CyBOK
www.cybok.org

CyBOK: Law and Regulation Knowledge Area

Robert Carolina

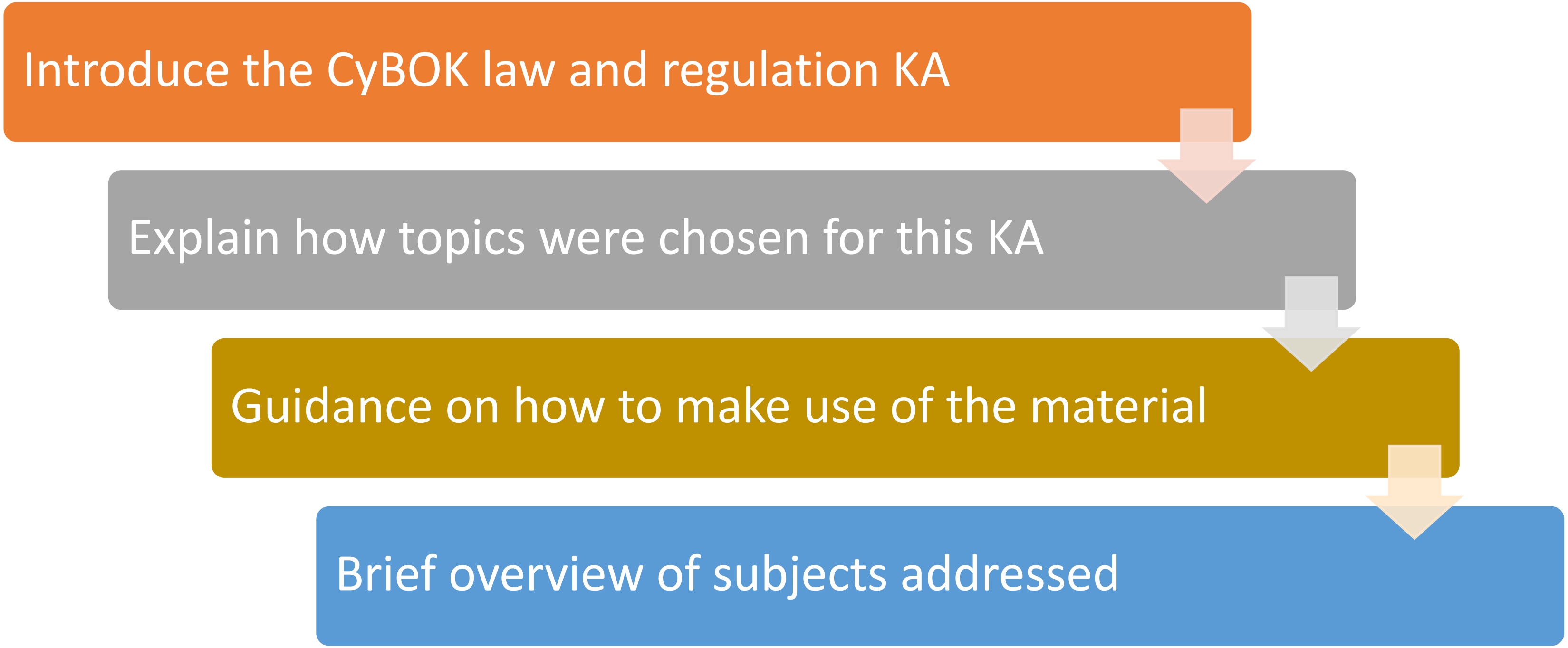
Information Security Group
Royal Holloway, University of London

CyBOK
www.cybok.org

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

NOTICE AND DISCLAIMER:
Both the CyBOK law and regulation knowledge area and this webinar do not constitute the provision of legal advice or legal services and should not be relied upon as such. The work is presented as an educational aid for cyber security practitioners. Opinions expressed are solely those of the author. This work does not represent official policy or opinion of the NCSC, the government of the United Kingdom, any state, any persons involved in its production or review, or any of their staff, employers, funders, or other persons affiliated with any of them.

