Legal Perspectives on the Software Industry in a Surveillance Economy:

* intentions and motivations - what's in your head
  + the bush protections people example, they only protested against people they believed were doing wrong
  + the greenies tried to stop endangered habitat being destroyed were able to prove they were stopping a greater crime than they were charged with, so their charge was thrown out
  + it's good if you have evidence of your intentions. They passed a leaflet around that showed they were only doing it to stop greater unlawful activity
  + but sometimes they don't care about intentions, just what you did
* law
  + law isn’t universal like values, it is made by specific people
  + laws change, but who changes them? what influences them?
* liability
* software
  + if a piece of software prevents you from doing something you are legally entitled to doing should you be able to bypass it legally (hack the software) OR should that hacking be illegal?
  + Students have weaker restrictions when it comes to copyright i.e. they can legally copy DVD’s for example. Manufacturers at the time didn’t take this into account though, and DRM blocked everyone from copying. It was made illegal to hack any software, even if you have the legal right to do what the hacking will achieve, and so student cannot legally hack DRM, even though they do have the right to copy DVD’s.
* OzTrack
  + Tracking all transactions between all accounts, not just big transactions. Criminals worked out that lots of small transactions spread out over multiple accounts can go undetected.

PART A – intro to law and ethics

* Strange bedfellows – law and IT/Comp Sci
  + Law is very self-referential. It is what the judge says it is, it’s what politicians say it is etc. it’s not universal.
* About the legal system
* Liability
  + what can possibly go wrong? who is responsible for it?
  + Were you at fault? Or did someone trick you? Did someone force you? Di they have obligations they didn’t hold up? (lawyer/doctor)
  + start-ups are trying to go 0 liability
* Software development – immature?
  + Very creative industry but it’s immature and thus not predicable.
  + We don’t yet know the right way of doing things, so it’s hard to tell if someone did something wrong
* Data integrity profession
  + Doctors, architects, psychiatrists are legally professionals, are software engineers?
* What shapes the law?
  + Its ever changing
  + The law is actually contextual to time. Good law students know what ‘the law’ was at different times
  + Struggles between interests e.g. worker vs employers
    - The gig economy: employers are trying to remove all their obligations to employees by technically making them contracted workers. This removes all the pros that come with being an employee (sick pay, annual leave, guaranteed hours etc.) whilst the company still gets all the value out of you.
  + Some other stuff, see the slides, he didn’t elaborate
* Features of the legal system
  + Criminal cases
    - You’re charged with a particular very specific offence
  + Civil cases
    - State not involved other than facilitating it via courts
    - Individual vs individual
    - Individual vs company
    - Company vs company
    - Regulatory body vs company
    - Etc.
  + Sources of law
    - Jurisdiction gives you context, state law vs federal etc.
    - Contract is a deal between us, we don’t need to consult the law. Contracts need to be non-unilateral though and one party can’t have the power to change it at will. Contracts were the power balance is so bad are able to be thrown out by courts.
    - Credit act 1984, unless the bank does the right thing they can’t charge interest. Huge class action lawsuit. The banks lobbied against it to change it from a law to a code, because a code cannot be enforced, and they want all the power. Credit act abolished, now have a credit code. Codes are more like conventions.
  + There is no right answer, whoever argues their side best wins
* The 3 wings of the government
  + Executive
    - “the government”
    - It is what **uses** the legal powers i.e. we’ve passed the budget act, we’re spending all this money OR we’ve passed the metadata retention law and now we’ll force ISP’s to maintain all data on Australians
  + Legislature
    - Parliament/congress
    - Makes the laws (statutes)
  + Judiciary
    - The courts and judges
    - Make decisions on individual disputes using the current laws
* What matters?
  + Liability and enforcement
    - Everyone breaks copyright but no one really gets caught (they were liable, it just wasn't enforced)
    - just because you get away with it, doesn't mean it wasn't legal
    - just because it is okay today, doesn't mean it will be okay tomorrow
    - just because they charged you, doesn’t mean they have to charge everyone else who was also liable
* **Rule of law**
  + No one if above the law (Donald Trump thinks he is)
  + The 3 wings of government should be separate, especially the legislature and executive parts.
  + Natural justice (also see the side specifically on it that was skipped if you need more info)
    - If you are accused of something, then you need to know what it is and the facts of the situation
    - And you have the right to present your side
    - If someone just says “we’re locking you up for 10 years for doing x”, then you might want to say “I didn’t do x” or “10 years is too much”. Either way you need to have your say.
    - Watch “natural justice – tech fail” and see that slide if you need it. Should at least mention app stores and their lack of natural justice though
  + Court decision is binding
    - You cannot refuse to implement the decisions that the legislature make. The whole system starts to collapse if this occurs too much, which is currently happening in the US.
  + Statutes interpreted by known principles
    - This is why we have lawyers, we need people that we can ask “is it legal if we do this?”
  + All interests and arguments must be taken into account
    - Lots of civil liberties bodies in Australia appealed to parliament about weakening or removing meta-data retention laws. They has a good argument, showing the downsides of metadata retention and referencing it being cancelled in the US and EU, but the committee on intelligence and security intentionally went out for lunch and missed it because it wasn’t in their interest.
  + Restraint on arbitrary power
    - Protection against tyrants
  + If you don’t like it, it can be changed
* Risk was skipped
  + Only thing mentioned was negligence, you may not have meant to kill someone or cause a huge tech blackout etc. but you still did it because you weren’t careful enough
* Professional liability
  + One of the big things is you can be struck off, there’s membership and you cannot work if you are on that list. If you get struck off as a doctor then you cannot work as a doctor ever again, time to go elsewhere. It’s very exclusive, and you cannot just claim to be part of the group, you must be registered with whatever official body represents that group.
  + Self-regulation
    - All members of the group are regulated by the group. Example of psychiatrist clearly giving the wrong meds to a high risk patient due to incompetence which led to their death. They would either be severely limited in what they’re allowed to practice or expelled from the group.
  + Professional indemnity insurance
    - If you do stuff up, you likely won’t have the means to cover the fallout. Insurance that you get from being part of the group will pay it for you, but not before they severely audit you to check whether they should.
  + Peer attitudes
    - There are acceptable standards and there are unacceptable ones. The group will deem what is what, and you must only use acceptable standards.
    - If your style of coding is to hack together solutions because you’ve generally be smart enough to do so and the ramifications have never been major, then you might be shocked if you applied that to a airliner company because your hacky solution could cause real planes to crash. They would decide that hacky styles of coding are not allowed, and you’d be told to find another profession.
    - You may think waterfall is good, but agile might actually be better.
    - Software is so plastic
    - Vs architecture where we’ve known how to build buildings that are structurally sound for hundreds of years, and so if you build a building that collapses due to poor design then you’ll probably be kicked because you haven’t met the acceptable standards for that industry

