CyberSecurity: the legal dimension

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE

National Laws and Regulation Governing Cyber Defence, Cyber Effects and Cyber Attack

- **There are no laws which address these issues directly. We have:**
- **UK Criminal Law and Procedure**
- **International Treaties on co-operation in criminal matters**
- **International "laws of war" (treaty obligations)**
- **UK "laws of war" (lawful commands)**
- **UK Intelligence Services Act, 1994**

LSE

- **Criminal enforcement is only part of the story in tackling cybersecurity**
  - ➔ It refers to punishment via the courts
  - ➔ It requires admissible evidence
- **This lecture / seminar / workshop is not legal advice**
  - ➔ The aim is to give a policy overview
  - ➔ For advice in specific circumstances – consult a lawyer

LSE

- Substantive Law
- Investigations and the Law
- International Framework
- Future Policy

Substantive Law

- Computer Misuse Act 1990 is *fill-in* legislation; the whole of the criminal law is available for use in charging cyber crimes
- CPS prosecuting policy is to aim, where ever possible, for the substantive offence, not the *modus operandi*
  - ➔ Fraud, Money Laundering, Extortion, Terrorism, etc etc

LSE

Substantive Law

Fraud Act, 2006

- By false representation (s 2)
- Possession of articles for use in fraud (s 6)
- Making or supplying articles for use in fraud (s 7)

Money Laundering

- Proceeds of Crime Act, 2002; Serious Organised Crime & Police Act, 2005
- Almost any possession of monies or assets derived from illegal sources, including those obtained innocently + failure to disclose knowledge or suspicion

LSE

Substantive Law

Extortion / Blackmail

- **S 21 Theft Act 1968 (unwarranted demand with menaces)**
  - ➔ **14 years + confiscation**

Substantive Law

Indecent Images of Children

Protection of Children Act, 1978, s 160 Criminal Justice Act, 1978 (as amended)

Extreme Pornography

S 63 Criminal Justice & Immigration Act 2008

Intellectual Property Piracy

Copyright Designs & Patents Act 1988, s 107

Trade Marks Act, 1994, s 92

LSE

Substantive Law

Terrorism

- **Terrorism Act, 2000**
  - ➔ Definitions, interpretation
  - ➔ Fundraising
  - ➔ Possession of articles connected with etc etc
  - ➔ Powers: arrest, stop & search
- **Anti-Terrorism, Crime & Security Act, 2001**
  - ➔ Terrorist cash & property, disclosure powers, toxins, police powers, retention of communications data
- **Prevention of Terrorism Act, 2005**
  - ➔ Control orders etc
- **Terrorism Act, 2006**
  - ➔ Encouragement of terrorism, publications, preparation, training
- **Counter-Terrorism Act, 2008**
  - ➔ Post-charge questioning, powers over those subject to control orders, money laundering, DNA database

LSE

Substantive Law

Computer Misuse Act 1990 (amended P&JA 2006)

- S 1: Unauthorised access (12 months)
- S 2: Unauthorised access with intent to commit a further crime (5 years)
- S 3: Unauthorised data modification / with intent to impair (10 years)
- S 3A: "hacking tools" / making or supplying (2 years – can also use s 7 Fraud Act 2007)

LSE

Investigations and the Law

- PACE and other powers to seize, Police Act 1997 etc
- Intelligence Services Act 1994
- Human Rights Act 1998
  - ➔ Necessity and proportionality tests
- Data Protection Act 1998
  - ➔ Protection of personal data
- Regulation of Investigatory Powers Act 2000
  - ➔ Interception
  - ➔ Communications data
  - ➔ Decryption Powers
  - ➔ Directed and Intrusive Surveillance
- Codes of Practice
  - ➔ PACE
  - ➔ Regulation of Investigatory Powers (Covert Surveillance and Property Interference: Code of Practice) Order 2010
  - ➔ Interception
  - ➔ Covert Human Intelligence Sources