About this webinar



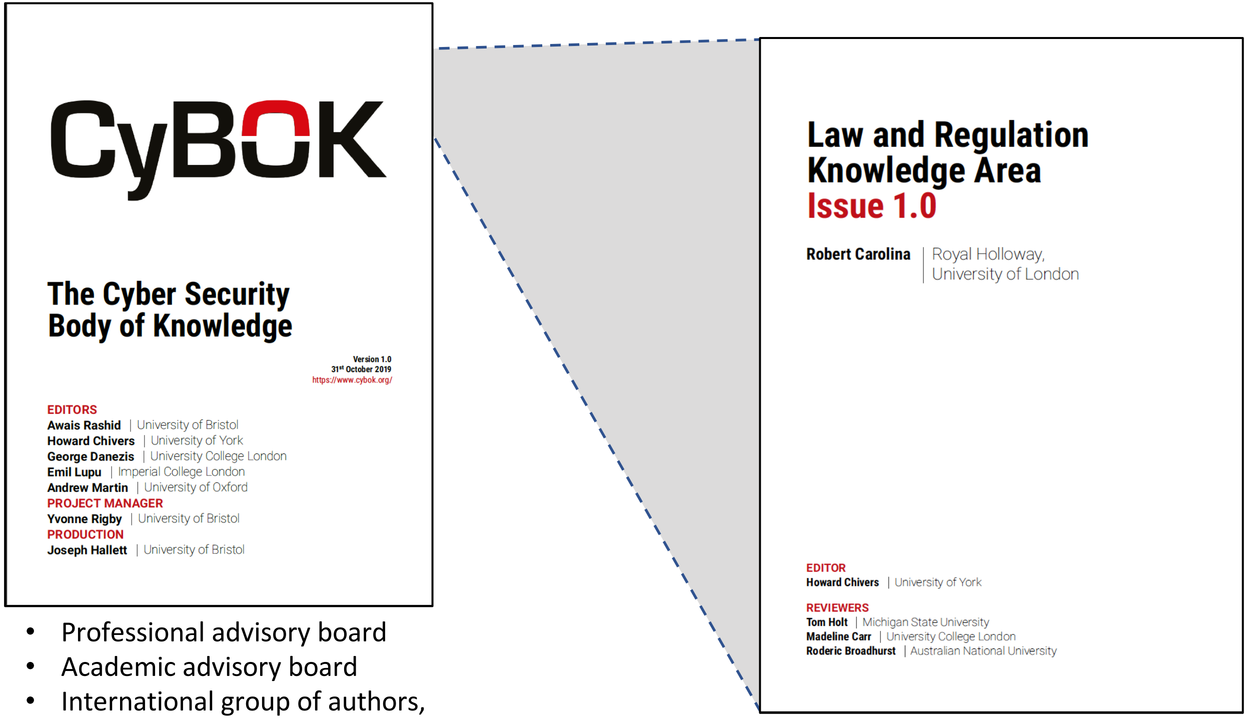
Introduce the CyBOK law and regulation KA

Explain how topics were chosen for this KA

Guidance on how to make use of the material

Brief overview of subjects addressed

CyBOK



CyBOK

The Cyber Security Body of Knowledge

Version 1.0
31st October 2019
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
George Danezis | University College London
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
PROJECT MANAGER
Yvonne Rigby | University of Bristol
PRODUCTION
Joseph Hallett | University of Bristol

Law and Regulation Knowledge Area
Issue 1.0

Robert Carolina | Royal Holloway, University of London

EDITOR
Howard Chivers | University of York

REVIEWERS
Tom Holt | Michigan State University
Madeline Carr | University College London
Roderic Broadhurst | Australian National University

FREE to download
www.cybok.org

- Professional advisory board
- Academic advisory board
- International group of authors, editors and reviews
- Public comments
- Feb 2017 – Oct 2019 v1.0
- Knowledge areas: 19
- Pages: 854 (20 MB pdf)
- Sources cited: 1839

- KA number 3 of 19
- Pages: 112 (0.7 MB pdf)
- Sources cited: 269

Law and regulation KA Contents

Introduction

1. Introductory principles of law and legal research
2. Jurisdiction
3. Privacy laws in general and electronic interception
4. Data protection
5. Computer crime
6. Contract
7. Tort
8. Intellectual property
9. Internet intermediaries – shields from liability and take-down procedures
10. Dematerialisation of documents and electronic trust services
11. Other regulatory matters
12. Public international law
13. Ethics
14. Conclusion: legal risk management

Cross-reference table

End notes (15 pages)

References (12 pages)

Acronyms

Glossary

Introduction

Challenges

Universality

- CyBOK is presented to practitioners globally
- Science and mathematics are universal
- BUT… laws and regulations are local; they differ from place to place

Scope

- Broad scope of activities identified as “security” practice leads to broad scope of legal issues

Accessibility

- Make the subject matter accessible to non-lawyer security practitioners

Response

High level overview

- Review branches of law that address practitioner responsibility, liability, and degrees of freedom
- Identify some generalisable legal norms
- Introduce issues of professional responsibility & ethics

Goals

- Framework for thinking about law
- Help identify issues of concern
- Provide guidance in the search for answers
- Describe law “as it is”, not “as people wish it would be”

Out of scope

- Subjects that are difficult to generalize globally.
- Examples:
  - Rules of evidence
  - Rules of civil procedure
  - Rules of criminal procedure
  - Criminal content laws

