

KV6002 Team Project

LSEPI & Security

The Royal Academy of Engineering funded a Visiting Professorship in Practical Cybersecurity Insights at Northumbria University, 2019–2022. These slides are a slightly modified version of those delivered, intended to be available after the project has ended

© 2019–2022 University of Northumbria at Newcastle *and* Green Pike Ltd

Web <https://green-pike.co.uk/nvp>

Email p.brooke@northumbria.ac.uk (until it stops working. . .)
phil@green-pike.co.uk



Today

- L Legal
- S Social
- E Ethical
- P Professional
- Issues

and

- security

Who am I?

An “information security professional” with experience in academia, the public sector, consultancy. . .

Generalist computer scientist and software engineer

OED

“The competence or skill expected of a professional.”

All the issues we're about to cover *and* technical competence

Doing the right thing for the right reasons?

Are *you* trustworthy?

Large amount of legislation:

- Forgery and Counterfeiting Act 1981
- **Copyright Designs and Patents Act 1988**
- **Computer Misuse Act 1990**
- **Data Protection Act 2018** (a.k.a. –but not only– EU GDPR)
- Freedom of Information Act 2000
- Copyright, *etc.* and Trade Marks (Offences and Enforcement) Act 2002
- **Communications Act 2003**
- Fraud Act 2006
- Wireless Telegraphy Act 2006
- Identity Cards Act 2006/Identity Documents Act 2010
- Investigatory Powers Act 2016

- Data Protection Act 2018
Later in these slides — DPIAs and the implications for security
- Copyright Designs and Patents Act 1988
Covers some (but not all) intellectual property rights (in E&W)
Much related international law and conventions, e.g., Berne Convention

- Computer Misuse Act 1990
Provides for offences of unauthorised access, facilitation, supply tools for misuse, impairment of operation, . . .
- Communications Act 2003
s125 “Dishonestly obtaining electronic communications services”
s127 “Improper use of public electronic communications network”

Is our legal system “ethical”? Is it “just”?

Ethics Explicit, philosophical reflection on moral beliefs and practices. Ethics is a conscious stepping back and reflecting on morality

Morality first-order beliefs and practices about good and evil by means of which we guide our behavior

- ① *Should* you take into account societal issues?
- ② Do we —as IT professionals— just implement systems or do we consider what they are for...?
 - *Should* we?
 - Consider:
 - “Digital by default”
 - Exclusion of communities or groups
 - Potential for abuse
 - Potential for social good

Examples

- 1 Facial recognition
A useful biometric for access control? Surveillance? *cf.* use by British police forces or China?
- 2 ANPR
Parking systems? Detection of crime?
- 3 Medical consultations online
What if you don't have a smartphone?
(Is a smartphone the right tool?)
- 4 Online advertising, how much should we track users?
cf. Belgian data protection authority's decision on IAB Europe and the "Transparency & Consent Framework (TCF)"
https://www.theregister.com/2022/02/02/europe_iab_decision/
...what about GPU fingerprinting?!

Some questions to ask yourself:

- How could this project go wrong?
- How could the product / components be misused or abused?

What assets are involved?

- DPA 2018, incorporating UK GDPR, is sometimes subtle
- Is *personal data* involved?
 - Is *special category* personal data involved?
 - Consider a data protection impact assessment (DPIA)?
 - Legal basis for processing. . .
- There is lots of guidance from the ICO
- Not just personal data — intellectual property, operationally sensitive content

Security controls

- Is encryption-at-rest required?
- Is encryption-in-transit required?
- How are users created and authenticated?
- Are databases required? What will they store and where?
How is access controlled?
- Where is source stored?

Consider the previous points... and then read

- 1 the BCS¹ Code of Conduct
<http://www.bcs.org/category/6030>
- 2 the Engineering Council's Code of Conduct
<https://www.engc.org.uk/engcdocuments/internet/website/Guidance%20for%20Institution%20Codes%20of%20Conduct%202017.pdf>
- 3 the Engineering Council's policy statement on whistleblowing
<https://www.engc.org.uk/engcdocuments/internet/website/Whistleblowing%20Policy%20Statement.pdf>

¹The British Computer Society (BCS) is the most relevant professional body for this course.

Nearly the end

Web <https://green-pike.co.uk/nvp>

Email p.brooke@northumbria.ac.uk (until it stops working...)
phil@green-pike.co.uk



Your projects!

- What do they involve?
- What LSEPIs are important?
- What security issues might arise?

Talk to me! Send an email, can arrange calls via Teams