LSE

Investigations and the Law

Examination of Computers, Cellphones, data media

- Powers to seize under PACE and many other laws
- Computer forensics well advanced
- Findings
  - ➔ Substantive Files, Emails, web traffic etc
  - ➔ Recovery of deleted files
  - ➔ Chronologies of activity
  - ➔ Evidence of research, planning etc, *mens rea*
  - ➔ Evidence of "bad character" under s 98 ff CJA 2003, CPR 35

LSE

Investigations and the Law

Production Orders

- Banking records
- Telephone records etc
- S 9 PACE 1984, sch 5 Terrorism Act 2000, s 22 Crime (International Co-operation) Act 2003, s 345 *ff* Proceeds of Crime Act 2002 (s 349 covers information in a computer)

Investigations and the Law

Interceptions and Communications Data under RIPA

- Part I Chapter 1: Interception of Content
  - ➔ Warrant from Home Secretary
  - ➔ Inadmissible, intelligence use only
- Part I Chapter 2: Traffic Data
  - ➔ Self-authorised by law enforcement but also many other "authorities"
  - ➔ Admissible
- Part II: CHIS - Covert Human Intelligence Sources
- Part III: Encryption

LSE

Investigations and the Law

Interceptions and Communications Data under RIPA

- **Data Retention**
  - ATSCA 2001
  - Data Retention Directive 2006/24/EC
  - Data Retention (EC Directive) Regulations 2009 (12 months)
  - Reference to ECJ?
- **Private Networks:**
  - Employment Practices Data Protection Code, 2005
  - Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

LSE

Interception Evidence: Emails

- Traffic Data, Not Content
- Admissible: email headers (but not "subject") caught in transit
- Inadmissible: email content
- Admissible: emails found on computer hard-disks
- Inadmissible: email content on ISP mail-servers unless there is proof of delivery

LSE

Interception Evidence: Web-browsing

- Traffic Data, Not Content
- Admissible: material found in internet cache (or associated recovered data)
- Admissible: traffic data caught at ISP's facilities
- Inadmissible: content caught at ISP's facilities
- Where does traffic data end and content begin?

LSE

Interception Evidence: P2P, IM, Chat, etc

- Traffic Data, Not Content
- Does your investigatory method amount to interception?
  - ➔ Not if you are a participant, because you can consent
  - ➔ But you will need authorisation for intrusive or covert surveillance (RIPA Part 2)
- Forensic artefacts found on computer: admissible as real evidence
- Chat logs… ???

LSE

Interception Evidence: Cloud Services

- Traffic Data, Not Content
- In transit: how do you separate content from communications data?
- Forensic artefacts found on computer: admissible as real evidence
- Jurisdiction: location of remote server(s)

LSE

Interception Evidence: VOIP

- Traffic Data, Not Content
- Practical problems of how to intercept – H.323, SIP, Skype
- Suppliers may not be able to provide a full intercept capability because protocol is P2P
- If you can intercept – almost impossible to separate traffic data from content and still be forensically sound ….
- Local config files: admissible

LSE

Interception Evidence

Disclosure issues

CPS Disclosure Manual Guidance:

- **http://www.cps.gov.uk/legal/section20/chapter_a.html#147**

Part of the skill of the forensic practitioner is to find admissible alternatives to initial evidence that may be inadmissible!

LSE

Investigations and the Law

Participation in “underground” online communities

- Possible and admissible under Police Act and RIPA
- CoP – subject to necessity and proportionality tests
- Investigator participants must not act as *agent provocateurs*
- Important to maintain full audit trail of activity
- Used by CEOP, SOCA +++ ???