How to use this Knowledge Area

FIRST…

- Review key definitions (glossary)
  - person, legal person, natural person
  - state
  - territory
  - legal action, right of action
- Read Introduction
- Read sections 1 & 2
  - Principles of law and legal research
  - Jurisdiction

THEN…

- Read individual subject areas in sections 3-12 as needed. Road maps to help:
  - search for better answers
  - ask better questions
  - understand and apply the answers you find
- Read sections 13-14
- N.B.
  - ‘Alice’ and ‘Bob’ are persons, not devices
  - Read the end notes
  - Use the references for further research

1. Introductory principles of law and legal research

Basic principles

Dynamic

- Law influences society
- Society influences law

Degree of uncertainty

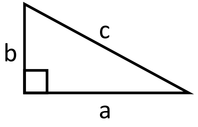
- Finding a definitive statement of “the law” is a difficult research task
- Differing sources, and methods of interpretation

Cyber environment

- Law is (mostly) about addressing the responsibility of persons, and the disposition of property
- Law is territorial; a reflection of society
- There’s no such place as cyberspace
- Laws do not recognise AI as a person

“To prove” something

- Mathematics
  - Establish, as a logical necessity, undeniability
  - Establish a truth beyond dispute



$$a^2 + b^2 = c^2$$

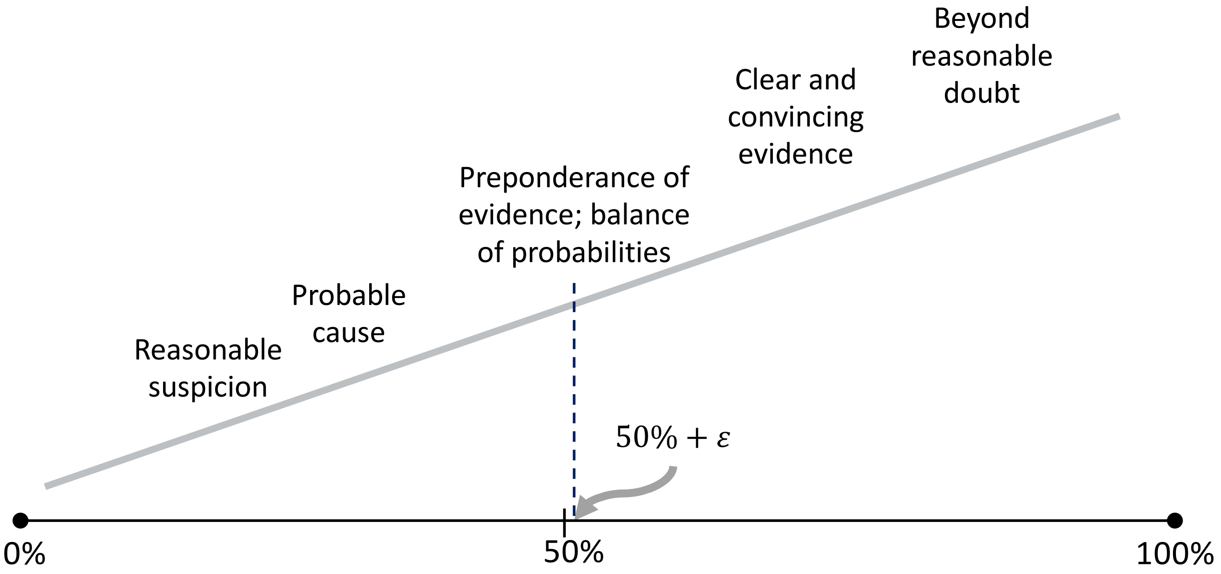
– Pythagoras (c.5th century BCE)

- Law
  - Using permissible evidence, persuade a tribunal of the correctness of a disputed issue
  - Some uncertainty is inevitable

“[Col Jessup ordered the ‘Code Red’?] That's great! … And of course you have proof of that? … It doesn't matter what I believe! It only matters what I can prove [to a jury]!”

– LTJG Kaffee, A Few Good Men (1992)

“Standards” of proof



Degree of "certainty" of the fact finder after examining allowable evidence

Assessing legal risk

Consider a function:

$$R = f(P, D, Q, X)$$

R = the risk-weighted cost to Bob that Alice will commence and win a legal action against Bob;

P = Alice's relative ability (using admissible evidence) to prove her prima facie case against Bob (adjusted by Bob's ability to rebut such evidence);

D = Bob's relative ability (using admissible evidence) to prove any affirmative defence that might reduce or eliminate Bob's liability (adjusted by Alice's ability to rebut such evidence);

Q = the total cost to Bob (other than transaction costs) if Alice pursues and wins her legal action; and

X = a variety of additional factors, such as Alice's willingness and ability to commence legal action, Bob's willingness and ability to defend, Alice's ability to secure enforcement jurisdiction over Bob or his assets, plus transaction costs such as investigation costs, legal costs, and court costs

