely

Procedures

- Concrete and detailed, expressed in technical terms
- Set by middle managers and technical staff
  Specific to particular classes of employees
- Can change with technology
- Should be in line with policy

Physical security

- An important aspect of security procedure involves controls on hardware, how it is operated, and its environment.

- Examples:
  - locks on rooms,
  - power supply,
  - movement of equipment,
  - storage of backups

Facilities

- Threats from nature:
  - Flood
  - Fire
  - Earthquake
  - Power outages.

- Threats from people:
  - Damage to machines
  - Theft
  - Damage to power supply, air con, water, etc
  - Loss (especially mobile devices)

From disgruntled employees, competitors, random vandalism, mistakes.

When it has happened: do you have backups?

- Always assume: you **will** be hacked. Promise.
- Probably the most important recovery mechanism is to have backups of the data.
  - Take regular, frequent backups.
  - Store them away – and not just the most recent.
  - Keep them on independent media, ideally off-site
- Check that they are usable.
  - Try to restore from backups
- Backups help with availability.
  - But also with integrity (if data is corrupted, use a backup to get a previous, good version)

Business continuity

- There should be procedures for carrying on with core business functioning during and after an incident that interrupts computer system availability.
  - What work is low-priority, and can be postponed
  - What paper records need to be kept of activity during the outage, to enter into the computer system later
  - How to test whether the system is usable again

- Also called "disaster recovery"

Security risk analysis

- To arrive at sensible policy and procedures, one needs to understand what threats there are, and how serious they are.
- Many organizations do this informally and intuitively, but this often leads to poor decisions.
  - “Fighting the last war”
  - Driven by security-product vendors (Fear, Uncertainty, Doubt)
  - Lack of security because incentives are wrong
- Many organizations blindly follow "compliance documents"
  - "If we complied, they can't sue us"
  - Hardly a proper security proposition
- A defined process of analysis of risk follows.
  - Team of stakeholders and experts
  - Aim to systematically categorize dangers, and prioritize them for control

Methodology

- There are many different detailed methodologies for risk analysis.

- Most are adapted for more general risk analysis.

- We describe a simple 3 step approach.
  - Identify the assets
  - Identify the vulnerabilities and threats
  - Give values to key parameters for each risk

- For proper attack modelling: INFO3616

Asset identification

- What computing-related assets have value which could be reduced by an attack?
  - How are they used in providing the needs of the organization?

- Hardware
- Software
- Data
- People (skills)
- Documentation
- Infrastructure

Vulnerability and threat identification

- Brainstorming to consider how each asset may be affected.

- Use experience of previous attacks, but also think outside the box.

- Consider what current procedures say, but do not assume that they are followed!

- Make a long list of possibilities
  - (don't worry if some are far-fetched)
  - A useful guide: how could confidentiality be reduced? How could integrity be reduced? How could availability be reduced?

Estimating parameters

- Key to sensible decision making is to estimate how seriously each threat needs to be taken.
- Two essential parameters:
  - Depending on the methodology, these may be given numeric values, or just categories (high, medium, low)
  - **Risk impact:** how much damage do we suffer if an attack succeeds?
  - **Risk probability:** how often will an attack succeed?
- Problem: we often have no precise number
  - That's why we need empirical analyses of security breaches
  - Developing field
- From these, we work out the seriousness of our exposure to risk.
  - Worst exposure is from a frequently successful attack that does a lot of damage

Risk impact

- Consider the loss: what negative effects are there on the organization if a problem happens.

- Typically, one converts other difficulties into money lost. Examples:
  - Inconvenienced customers leads to lost revenue
  - Virus infection requires staff time to clean up

Risk probability

- Consider the chances of the loss occurring.
  - This might depend on how often an attack is tried, and what fraction of attacks succeed in actually doing damage

- Quantitatively, we want to know the expected number of losses.

Risk exposure

- The importance of a threat comes from both impact and probability.
- Quantitatively, define expected loss as
  (impact if damage occurs) * (expected number of damages)
- Gives Annualized Loss Expectation (ALE)
- Qualitatively, use methodology-specific table.

