Teesside University

Information Governance CIS3005

LEGAL & ETHICAL ISSUES

School of **Computing, Engineering & Digital Technologies**

Introduction

- This week we will be looking at legal issues, specifically targeted at the scenario in the ICA:
  - Data Protection
  - Intellectual Property
  - Computer Misuse (?)
  - Vicarious Liability (tort of negligence)
  - Also give a few pointers regarding the ICA
- We will also be addressing the concept of ethics
- All of these are HUGE areas in their own right, we are barely going to begin scratching the surface, but it should highlight some issues you might want to discuss in your assignment
- This lecture will feed into L0s 3, 4, 6 & 8

Data Protection

- Current Legislation is the Data Protection Act 2018, it sits ***alongside*** the GDPR (see ICO)
- Its probably the closest thing we've got to Privacy legislation in this country
  - Also Article 8 Human Rights Act
- *"The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default',"* (see ICO)

GDPR 7 Key Principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- **Integrity and confidentiality (security)**
- Accountability
  - Accountability is a new principle when compared to the provisions of the old DPA – "*This specifically requires you to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply.*"
  - Do you think there might be a link here with ISO27K?

Some Data Protection issues to consider

- Processing "Personal Data" according to the DPA.
- What are the possible implications to a company of not complying with the DPA/GDPR?
- What is special category data?

Intellectual Property (IP)

- Current Legislation is the Copyright, Designs and Patents Act 1988
- IP is “intangible property” & so has value like any material/physical property
  - Can be exchanged for something of equal value & also be bequeathed in a will
- Let's dispel some myths first:
  1. “If it hasn’t got the © symbol then its not copyright protected and I can use it” – NO!
     a) Copyright is ***automatic***, you just have to be the author and that the work is “original” under the terms of the Act, unless there is a statement to the contrary you need to assume that the work is protected
  2. “I need to register my work in order for it to be protected by copyright” – Really? Where?
     a) See statement above
     b) There are organisations (e.g. https://copyright.co.uk/ who will record evidence that you produced your work, for a fee of course
        a) This might help in a legal dispute over originality, but is **not** a legal requirement

Intellectual Property (IP) - Ownership

Ownership v important – *owner* makes the money

- Employee?
  - Employer owns it - s.11(2) CDPA states: "*Where a literary, dramatic, musical or artistic work **[**F1, or a film,**]** is made by an employee in the course of his employment, his employer is the first owner of any copyright in the work subject to any agreement to the contrary*"
- Freelancer?
  - Freelancer owns it – would be expected assign the copyright over as part of the contract
  - This is done by a legal doc known as a **Deed of Assignment** (e.g.)

Intellectual Property (IP) – Ownership Contd

- 2 types of legal action in English law:
  a) Civil law – claimant has to sue
  b) Criminal law – defendant is prosecuted by the Crown
- E.g. (1) - If there was a dispute over authorship/originality of some or all of computer code and perhaps someone produced a very similar product (known as a "look and feel" case) it would be up to wronged to *sue* the other party
  - Damages may be awarded
- E.g. (2) – If someone acquired the code/product and started to sell copies of it to other people then under s.107 of the CDPA they would be liable to arrest (by police) and prosecution (CPS)
  - Offender could be fined or go to jail

Some issues to think about IP & ICA

- Could an ISO27K certified ISMS help in protecting this IP?
  - What controls could you use?

Computer Misuse

- Talking about the Computer Misuse Act 1990 here – 5 offences listed:

1. 1. Unauthorised access to computer material.
2. 2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. 3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
4. 3ZA. Unauthorised acts causing, or creating risk of, serious damage
5. 3A. Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA

Hacking

- If the company were hacked by an outsider, they would have to report this to the police – it's up to them, not the 'hacked' company, to investigate and bring the criminals to justice (how important is this to discuss?)
- Hopefully they would have adequate policies, procedures and disaster recovery planning in place to prevent the impact from being too serious
- What about an employee with authorisation to access the system but who abused it?
- Case law (an important legal concept) is important here:
  - R v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America (on Appeal from a Divisional Court of the Queens Bench Division)

Vicarious Liability (?)