2. Jurisdiction

Multinational environment

Degree of multinational contact

- The internet enables unprecedented routine contact between persons in different states

State priorities

- Each state is interested in applying its own laws for the benefit of its residents and nationals

Triggers three legal topics

- Jurisdiction: scope of state authority [s.2]
- Private international law, aka conflict of law:
  which state law(s) will apply when parties are connected to different states [ss.6, 7, 8, 10]
- Public international law: regulation actions among and between states at times of peace and during armed conflict [s.12]

A taxonomy of jurisdiction

Prescriptive jurisdiction	Authority asserted by a state’s law makers to regulate activity
Juridical jurisdiction	Authority asserted by a tribunal to decide a dispute
Enforcement jurisdiction	Authority of a state to enforce its will – its ability to project power over persons and property

Prescriptive jurisdiction

- Extraterritorial
  - Lawmakers routinely adopt laws that apply to people and activities outside the territory of their state
  - Various theories adopted by courts to endorse this practice (e.g., effects doctrine)

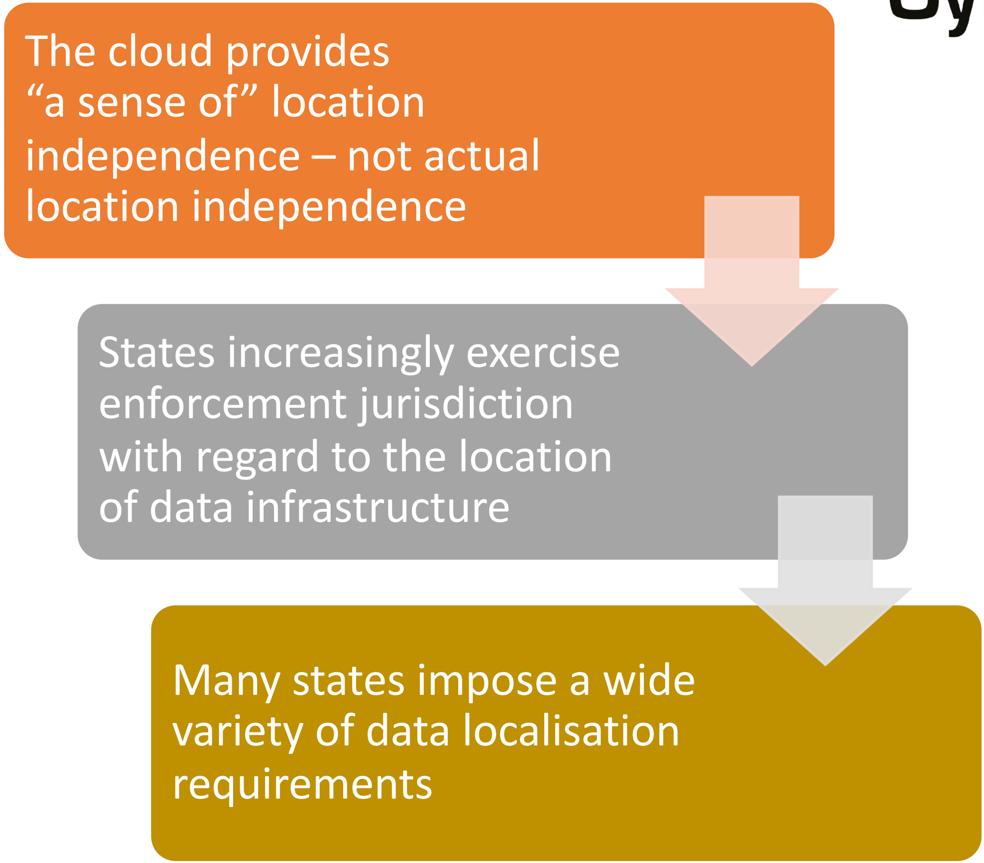
- Examples include laws that apply to
  - Offshore content visible in-territory
  - Offshore hackers who attack in-territory systems
  - Offshore data controllers who process personal data related to in-territory data subjects

Enforcement jurisdiction

- Domestic asset seizure and forfeiture
- Domestic seizure and forfeiture of servers and domain names
- “Location” of a bank account
- Foreign enforcement of domestic civil judgments

- Arrest while present in state
- Extradite from foreign state
- Technological means to filter content geographically
- Orders addressed to domestic persons to produce data (wherever located) under their control
- International legal assistance

The data sovereignty problem



The cloud provides "a sense of" location independence – not actual location independence

States increasingly exercise enforcement jurisdiction with regard to the location of data infrastructure