- Examples:
  - top exposure is high impact
  - with medium or greater probability
  - medium exposure is either high impact with low probability, or medium impact with medium or greater probability

Evaluating risk analysis

Advantages

- Value of varied participants
- Benefit of doing this in advance, with less panic
- The discussions often throw up useful knowledge
- Articulating the tradeoffs can lead to better decisions
- It can strengthen the political case for security investments

Disadvantages

- False sense of precision
  - Real data are not available
  - Estimates of probability are very hard to do sensibly
- Time consuming to carry out
  - Staff are deflected from other duties
- Results may get locked in
  - continue to be used even after the underlying situation has changed
  - very common, and counter-productive

Evaluating risk analysis

- Planning to change a system to reduce risk exposure, involves introducing controls.
  - There are many known controls, including those covered in this course
  - A control may mitigate: reduce the probability of damage occurring
  - Or it may be a contingency: reduce the impact when the damage occurs

- Decide on a relatively small set of controls that between them improve the risk exposure for the most serious threats.

Making a business case

- IT staff often need to convince senior management to fund security activities.
  - Many organizations see IT as a cost, not a profit center
  - Budget is always under pressure
  - Competition between proposals from different business units
- One key approach is “return on investment”.
  - Estimate the savings from doing the activity, minus the cost of doing it
  - Also consider time value of money (eg savings in future are worth less than costs now)
- Tools exist from vendors, but doing it needs numeric values for impact and probability.
  - Very rubbery
- Compliance requirements are often more effective arguments.

Operational planning

- Once funding is approved, a detailed project must be planned
  - Just like any project management task

- Determine steps
  - Find dependencies
- Estimate how long each takes
- Allocate people to do each
- Check on progress
- Modify plans if progress is too slow

Assurance

- It is important to make sure that changes are working as anticipated.

- Especially, check whether documented procedures are actually followed:
  - Do people allow colleagues to use their account?
  - Is the password kept on a post-it note on the desk?
  - Is the operator making sure that the backup is usable?
  - Does the security guard come around when they should?

- People get into routines, and procedures need to be refreshed.

Responsibility

- A vital ingredient in planning is the decision about who is responsible.
- Who can make decisions.
- Who checks that things are happening.
- To whom do these get reported.
- Security aspects should fit with overall management structure.

Review cycle

- Security policy and procedure should be reviewed regularly.

- Make sure that they are still appropriate.
  - Organizational purpose may change
  - Threats may arise
  - Especially as organizations are restructured

- Every document should include a date for review, and someone needs to plan to carry out these reviews.

Reflections

- Costs and benefits must be considered and traded off.
- IT Security should fit into general management framework.
  - Document decisions and their reasons
- Policy should drive procedures.
- Don’t confuse documented procedures with actual practices.

Legal issues & ethics

Goal of this section

- You know of a range of issues that can have legal significance.

- You know that you don't know the law.
  - Don't rely on lectures, newsgroups, popular books, etc, for the rules!
  - Don't assume that fairness, common sense, or morality determine what is legal and what is not

- You know how ethical positions can be argued.

- You have practice in identifying the stakeholders and their interests.

Questions

- You bought a copy of a program; are you allowed to keep a backup copy?
- Your computer has been infected by a worm which turns your machine into a zombie that takes part in a DDoS attack. Can you be sued by the target?
- You lend a coworker your machine when they need to rapidly print out an important document, and they use the opportunity to copy some files to their USB drive, and take it home. Can you be fired?
- You write a program to encrypt data, and release it as open-source. Can you be arrested and extradited to another country?

