Cybercrime, digital investigations & cloud computing

Professor Ian Walden
Institute of Computer and Communications Law
Centre for Commercial Law Studies, Queen Mary, University of London

Multi-disciplinary Cooperation for Cyber Security, Legal and Digital Forensics Education Project

December 2014-March 2016

BIRMINGHAM CITY
University

Queen Mary
University of London

Introductory remarks

- Cybercrimes
  - Criminalising behaviours
- Digital investigations
  - Computer & device forensics
  - Network forensics
    - Investigatory Powers Bill
- Cloud computing
  - Contracts
  - Service level agreements

CYBERCRIMES

Defining cybercrime

- Council of Europe Cybercrime Convention (2001)
  - 'Budapest Convention': some 56 signatories, from Europe & beyond
    - Harmonisation of offences & criminal procedure
    - Enhance international co-operation
- 'old wine in new bottles' or 'new wine in no bottles'?
  - Computer-related crimes, e.g. fraud
  - Computer-integrity crimes, e.g. hacking
  - Content-related crimes, e.g. child sexual abuse images
  - Contact-related crimes, e.g. harassment

Computer integrity offences

- Cybercrimes
  - Unauthorised access, e.g. ‘hacking’
  - Unauthorised interference, e.g. viruses & malware
  - Unauthorised interception: e.g. ‘snooping’
  - Illegal devices
- Criminalizing conduct & fault, not the technology
- Legal analogies & physical reality
- Over-criminalization
- Imposing obligations on (potential) victims
  - Prevention being better than cure.....

‘Unauthorised’

- Legal definitions
  - Limits of entitlement
- Implied limits
  - By conduct of perpetrator
  - By conduct of victim, e.g. ‘controller’ of resource
    - Code-based
- Operation of law
  - Public law
    - Jurisdictional limits
  - Private law
    - Employee usage, terms of service, licence conditions

Authorisation

- UK: Computer Misuse Act
  - "entitled to control access of the kind in question to the program or data" s. 17(5)
    - *DPP v Bignell* (1998)
    - *R v Bow Street Magistrates' Court, ex parte Allison* (1999) 3 WLR 620
    - *DPP v Lennon* [2006] All ER (D) 147 (May)
  - Law enforcement: s. 10 *Savings*
    - Amendments for access (1994) & interference (2015)
    - CDPA, s. 296ZB(3) re: circumvention of technological measures
- US: CFAA 18 USC § 1030(e)(6)
  - "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;"

Unauthorised by statements

- *US v Drew* (2009) U.S. Dist. 259 F.R.D 449; (CD Cal. Aug 28, 2009)
  - "if every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution."
    - So 'void for vagueness', as 'ordinary people….would not expect criminal penalties..'
- Legal nature of the statement
  - Contractual
    - e.g. terms of service in contracts of adhesion
    - Statutory controls may render the agreement invalid: a first issue to be decided upon
    - Directive 13/40/EU, recital 17
      - "contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service,…should not incur criminal liability"

Access what?

- Cybercrime Convention – Art 1(a) defines 'computer system' and 'computer data'
  - any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
    - Guidance Note # 1, 'On the notion of "computer system" – Article 1.a Budapest Convention on Cybercrime', T-CY(2012) 21
  - Directive 13/40/EU
- Devices, programmes & data (electricity)
  - 'without right'
    - "access, interference, or interception, which is not authorised by the owner or by another right holder of the system *or of part of it*"
  - Impact of licence breach?

Illegal Access

- Mere access: Computer Misuse Act 1990, s. 1: "unauthorised access"
  - elements
    - *actus reus*: "..causes a computer to perform any function (with intent to secure access to any program or data held in any computer;")
    - *mens rea*: intent to secure access & knows at the time of the *actus reus* that intended access is unauthorised
  - case law
    - *Sean Cropp* (1991): *Attorney-General's Reference (No.1 of 1991)* [1992] 3 WLR 432

Illegal Access +

- ‘by infringing security measures’
  - e.g. Germany, Brazil, Switzerland, Finland, Japan
- Information-related
  - e.g. Data Protection Act 1998, s. 55
    - Obtaining personal data without the consent of the data controller
- Connected systems
  - Budapest: ‘in relation to a computer system that is connected to another computer system’
    - e.g. Japan: ‘specific computer…..via a telecommunications line’
- Target or facility-related
  - 18 USC. § 1030(e)(2): ‘Protected Computer’

Illegal interference

- Integrity
  - Computer Misuse Act 1990, s. 3
    - impair the operation of any computer;
    - prevent or hinder access to any program or data held in any computer; or
    - impair the operation of any such program or the reliability of any such data
  - Intention & recklessness (since 2006)
  - From ‘unauthorised modification’ to ‘unauthorised acts’
    - From ‘contents of the computer’ (internal) to ‘in relation to the computer’ (external) perspective
      - Denial-of-Service attacks (‘DDoS’)
    - **But**, s. 17(6): re: removable data media