Many states impose a wide variety of data localisation requirements

3. Privacy laws in general and electronic interception

Privacy basics

Strong international agreement

- Privacy is a human right
- Scope: includes private physical space and electronic communication
- Right to privacy is conditional – not absolute

Lack of international agreement

- Scope: where/when/how should you expect privacy, and to what degree?
- What conditions justify an invasion of the privacy you can normally expect?
- What process is used to decide when and how those conditions are fulfilled?
- What differences, if any, apply to intrusions by the state (e.g., police, security services) and by non-state actors (e.g., employers, parents, service providers)

State interception (lawful access)

- Legal systems heterogenous
- Some international agreement on technical standards
- State follows its law governing access (US is complicated by federal system)
- Service providers typically required to invest in facilities and provide technical assistance
- Varying degrees of secrecy

Non-state interception

- Legal systems heterogenous
- Restrictions sometimes vary with relationship with target
  - Most people usually prohibited from intercepting messages in a public telecommunications service (see also anti-computer intrusion laws)
  - People who operate a private system (employers, etc) are usually given some flexibility to intercept traffic, subject to a variety of legal rules

4. Data protection

Data protection generally

What is it

- Restrictions on collection, disclosure, and use of “personal” data
- European Union law (GDPR) currently the most influential example

More than “privacy”

- Data protection law attempts to vest some measure of control in the hands of living “data subject” about the manner in which “their” personal data is used.

Opinion

- Data protection law is a reaction to the birth and growth of the modern administrative nation-state and modern enterprise

The “players”

Player	Definition
Data Subject	The (living) natural person to whom that personal data relates
Data Controller	A person (natural or legal) who controls the dissemination of the personal data
Data Processor	A person (natural or legal) who merely processes personal data at the instruction of a Data Controller

What is regulated?

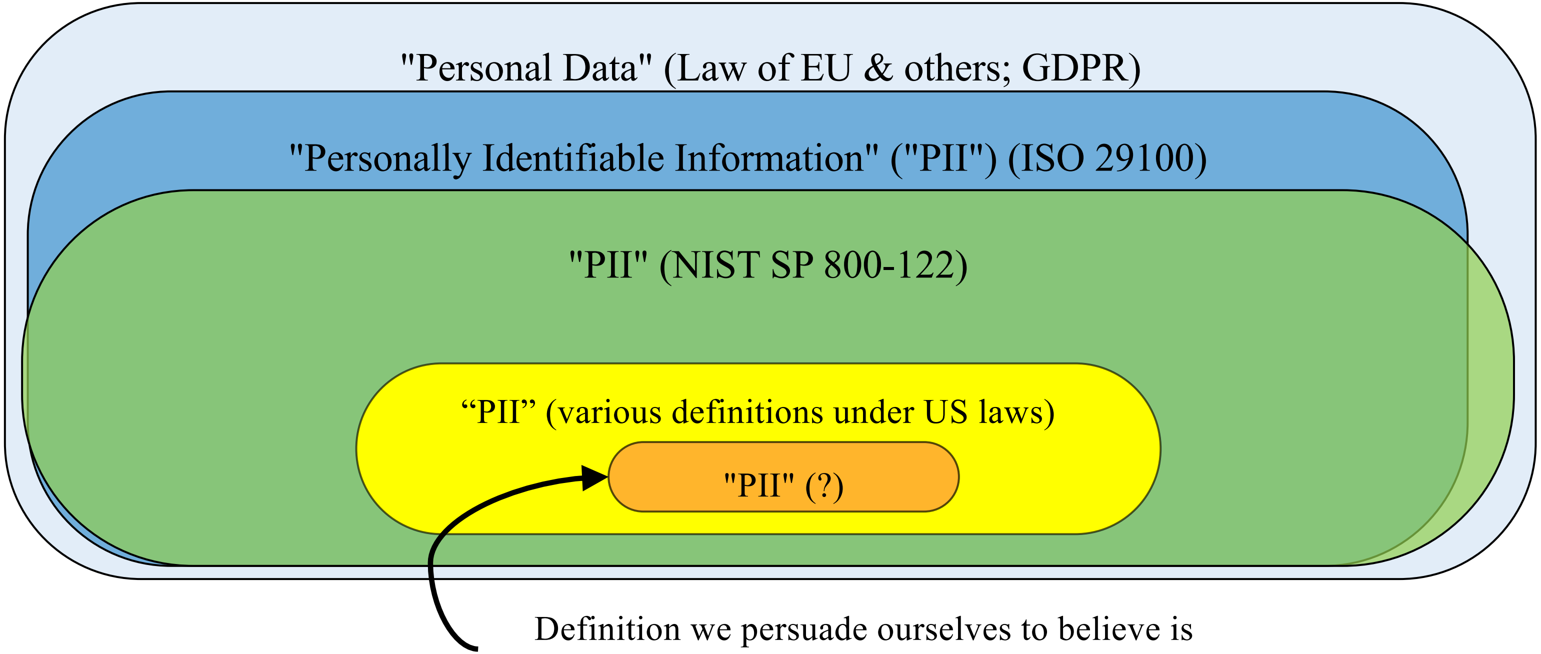
“Processing”

- “any operation … performed on personal data…, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”
  – GDPR Art4(2) (nearly identical to Directive 95/46)

“Personal data”

- Data concerning a living individual
- Includes data that is **capable of being attributed** to a living individual **by any person**, even if that person is unknown to you (e.g., pseudonymous data, encrypted data, data capable of de-anonymisation, etc.)