"It depends"

- **General** legal questions usually don't have clear-cut answers.
  - Different laws apply in different jurisdictions
  - Many laws might be relevant and many were not written specifically for IT
  - It takes many cases to clarify the exact features which determine how the law is applied in particular situations
  - The law comes from both legislation and precedent decisions

Jurisdictions

- Depending on the laws and the situation,
  - rules might be based on where the server is located
  - where you are resident
  - what it says in a contract
  - where the person lives about whom data is kept
  - where a company is incorporated
  - how much money the company earns in a year
- Take this very seriously
  - The European General Data Protection Regulation (GDPR) generally extends to all companies operating in the EU – even if they are incorporated in Australia, they need to follow EU regulations
- It is possible for several different legal systems to each claim that their (contradictory) rules apply to the same situation.

Digital property

- Many laws are applied in IT, even though they were written mainly for quite different domains.
- Copying, or manipulating, files of bits can be covered by laws such as:
  - Copyright
  - Patent Law
  - Contract Law
    - Example: a licence agreement that was signed
  - Theft, fraud, misuse of authority
    - Especially if the information has commercial consequences
  - Trademarks

Clear Wealth theft

"The plaintiff claims that, before he left Clear Wealth, Mr Kwong copied client lists stored in Mr Kwong's Clear Wealth computer (and deleted those lists from his Clear Wealth computer) and, by means of a USB drive, loaded those lists onto his own computer and external hard drives at home. The plaintiff claims that those lists comprise information confidential to Clear Wealth and that Mr Kwong was precluded contractually from taking and from using those lists. The plaintiff also claims that Mr Kwong, in breach of an express contractual provision, conducted work on behalf of Your Life Now Pty Ltd within the period of three months after his departure."

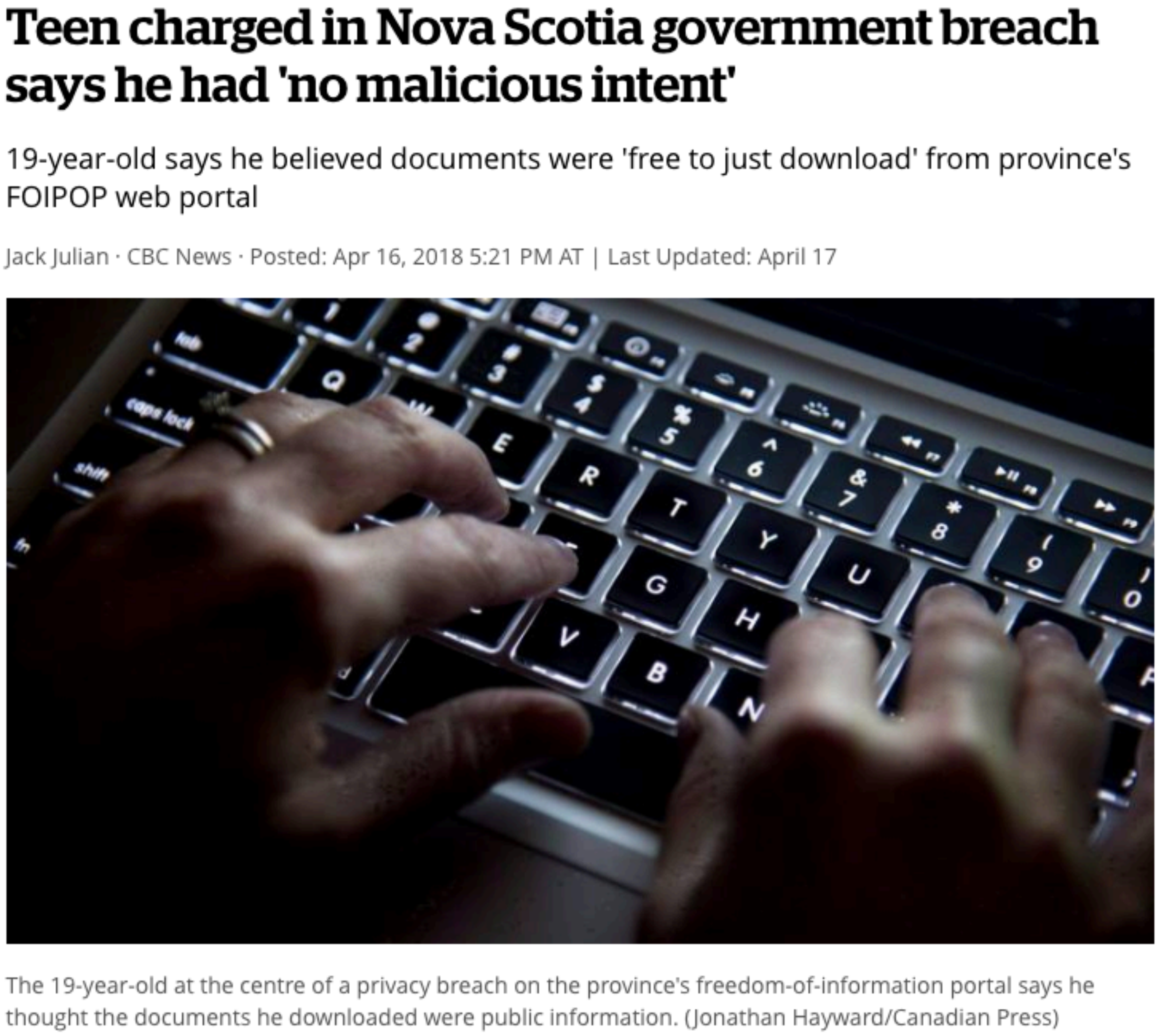
Clear Wealth Pty Ltd v Kwong (No 2) [2012] NSWSC 1233