PART B – Dataveillance / Uberveillance – Government and Corporation ‘Surveillance Economy’

* Data protection, data security, privacy, confidentiality
* The discussion around online surveillance has been around for 30-40 years, there have been some losses and wins for data protection, the key takeaway from this section is to be able to get a feel for the history and evolution and perhaps future of these issues so that we can identify the past issues of a particular firm/industry sector or project that we may be working on and whether the area is at risk in the future or not.
* Why should we care about privacy?
  + PR usually attempts to say “if you’ve got nothing to hide then you’ve got nothing to fear”
  + But we need to be aware about what can happen at the extreme cases if we give up our data privacy
* Critical view of governance and oversight
  + A lot of these problems aren’t at the individual level, especially the significant ones.
  + Of more concern is government departments, companies, and international organisations who don’t have adequate protections of data in place.
  + FATF Financial Action Task Force, an international coordinating body for financial tracking bodies of different countries. OzTrack, the financial tracking body for Australia said that FATF isn’t interested in data minimization or data protection, they’re basically just cops and so they want more and more data. Ends up being data maximization with no specific focuses on data privacy.
  + OzTrack introducing the encryption of financial transaction data until it passes a threshold for suspicion, at which point it’s unencrypted. This shows the technological capabilities are there for data privacy but it’s not applied universally, and it’s only being applied so they can say “don’t worry that we’re now monitoring everyone”.
* Snowden, whistleblower that revealed a huge data retention and analysis issue in the US, perpetrated by the NSA. It also showed how, because our world is connected via the internet, dataveillance issues of one country can actually affect people from other countries because their data can pass through the country that is sucking up all the data.
  + They were trying to use it to catch criminals but it was shown to be very ineffective and so the breach of privacy that it created was deemed very unjustified and it was ultimately shut down.
* Covid-safe app
  + It doesn’t track location, but it does track proximity, which is very useful for social network analysis (who knows who, who was in who’s house at 3am, who was hanging around the drug dealer etc.)
  + They talked to a lot of entities in Australia to figure out how to protect the data and ban it (legally) from being used for other purposes.
  + This doesn’t stop spies from using it though.
  + The app uses a centralised token server. Every 2 hours each app gets a new token, and it is this token that is shared between app instances that are in close proximity to one another, not phone numbers. This token is partially de-identified which means reidentification is a potential issue.
  + **Concept of proportionality** – is it working? how many people has it notified? Is that amount worth the potential privacy concerns.
  + As the data is partially de-identified via tokens, you can have someone analyse the data to see how many people have ever logged in, how many have logged in today, when was the peak hour login etc. This allows us to gauge how beneficial the app is, but they seem very reluctant about doing this.
  + This is probably because if you reveal that only a small amount of people are using it, people will stop using it all together – a self-fulfilling prophecy. If you say lots of people are using it, more people are more likely to use it.
  + If people become aware of how ineffective it is, it would become even more ineffective because people would stop using it altogether. On the other hand, telling them it is working would lead to more people using it, and it may actually end up succeeding.
  + You’re lying to them though if you say that. If they find out then you’ve lost all credibility for the future (tarnished representation)
  + Uninformed or coerced consent. You say you have read and understand the terms but really you haven’t because it is too inconvenient to, and so you’re actually just a victim of a formality.
  + Informed consent is the gold standard! It’s not enough to get their consent, they need to understand all possible ramifications. He uses the example of the eye doctor who didn’t tell his patient that operating on one of her eyes may cause both eyes to go blind even though he knew this could happen, and it did end up happening. She may not have agreed to the procedure if she was aware of this.