- Who would be liable if one of the company's employees was negligent in the computer code they wrote, and this resulted in the death or injury of a member of the public?
- Various examples of death and injury caused by driverless cars:
  - https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html
  - https://www.wired.com/story/teslas-latest-autopilot-death-looks-like-prior-crash/
  - Latest case update: Tesla settles lawsuit over 2018 fatal Autopilot crash of Apple engineer
- *"Vicarious liability refers to a situation where someone is held responsible for the actions or omissions of another person. In a workplace context, an employer can be liable for the acts or omissions of its employees, provided it can be shown that they took place in the course of their employment."* (ACAS)

Morrison's data breach case – very important

- In 2014 disgruntled employee leaked entire company payroll database onto the internet & leaked to journalists
- He was prosecuted for offences under the Fraud Act & jailed for 8 years
- Employees took Morrisons to court for not protecting their data and won in the High Court and the Appeals Court
- Morrisons appealed yet again to the Supreme Court (making it a very important case)
- 2020 Supreme Court ruling – did not find Morrison's vicariously liable for the data breach, but said that in similar cases each should be judged on the facts

What are “Ethics”?

- “Moral principles that govern a person's behaviour or the conducting of an activity.”
- “Ethics is based on well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues.” (Markkula Center for Applied Ethics)
- Is there a difference between “morality” and “ethics”?
  - Morality: “Principles or habits with respect to right or wrong conduct. While morals also prescribe dos and don'ts, morality is ultimately a personal compass of right and wrong.”

What does it mean to work "ethically"?

- Many professional bodies have Codes of Ethics:
  - ISSA (Information Systems Security Association) NB this is a "community" not a professional body, but looks reputable), https://www.issa.org/issa-code-of-ethics/
  - GIAC (Global Information Assurance Certification) https://www.giac.org/about/ethics
  - IEEE: https://www.ieee.org/about/corporate/governance/p7-8.html
  - BCS (The Chartered Institute for IT): https://www.bcs.org/category/6030

White, grey and black hats

White hat hackers: sometimes known as “ethical hackers”. May even have done an Ethical Hacking course. Usually thought of as hackers who on finding a vulnerability in a system will notify the developer first in order to allow them to fix it. Should only work in a system if they have permission to do so.

Grey hat hackers: may break into systems without permission, but will alert developers to flaws. Does not have malicious ***intent***. E.g. Marcus Hutchins who stopped the Wannacry attack on the NHS in 2017, (NB he has since been arrested in the US charged with developing malware). What about “hacktivists” – where do you think they fit in? May knowingly do harm to a system, but their **intent** is usually some sort of activism.

Black hat hackers: criminals who break into computer systems with *malicious intent*. Some may have started as “script kiddies” who are then trained up to commit more serious offences. Nowadays will probably be part of some organised crime network, offering “services” to customers sometimes complete with SLA!

WikiLeaks

- What is Wikileaks?
- Julian Assange (video) "Why the world needs Wikileaks" (2010) – watch from about 2.10 minutes in
  - Chelsea Manning - leaked 750,000(?) classified & un-classified docs to Wikileaks
  - Reports of damage done is contradictory: No damage or damage
  - Following leaks financial institutions (e.g. Mastercard, PayPal, Bank of America) blocked donations to Wikileaks
    - Did they have the moral right to do this? Should banks dictate who people can pay money to or not? (See Icelandic case)
    - Hacktivist group Anonymous launched "Operation Payback"
  - Also embroiled in 2016 US election campaign after leaking emails from Democratic party
- "is Wikileaks a force for good?" – very mixed - WikiLeaks: not perfect, but more important than ever for free speech, Assange himself doesn't come across as a particularly likeable person (IMHO).