“Personal data” vs “PII”


"Personal Data" (Law of EU & others; GDPR)
"Personally Identifiable Information" ("PII") (ISO 29100)
"PII" (NIST SP 800-122)
“PII” (various definitions under US laws)
"PII" (?)

Definition we persuade ourselves to believe is correct after multiple committee meetings

CyBOK

Data protection highlights

- CORE DATA PROTECTION PRINCIPLES
- INVESTIGATION AND PREVENTION OF CRIME
- APPROPRIATE SECURITY MEASURES
- ASSESSMENT AND DESIGN OF PROCESSING SYSTEMS
- INTERNATIONAL DATA TRANSFER
- DATA BREACH NOTIFICATION
- ENFORCEMENT AND PENALTIES – ESPECIALLY GDPR

5. Computer crime

Taxonomy of computer crime

Instrumentality [out of scope]

- The Internet is merely the means used to commit crime
- E.g., financial fraud, conspiracy

Content [out of scope]

- The crime is based on message content
- E.g., pornography, hate speech

Crimes against information systems

- Crime is addressed to infrastructure itself
- E.g., unauthorised access to a computer

Crimes against information systems

IMPROPER ACCESS TO A SYSTEM

IMPROPER INTERFERENCE WITH DATA

IMPROPER INTERFERENCE WITH SYSTEMS

IMPROPER INTERCEPTION OF COMMUNICATION

PRODUCING HACKING TOOLS WITH IMPROPER INTENTIONS

Recurring challenges

- [Lack of universality]
- [Extradition]
- De minimis exceptions and measuring harm
- Warranted state interception
  - (also public international law)
- Research and development by non-state persons
  - Uninvited remote technical analysis
  - Covert threat analysis
- Self-help
  - Software locks
  - Hack-back

6. Contract

Contract

IS a legal relationship between persons

IS NOT a piece of paper

Privity
(common law systems)

Contract as means to encourage security behaviours

Whose behaviour?

- Supply chain
- Participants in trading/payment systems

Typical mechanisms

- Promises to comply with security standards (ISO 27001, PCI DSS, etc)
- Promises to notify counter-parties of incidents
- Promises to grant audit rights

What's at risk?

- High: loss of the value of trade/payment
- Medium/low: loss of relationship, legal action for breach of contract

Limits of influence

Cost of breach

- Low quantum of provable loss (Q) lowers risk-weighted cost of breaching contract (R)
- Disappointed party not willing to pursue legal action influences (X), lowers (R)
- Problem of privity, “flow down” of responsibility
- Disappointed party not willing to terminate relationship

Examples

- Party can’t prove security violation caused financial loss
- Limitations of liability: non-cognisable losses, limitations and exclusions imposed by contract clauses, etc
- No credible alternative source of supply

Relative influence of contract over security behaviours

Strong influence

- Security is a foundation for reducing some much larger commercial risk of the behaving party
- Contract supported by external regulation
- E.g., payment systems

Medium influence

- Security is the subject matter of goods or services supplied by the behaving party
- E.g., security-related devices and services

Weak influence

- Security is an encouraged feature, but not core to success of behaving party
- E.g., supply of “routine” software, hardware, SaaS, IaaS, other goods & services, etc

7. Tort

Tort

Civil wrong other than breach of contract

Based on principles of social responsibility; relationship between parties can be involuntary

Requires the person who commits a tort (tortfeasor) to compensate the victim

Tort examples

Negligence (s.7)

Strict liability for defective product (s.7)

Intellectual property infringement (s.8)

Violation of data subject rights under data protection law (s.4)

Many others (out of scope)

Negligence (fault based liability)

Duty of care

- Under what circumstances are we responsible to others?
- Core concept: foreseeability
- Cybersecurity examples in Table

Breach of duty

- What does it mean to act “unreasonably”?
- What if the environment changes?
  “Common practice is not the same as reasonable practice”

$$B < PL$$

Negligence (fault based liability)

Static framework, dynamic results

- Foreseeability expands with experience
- “Reasonable” is grounded in society’s expectations
- These change over time
- These differ by society
- Warning : Tortfeasor may be held to the standards of the territory where the victim is located