LSE

Investigations and the Law

Covert entry into suspect computers

- **Local entry: s 10 CMA – law enforcement powers**
  - → **Covers unauthorised access but not unauthorised data modification**
- **Remote entry using trojan:**
  - → **Police Act, 1997, Part 3; s 5 Intelligence Services Act 1994.**
  - → **Potential breach of s 3 CMA (does s 10 apply?)**
- **Practical problem: defence accusations that data has been altered to "improve" a case**

LSE

Investigations and the Law

Power to require decryption key

- **Part III RIPA (extended in Terrrorism Act 2006)**
- **Used against Animal Rights activists and suspected child abusers ++++ ???**
- **Police give notice with a disclosure requirement, subject declines, jury must be satisfied:**
  - ➔ **There is encrypted material**
  - ➔ **Subject has key or means of decryption and is deliberately withholding ("I have forgetten" defence)**
- **Punishment is usually less than for the suspected offence (5 years for "child indecency", 2 years for everything else)**

LSE

Investigations and the Law

Keyloggers

- 2 types:
  - ➔ Hardware (between keyboard and computer)
  - ➔ Software
- Hardware: Police Act, 1997, Part III
- Software: RIPA, possible CMA problem
  - ➔ S 10 CMA covers police against unauthorised access but not data modification – which is what the deployment of a keylogger or back-door involves

LSE

Investigations and the Law

Disclosure

Disclosure: Principles

Every accused person has a right to a fair trial, a right long embodied in our law and guaranteed under Article 6 of the European Convention on Human Rights (ECHR). A fair trial is the proper object and expectation of all participants in the trial process. Fair disclosure to an accused is an inseparable part of a fair trial.

What must be clear is that a fair trial consists of an examination not just of all the evidence the parties wish to rely on but also all other relevant subject matter. A fair trial should not require consideration of irrelevant material and should not involve spurious applications or arguments which serve to divert the trial process from examining the real issues before the court.

A-J Guidelines

LSE

Disclosure: History

- **Common Law disclosure: the "materiality" or "relevance" test – *R v Keane (1994) 99 Cr. App.R 1***
- **Concern about "fishing expeditions"**
- **CPIA 1996 placed a duty on:**
  - ➔ ***Prosecutors*** **to disclose**
  - ➔ ***Defence*** **to provide defence case statement**

LSE

Disclosure: History

- Under CPIA 1996:
- Primary disclosure based on prosecution case
- Secondary disclosure based on further material arising from defence case statement
- Defence can ask for further information via Court Order on a “relevancy” test
- Amended in Criminal Justice Act 2003, Part 5.

Disclosure: Current Regime

- **Criminal Justice Act 2003, Part 5 (ss 32-40)**
- **Main effects are to tighten up mutual obligations:**
- **Prosecutor must use the might reasonably be considered capable of undermining test; has a continuing duty of disclosure**
- **Requirements for detail (and timing) of defence case statement set out – includes notice of name of any expert giving likely to give evidence. Initial and updated defence statements.**

LSE

Disclosure: Current Regime

- **Criminal Justice Act 2003, Part 5 (ss 32-40)**
- **Main prosecution "punishments": s 78 PACE – evidence is excluded, "abuse of process", costs, defence release from obligation to provide defence case statements**
- **Main defence "punishment" – adverse inferences in trial; may not be able to ask for further disclosure**

LSE

Disclosure: Current Regime

- **Main Practical Guidance: CPS Disclosure Manual**
- **http://www.cps.gov.uk/legal/section20/chapter_a.html#003**
- **http://www.lslo.gov.uk/pdf/disclosure.doc (Attorney-General's Guidelines)**
- **But:**
  - **These are not, strictly speaking, Law, but Guidance**
  - **CPS Manual directly binds CPS, law enforcement**
  - **But not the courts, nor the defence**

LSE

Practice

- all police officers have a responsibility to record and retain relevant material
- the officer in charge of the investigation has special responsibility
- Role of disclosure officer - duties

Practice

- investigations into crimes that have been committed
- investigations whose purpose is to ascertain whether a crime has been committed, with a view to the possible institution of criminal proceedings and
- investigations which begin in the belief that a crime may be committed. For example, a surveillance operation is part of an investigation even if it is directed to a target without there being a specific offence in mind.