Illegal interference +

- Target
  - e.g. ‘Critical information infrastructure’
    - EU Directive, art. 9(4)(c): ‘against a critical infrastructure information system
- Motivation
  - Organised crime
    - EU Directive, art. 9(4)(a): ‘committed within the framework of a criminal organisation’
  - Terrorism Act 2000
    - “designed seriously to interfere with or seriously disrupt an electronic system” (s. 1(2)(e))

Illegal interference +

- Harm-related
  - EU Directive, art. 9(4)(b): 'serious damage'
    - 2015 amendment to Computer Misuse Act 1990: Section 3ZA: 'unauthorised acts
    - Damage of a 'material kind'
      - To human welfare, environment, economy or national security
      - "of any country"
    - 'Human welfare'
      - Including 'disruption of a supply of money, food, water, energy or fuel', 'system of communication', 'facilities for transport' & 'services relating to health'
    - Tariff
      - 14 years to life imprisonment (for serious loss of life or injury)

Illegal interception

- Interception or 'network access'
  - To content (data), not communication attributes
- Data 'in transmission'(-ish)
  - Storage
  - Issues of confidentiality and privacy (relational *not* subject matter)
- As criminal conduct
  - Or commercial practice
- As criminal procedure
  - Controlling law enforcement investigations

‘Without right’

- Authorisation (positive)
  - of the ‘system controller’
    - From criminal to civil liability
    - US: ‘owner or operator of the ‘protected computer’
  - of the network users
    - Consent of both parties (UK: RIPA, s. 3(1), since 2011)
      - EU data protection law
    - Consent of one party (US: 18 U.S.C. § 2511(2)(c)-(d))
  - of law enforcement agencies
    - e.g. warrant

‘Without right’

- Lawful excuse (negative)
  - of the service provider
    - Technical need v commercial desire, e.g. Spam & malware detection; behavioural targeted advertising
      - RIPA, s. 3(3): “for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.”
  - “in the course of lawful business practice”
    - Directive 02/58/EC, art. 5(2)
      - ‘Lawful business practice’ Regulations 2000

Transmissions

- ‘in the course of transmission’
  - Intermediate storage
    - S. 2(7): “....shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.”
      - *Edmondson & ors v R* [2013] EWCA Crim 1026
    - Investigatory Powers Bill, s. 3(4): ‘relevant time’, includes stored data ‘whether before or after its transmission’

Illegal interception

- Regulation of Investigatory Powers Act 2000
  - Offences of unauthorised interception
  - 'Public telecommunication systems'
    - Intentional & without lawful authority: s. 1(1)
      - 2 yrs imprisonment
      - DPP consent required, but no express public interest defence
        - e.g. CPS & Ofcom (Sky News & the Darwins)
    - Unintentional but without lawful authority: s. 1(1A) (2011)
      - Directive 02/58/EC, Art. 5(1) & Recital 21
        - Only applicable to CSPs?
      - Office of the Interception of Communications Commissioner: 'monetary penalty notice' & procedure: £50,000 max.

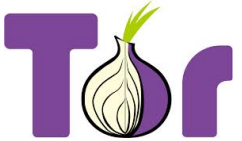
Illegal interception

- 'Private telecommunication systems'
  - Intentional & without lawful authority: s. 1(2)
    - 2 yrs imprisonment
  - Statutory tort: s. 1(3)
    - If system controller or has authority of system controller
- 'System controller'
  - "a person with the right to control the operation or use of the system"
    - *Stanford* [2006] EWCA Crim 258
      - "more then merely the right to access or to operate the system. It meant the right to authorise or forbid the operation or the use of the system"

Illegal devices

- Tools designed to facilitate cybercrimes
  - Devices & data
    - e.g. ‘zero-exploits’, ‘rootkits’, ‘botnets’, ‘key-logging’ software
    - Lowers threshold of skill required
- Crime prevention
  - “prohibit specific potentially dangerous acts at the source, preceding the commission of offences” (CCEM, at para. 71)
- ‘Malicious marketplace’
  - Organised crime



Legal issues

- Criminalising what?
  - Device & data
- Criminal conduct?
  - Inchoate offences
    - Attempt, conspiracy & incitement
  - Supply & possession
    - Export controls: dual use
- Distinguishing lawful from unlawful
  - Scientific research…

UK law

- Computer-integrity offences
  - Computer Misuse Act 1990, s. 3A (2006 amendment)
    - 'Article' includes "any program or data held in electronic form"
    - 3 offences: (i) supplies with intent; (ii) supplies 'believing that it is likely' and (iii) obtains intending to use or with a view to supplying
      - *Invicta Plastics Ltd v Clare* [1976] RTR 251
    - CPS Guidance (requested by Government)
      - Is the article widely available?
      - Is it sold through legitimate channels?
      - Does it have a substantial installation base?
    - Maximum 2 yrs imprisonment