Product liability (strict liability)

Core idea

- Product manufactures (and/or relevant supply chain partners) should compensate victims who suffer death or personal injury caused by product defects
- Focus of “fault” moves from person to product

Increasing relevance

- IoT creating more use cases where cybersecurity failures can lead to personal injury or loss of life (from self-driving automobiles to remote-control thermostats)
- Definition of “product fault” may be linked to consumer expectation of safety

Limited to “products”

- This standard would not apply to supply chain partners who supply a defective software-only component

Quantum of loss (Q)

Causation of victim’s provable loss

- Especially challenging for victims of data loss events
- Difficulty valuing privacy

Statutory schedule of damages

- Lawmakers impose fixed amounts

Punitive / exemplary damages

- Intended to punish especially careless behaviour or indifference to human suffering (mostly USA)

Attributing and apportioning liability

Vicarious liability

- “Morrison Supermarkets” case (2018) was recently overturned by UK Supreme Court (April 1, 2020)
  - YES, vicarious liability can apply in data protection law
  - BUT, this Morrisons employee was off on “a frolic” and not acting within scope of employment

Joint & several liability

- Small % of joint responsibility can lead to 100% of liability

CyBOK

8. Intellectual property

Intellectual property basics

- Negative rights
  - Each IP right is a type of “red card” that says stop doing a defined action
  - Owning IP does not guarantee freedom to act

- Short catalogue
  - Copyright
  - Patent
  - Trademark
  - Trade secret

Reverse engineering

Traditionally accepted as normal behaviour

- Does not invalidate patent or copyright protection
- Destroys trade secret

Challenges from copyright law

- Anti-circumvention of copyright protection technology

Testing trade secret security method

- Megamos Crypto case
- Intersection with “responsible disclosure”

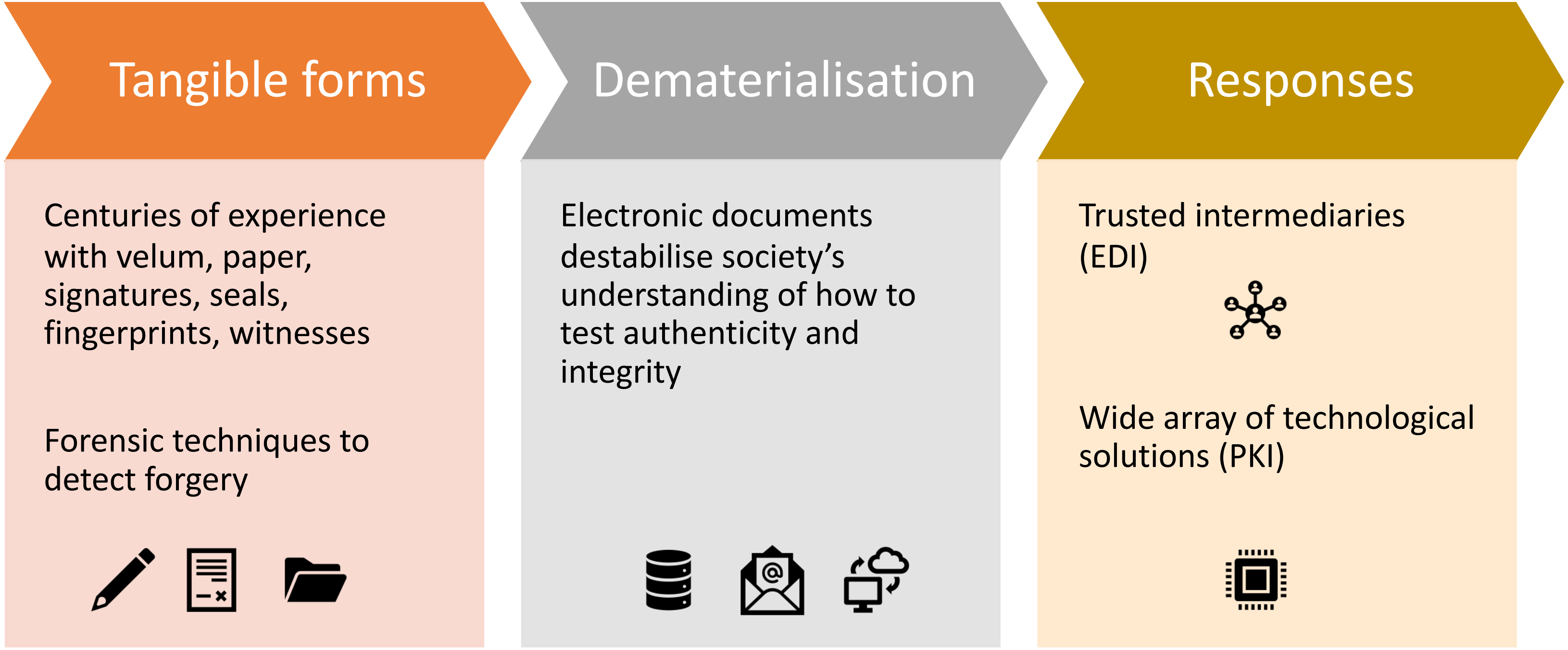
9. Internet intermediaries - shields from liability and take-down procedures