Intelligence ops may become disclosable, subject to PII – need for regular review

LSE

Practice: Withholding

- **Sensitive Material Disclosure**
- **Public Interest Immunity (PII)**
  - → **Application to Court**
  - → **Ministerial Certificate**

The disclosure officer must describe on the MG6D any material the disclosure of which he or she believes would give rise to **a real risk of serious prejudice to an important public interest** and the reason for that belief. This form will not be disclosed to the defence.

LSE

Practice: Withholding

- the ability of the security and intelligence agencies to protect the safety of the UK
- the willingness of foreign sources to continue to cooperate with UK security and intelligence agencies, and law enforcement agencies
- the willingness of citizens, agencies, commercial institutions, communications service providers etc to give information to the authorities in circumstances where there may be some legitimate expectation of confidentiality (e.g. Crimestoppers material)
- the public confidence that proper measures will be taken to protect witnesses from intimidation, harassment and being suborned

LSE

Practice: Withholding

- the safety of those who comply with their statutory obligation to report suspicious financial activity
- national (not individual or company) economic interests
- use of covert human intelligence sources, undercover operations, covert surveillance etc
- the protection of secret methods of detecting and fighting crime
- the freedom of investigators and prosecutors to exchange views frankly about casework.

Initially: Prosecutor's Decision, Court finally decides!

LSE

Practice: Withholding

Disclosure Test:

- the nature and strength of the case against the accused
- the essential elements of the offence alleged
- the evidence upon which the prosecution relies
- any explanation offered by the accused, whether in formal interview or otherwise
- what material or information has already been disclosed.

LSE

CPIA: Implications for Investigators

- Retain, Record, Reveal
- Decisions about Disclosure are not for you – but you must facilitate them
- When you give evidence: your over-riding duty is to the court

LSE

International Dimensions

- Mostly on the basis of bilateral MLATs (Mutual Legal Assistance Treaties)
- Interpol / Europol
  - ➔ Facilitators, research
- CoE Cybercrime Convention (Treaty of Budapest) 2001
  - ➔ Harmonises definitions of cybercrime and procedure; 24/7 network
  - ➔ UK has signed but not ratified
  - ➔ Some nations have concern about impact on sovereignty

LSE

Law Reform?

- Breach Reporting Law
- Increased ICO Powers & Penalties
- Extension of s 10 CMA to s 3 CMA
- Criminal Procedure Rules / Expert witnesses
- Interception Modernisation / RIPA /admissibility

Interception Modernisation / RIPA

- Reform necessary because of the many new forms / protocols of communication on the Internet
  - ➔ Web-based interfaces: emails etc
  - ➔ Message / Chat services
  - ➔ Apps – Apple, Android, Blackberry, Symbian
  - ➔ Cloud Services
- Where is the data held?
  - ➔ Jurisdiction
- CSPs are required to have an interception capability but interpreting the “content” / “data communications” distinction increasingly difficult
  - ➔ In practice you have to capture the whole data / packet stream and then apply rules *post hoc*

Interception Modernisation / RIPA

- Does this mean that most requests will have to be for interception warrants?
  - ➔ Implications for role of Home Secretary
- Implications for inadmissibility of intercept evidence
- What happens to data retention?
  - ➔ Current data retention is confined to communications data
  - ➔ Implications for proportionality under Human Rights
- Implications for operational procedures
- Implications for costs
- Will LE have to expect less from interception?

LSE

National Laws and Regulation Governing Cyber Defence, Cyber Effects and Cyber Attack

- Juridification of war
- What happens if a government feels that its people are being attacked
- It has intelligence it believes is reliable about identity of attacker
- It lacks legally reliable evidence / does not want to disclose investigatory methods / believes it will not get proper legal support from the jurisdiction from which the attack is being made
- ???

LSE

CyberSecurity: the legal dimension

Peter Sommer

London School of Economics, Open University

peter@pmsommer.com

p.m.sommer@lse.ac.uk

LSE