Writing software

- There are laws that forbid producing certain types of software
  - some countries (try to) forbid encryption/decryption,
  - some countries forbid reverse engineering,
  - some countries forbid format conversion

- Except for authoritarian states, you will generally find a spark of sanity in these laws
  - E.g. prosecution for "hacking" must prove intent to penetrate defences – accidentally visiting some unknown URL is not hacking
  - Unfortunately, some courts tend to put the bars really low

Nova Scotia, Canada, 2018



Teen charged in Nova Scotia government breach says he had 'no malicious intent'

19-year-old says he believed documents were 'free to just download' from province's FOIPOP web portal

Jack Julian · CBC News · Posted: Apr 16, 2018 5:21 PM AT | Last Updated: April 17

The 19-year-old at the centre of a privacy breach on the province's freedom-of-information portal says he thought the documents he downloaded were public information. (Jonathan Hayward/Canadian Press)

What had happened?

- Government of Nova Scotia operated a server with documents released **publicly** under the Freedom of Information act
  - The documents were simply numbered: 1.pdf, 2.pdf, 3.pdf, ...
  - A 19y old teen discovered that and wrote a script that downloaded one by one
- Unfortunately, the government had accidentally also uploaded non-public documents
  - These were downloaded as well
  - They discovered "the breach" and had police arrest "the hacker" in a raid
- Charged under an act that allows up to 10 years in prison

- **So – what is right here and what is legal?**

Extradition

- Mr Kalinovas violated four separate Lithuanian criminal code legislation.

  (a) making a fake non-cash payment instrument, faking a genuine electronic payments instrument or illegal disposal of an electronic payment instrument or data thereof;

  (b) illegal connection to an informational system;

  (c) illegal use of electronic payment instrument or data thereof; and

  (d) fraud

- On 23 January 2015, the Magistrate determined that Mr Kalinovas is eligible for surrender in relation to the four extradition offences.

Kalinovas v Republic of Lithuania [2015] FCA 961

Employment

- Most countries have specific laws that govern interactions between employer and employee
  - What rights an employee has
  - What responsibilities an employee has
  - What rights an employer has
  - What responsibilities an employer has
  - Some of these can be modified by employment contract, but others over-ride contract terms
- Issues include use of IT resources, care and competence in doing work, OHS, etc
- Very common: employer allowed to monitor all Internet communication
- A sysadmin or security officer may sometimes be an employee, and at other times they act on behalf of the employer

Medicare

- Marita QUETCHER – branch manager at Shellharbour.

- Medicare subsequently discovered the defendant had enrolled 65 false identities on the Medicare Program and had processed a total of 387 claims against those identities, amounting to $156,034.50.