Intermediary liability shields

- Basics
  - Shields a qualifying person who would otherwise be liable for offending message content
  - Originally designed to shield ISPs and telcos
  - Increasingly contentious (e.g., US FOSTA-SESTA)
  - Ongoing debate re social media and search platforms
- Take-down / blocking
  - As a condition of shield protection, some qualifying persons are required to take down offending content “expeditiously” after notice from complaining person
  - Others not subject to take-down notice may be ordered by state (judiciary or executive) to block or filter traffic

10. Dematerialisation of documents and electronic trust services

Background: assuring authenticity and integrity



Tangible forms

Centuries of experience with velum, paper, signatures, seals, fingerprints, witnesses

Forensic techniques to detect forgery

Dematerialisation

Electronic documents destabilise society's understanding of how to test authenticity and integrity

Responses

Trusted intermediaries (EDI)

Wide array of technological solutions (PKI)

Legal challenges emerge

- ADMISSIBILITY INTO EVIDENCE
- REQUIREMENTS OF FORM
- ELECTRONIC SIGNATURE
- IDENTITY TRUST SERVICES

11. Other regulatory matters

Subject matter regulation

Industry-specific regulation

- E.g., financial services, professions, regulated utilities
- NIS Directive

Consumer products

- Regulation
  E.g., EU Cybersecurity Act, US FTC
- Standards
  E.g., ETSI TS 103 645, IoT

Dual use product restrictions

- Export/import restrictions, use restrictions
- Free speech
  Junger v Daly (USA 6th Cir, 2000)

State secrets

- Applied to state insiders
- Imposed on others

12. Public international law

Principles of international law

Exists among and between states (including IGOs)

- Sources: Treaties, custom, norms, decisions of international tribunals
- Enforcement: States often enforce using self-help (i.e., counter-measures)

Application to cyber operations

- Most states acknowledge international law applies to cyber operations, but they don’t necessarily agree how
- Tallinn Manual 2.0: world’s leading source of expert analysis on application of international law to cyber
- Territorial principle

State attribution

- Legal standard (substance)
  - Act by a state agent
  - State encourages or directs act by a non-agent
  - Failure to exercise “due diligence”

- Forensic process (process)
  - Gathering and presenting evidence for use when making a legal attribution analysis

Limiting operations

- Prohibitions
  - Violation of sovereignty
  - Use of force
  - Armed attack
- Counter-measures
  - Must be proportional
  - Cyber or non-cyber

- Law of armed conflict
  - Military necessity
  - Humanity
  - Distinction
  - Proportionality

13. Ethics

The case for codes of conduct

- Position of trust
- Out of the glare of public scrutiny
- Special knowledge and skills
- Asymmetric power in client relationship
- Potential to harm members of the public

Codes of conduct

What makes a good code?

- Detailed guidance on how to interpret and apply principles
- Addresses the relationship between practitioner and client, between practitioner and society, and how to balance these
- Adoption and support by a well-defined community of practitioners

Examples worthy of study

- ACM Code of Ethics and Professional Conduct (2018)
- CREST Code of Conduct

Vulnerability testing and disclosure

Testing

- Lack of consensus on the difference between “research” and “computer crime”

Disclosure

- Lack of practitioner consensus on process of “responsible” disclosure, and potential of indefinite delay to publication
- Ongoing discussion of state security agencies (balancing equities, responsible release, etc)
- Bug bounties and other efforts to monetise vulnerability

Vendor action

- Some consensus on what should be done (e.g., ISO 29147, ISO 30111)
- But lack of ubiquitous implementation

14. Legal risk management

When thinking about future operations, consider:

$$R = f(P, D, Q, X)$$

- Subject matter areas of greatest risk
- Impact on human life
- Due diligence aligned with risk
- Practical limits of enforcement jurisdiction
- Costs of breaching (non-criminal) obligation
- Risk to personal liberty, safety, and reputation
- Likelihood of enforcement
- Challenges of collecting preserving and presenting evidence
- Vicarious liability
- Localising risky activity in separate legal persons
- Risks external to legal enforcement system
- Changes in law or policy likely to arise

CyBOK
www.cybok.org

CyBOK: Law and Regulation Knowledge Area

Robert Carolina

Information Security Group
Royal Holloway, University of London