Edward Snowden

- Was an intelligence officer in US who leaked docs to The Guardian newspaper that showed that the NSA & GCHQ were surveilling their citizens
  - No public oversight
  - “indiscriminate invasion of privacy”
  - See documentary “Citizenfour”
  - *“I don't want to live in a world where everything I say, everything I do, everyone I talk to, every expression of creativity and love or friendship is recorded.”*
- What did he achieve? – “The people are still powerless, but now they’re aware”
- Still believes that what he did was for the good
- Did he do the right thing? Is he a “traitor” as some have claimed?
  - Legislation has been passed in US & UK to give some framework to gov surveillance – in UK The “Snoopers Charter” or Investigatory Powers Act 2016 (parts ruled illegal in 2018!)
  - Tech companies forced to take steps to protect and encrypt user data or risk loss of trust

Other cybersecurity ethical dilemmas

- Surreptitious Surveillance on the Internet
- The Vulnerability Disclosure Debate
- Talk Talk data breach #1 & Talk Talk data breach #2
- https://www.theguardian.com/technology/2018/nov/11/alarm-over-talks-to-implant-uk-employees-with-microchips
  - Human microchip implants take center stage
  - Interesting (if somewhat disturbing) UK MoD document: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986301/Human_Augmentation_SIP_access2.pdf
  - Marie-Helen Maras, Michelle D. Miranda, "Augmented body surveillance: Human microchip implantations and the omnipresent threat of function creep", *Technology in Society*, Volume 74, 2023, 102295,
- Huawei controversy
- Facebook's use of *our* data
- Covid-19 – contact-tracing apps

Workplace monitoring

- Good example of ethical dilemma
  - Employers need to prevent theft, ensure safety of employees, protect security of their business assets e.g. data security etc. BUT
  - When does monitoring go too far and compromise an employee's privacy rights?
- Read:
  - TUC – I'll be watching you – What is workplace monitoring?
  - ICO - Employee monitoring – is it right for your business?
- Interesting article: How worker surveillance is backfiring on employers

Resources

- **Videos**:
  - Ethical challenges in Cybersecurity, by Mikko Hypponen (important to watch, only 11 mins long)
  - Cyber Security Seminar - Ethics in Cybersecurity: Three Approaches & Their Challenges, Kevin Macnish (41 mins)
- **Website**:7 security incidents that cost CISOs their jobs
- **Books** (available in the library):
  - "Computer network security and cyber ethics" by Joseph Migga Kizza (available in the library as e-book)
  - "The Ethics of Cybersecurity" by Markus Christen (2020)
- **Journal articles**:
  - Levy, Y., Ramim, M. M., & Hackney, R. A. (2013). Assessing ethical severity of e-learning systems security attacks. *Journal of Computer Information Systems*, *53*(3), 75–84. https://doi.org/10.1080/08874417.2013.11645634
  - Landwehr, C. E. (2010). Drawing the Line. *IEEE Security & Privacy Magazine*, *8*(1), 3–4. https://doi.org/10.1109/MSP.2010.35
  - Paul Formosa, Michael Wilson, Deborah Richards, A principlist framework for cybersecurity ethics, *Computers & Security*, Volume 109, 2021, https://doi.org/10.1016/j.cose.2021.102382.
  - Aleksandra Pawlicka, Marek Pawlicki, Rafal Kozik, Micha Choras What Will the Future of Cybersecurity Bring Us, and Will It Be Ethical?; The Hunt for the Black Swans of Cybersecurity Ethics *IEEE access*, 01/2023, Vol 11

Hints & help for your ICA

- Ethical issues – please refer to the document posted in Bb which will give you some links and reading to help you address this part of the ICA
  - Please make sure that, at the very least, you look at the professional body Codes of Ethics linked to in the doc
- Make sure that you reference all legislation correctly – 'Cite them Right' tells you how to do this
  - hint – look under the correct tab!
- What's wrong with the following phrase in an assignment?
  - Everyone has been hacked at some point
  - Be clear about the differences when citing something that is "common knowledge" and what needs supporting with evidence (i.e. a reference)
- Please make sure that you read the Guidance for completing parts 2,4 & 5 on Bb

Conclusion

This week we have looked at:

- Data Protection legislation (in the context of the ICA)
- Intellectual Property issues
- Computer Misuse Act
- Vicarious Liability

- All of which *can* be included in your legal issues discussion
  - Depending on your word count you may need to be selective in what you include – remember we want depth rather than breadth in your reports
- Next week we will be looking at Disaster Recovery management
- In the final week, I will be doing an ICA Q&A during the lecture time to answer any questions you may have but there will be no formal lecture as such