Medicare

- The defendant was found guilty of all the charges.
- In sentencing, the Court noted:
  - that the offences were above the mid-range of seriousness
  - the defendant abused the trust that she held through her position of authority
  - the offences were premeditated, deliberate and relatively sophisticated
  - the defendant had lied and denied her involvement in the conduct
  - and the amount of money involved was significant.
- The defendant was sentenced to a total of 8 years imprisonment to be released after serving 5 years.

Commonwealth Director of Public Prosecutions General Fraud

Privacy

- Varied laws that govern use of personal or identifying data.
- Think of large social networks, but also governments, bank, insurers
  - Can the data be released, sold, even moved?
  - Can the data be shared with collaboration partners?
  - Can the subject demand corrections?
  - Can authorities require access to data?
- Examples:
  - Commonwealth laws for federal government bodies, large companies
  - Australian state laws on health records
  - European GDPR: "right to be forgotten" – deletion rights
  - European GDPR: right to know how data is stored and processed

Privacy

- In technical terms, there are many ways to guarantee certain degrees of pseudonymization
- Key words: k-anonymity, l-diversity, t-closeness, differential privacy
- Some insights:
  - Absolute anonymity does not exist
  - "Anonymization" of a dataset always means "pseudonymization to a certain degree" – can in general be broken!
  - In fact, a truly anonymized data set would be indistinguishable from statistical noise (by definition) - and hence useless
  - We are hence always talking about trade-offs
  - Strong academic research, but little deployment
  - Corporations often store raw data – but this may change with more modern legislation

Reporting

- Some laws require release of information to police.

- Some laws require release of information
  - often also to those affected
  - particularly when personal data is compromised or released

- Some laws require release of information to investors - especially for a public company.

- Some laws forbid release of information
  - i.e. about a police investigation or a case being heard in courts

Ethics

- Ethics is a branch of philosophy: how to decide what is right or wrong action

- Ethics is also a branch of psychology: how people actually decide

- Our goal:
  - You recognize ethical tensions in security topics
  - You can justify your decision

- Not our goal:
  - Any particular decision

Tension between stakeholder goals

- Security always involves tension between goals of different people.
  - Alice wants to access resources; Jane doesn't want Alice to access these resources
  - For example: Alice wants to analyze sales data for trends, Jane doesn't want Alice to analyze sales data
    - Is Alice the sales manager?
    - Is Alice a vendor?
    - Is Alice a warehouse worker trying to gain skills that will be in demand in the future?

Ethical reasoning

- Attempts to provide a basis on which to make judgments of right or wrong

- Two main classes of reasoning:
  - **Teleological:** based on consequences of the decision
  - **Deontological:** providing general guidance on duties, and how to weigh up conflicting duties

Ethical pluralism

- Different people do in fact make ethical judgments differently.
- Leading philosophers and religious thinkers have advocated different frameworks or underlying principles.
- These do not always lead to the same recommendation for action.
- Even the same principles/frameworks can lead to different judgments in a case.

Employment

- In security work, you may find an employers policy or direction asks you to do something you would not do as an individual.

Teleologist: losing one's job or opportunities for promotion are important consequences.

Deontologist: fidelity to promises made to employer, gratitude to employer for what they have done for you.

Ethics with or against the law

- Sometimes your ethical principles align with the law.
- Sometimes what is (for you) an ethical act is illegal.
- Sometimes what is required by law is (for you) unethical.

- Civil disobedience.
  - A long and honoured tradition (Gandhi, ML King) but the tradition expects accepting the legal consequences

- Resistance to the law.

- Adherence to the law, while trying to get it changed.

Reflections

- The law is complicated – many facets and argued in court rooms every day, across many jurisdictions.

- As an individual, try to act reasonably – hope that others respond to the evident good will. Always get formal help if you are unsure. In a corporate setting – there are company lawyers.

- Ethics are hard – balancing many stakeholders and many views of ‘what is right and just’.

- Tread lightly, be open to other viewpoints.