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

DIGITAL INVESTIGATIONS

Introductory remarks

- From criminal code to criminal procedure
  - Including foreign jurisdictions
- Forensics: Obtaining data
  - Computer/device & network forensics
  - Retrieval, analysis and presentation
  - Evidential implications: Presenting data
- Law enforcement powers
  - Ordinary (e.g. surveillance), covert (e.g. interception) and coercive (e.g. search & seizure) policing techniques
    - Calls for new powers
      - Investigatory Powers Bill
    - Human rights concerns: e.g. right to privacy & fair trial

Network forensics

- Obtaining data
  - ‘in transmission’ or ‘at rest’ (but remotely)
  - Content, traffic data & subscriber data
  - Mandatory, voluntary, emergencies & conflicts of law
- Obtaining access
  - From suspect or 3rd party (e.g. a friend)
    - ‘publicly available’ data
  - From ‘service providers’
  - From foreign law enforcement agencies
    - e.g. ‘Five Eyes’

Some data problems

- Identity problem
  - Machine ≠ person
- Availability problem
  - Data logs & data retention
- Knowledge problem
  - e.g. *Atkins & Goodland v DPP* [2000] 2 All ER 425
- Location problem
  - Suspect, data & service provider
- Integrity problem
  - Data & meta-data
- Analysis problem
  - Volumes & time limits
- Protected data problem
  - e.g. Kevin Mitnick

Service providers

- Cybercrime Convention: 'service providers'
  - "any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
  - any other entity that processes or stores computer data on behalf of such communication service or users of such service."
- Explanatory Report
  - 'a broad category of persons'
    - Free or paid; public or private provision
    - Not a mere provider of content, with no "communication or related data processing services"
      - Who is encompassed? Telephony, internet access, OTT, cloud services……

Service Provider Data

- Content
  - 'In transmission' (lawful intercept) and 'at rest' (production orders)
    - "within its existing technical capability" or build 'intercept capability'?
- Communication attributes
  - Cybercrime Convention, art. 1(d): 'Traffic data'
    - "any computer data relating to a communication …. that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."
- Subscriber data
  - Cybercrime Convention, art. 18(3): 'Subscriber information'
    - "other than traffic or content data"
    - Relationship to user?

Identity problem

- Target IP address
  - e.g. 38.111.64.2
  - generated by application being utilised
- IP holder
  - 'whois' enquiry of regional, national or local registry databases
- Logging history
  - e.g. Network Addressing Translation (NATs) and Dynamic Host Configuration Protocol (DHCP) logs held by service provider
    - Retention obligations?
- Subscriber details
  - e.g. Credit card details

Data availability

- Retention for law enforcement purposes
  - Data Retention Directive 06/24/EC: Communication data for 6-24 months
    - Providers of 'electronic communication services'
    - Fixed & mobile telephony, internet access, email & telephony
    - Communication data *not* content
    - "investigation, detection and prosecution of serious crime" *not* prevention
  - Case C-594/12 *Digital Rights Ireland v Ireland* (8 April 2014)
    - Bulgaria (2008), Romania (2009), Germany (2010), Czech Republic (2011), Cyprus (2011)
    - UK: Data Retention and Investigatory Powers Act 2014 & Data Retention Regulations 2014

Data location problem

- Production order (art. 18)
  - Person 'in its territory' or service provider 'offering its services in the territory' with 'possession or control'
    - Rackspace (2013), Verizon (2014)
- Search and seizure (art. 19)
  - "another computer system…in its territory, and such data is lawfully accessible from or available to the initial system… *shall be able to expeditiously extend the search*"
    - Police and Criminal Evidence Act 1984, s. 20 "accessible from the premises…"

Data location problems

- The long arm of law enforcement
  - Microsoft Dublin case (2013 -)
- Solutions
  - Extraterritorial assertions
    - Belgium: Yahoo! case
    - UK: DRIPA 2014
  - Localization requirements
    - Mandated, e.g. Russia & Indonesia
    - Commercial, e.g. Microsoft Azure & Deutsche Telekom (Nov. 2015)
  - Foreign territory, domestic law
    - e.g. Switzerland & diplomatic immunity
    - Estonia Virtual Data Embassy

Foreign data: Location problem

- Convention, Article 32: "A Party may, without obtaining the authorisation of another Party….
  - (a) "access publicly available (open source) stored computer data, regardless of where the data is located geographically"
    - Including where subscription or registration is required
    - Customary international law?
  - (b) "obtains the lawful and voluntary consent of the person who has lawful authority to disclose the data…"
    - Other forms are 'neither authorised, nor precluded'
    - Cybercrime Convention Committee, Guidance note (Feb. 2014)
      - Not applicable "where it is uncertain where the data are located"
      - Cloud contracts & explicit consent?

Protected data

- Protected data problem
  - Apple iPhones: In California (brute force password) & New York (bypass lock screen)
- Access & conversion protections
  - e.g. Cryptography
- Legal response
  - Criminalise the use
  - Require the person to supply intelligible plain-text format;
    - User or service provider
  - Break the protection

Protected data

- Option 1: Criminalise Use
  - Control export, import, use
    - Export control regulations: 'Wassenaar Arrangement'
      - Singapore: Strategic Goods (Control) Order 2013, Schedule, Category 5, Part 2 *Information Security*
      - Breach of regulations is a criminal offence
  - Use in criminal activity
    - e.g. State of Virginia (US), Computer Crime Act at § 18.2-152.15: 'Encryption used in criminal activity'
      - "an offense which is separate and distinct from the predicate criminal activity"

Protected data

- Option 2: Obligations to assist law enforcement
  - Service provider
    - obligation to anything 'reasonably practicable' or to build an 'intercept capability' (RIPA, s. 11)
      - "is able to remove any electronic protection applied by the service provider to the intercepted communication and the related communications data" (SI 1931/2000, Sch. 1, Pt. II, para. 10)
  - Suspect
    - RIPA, Pt III: 'Investigation of Protected Electronic Information'
      - Code of Practice (2007)
      - Disclosure in 'intelligible form'; or delivery-up of 'key'
      - Failure to disclose: 2 yr term (5 yrs for national security & child indecency cases), e.g. *R v Padellec (Pierre)* [2012] EWCA Crim 1956

Rights issues

- Against self-incrimination
  - ECHR Article 6 – 'fair trial'
    - *S and A* [2008] EWCA Crim 2177
  - US, 5th Amendment
    - *Boucher* 2009 WL 424718 (D.Vt.)
- Evidence of offence
  - 'national security', 'child indecency' or 'specified serious offence'
    - *US v Hersh, a.k.a Mario* (2002)
      - Encrypted files on a Zip disk, so F-Secure provided partial source code to identify files names & pre-encrypted byte size
      - Compared files names with LEA database: 120 names matches; 22 byte match

Protected data

- Option 3: Breaking the protection
  - *Ex ante* measures: building 'backdoors'
    - e.g. US 'key escrow' & 'Clipper Chip' (1995)
    - Influencing the standards
      - e.g. Dual EC DRBG standard (Snowden)
  - *Ex post* arrangements
    - Exploiting vulnerabilities
    - Home Office Code of Practice: Equipment Interference
      - *Privacy International* [2016] UKIP Trib 14_85-CH
    - Based more on stolen goods than maths!

Investigatory Powers Bill

- Interception of communications
  - Targeted & bulk
- Acquisition of communications data
  - Targeted & bulk
  - Entity & event data
  - 'internet connection records'
- Retention of communications data
- Equipment interference
  - Targeted & bulk
- Acquisition of bulk personal datasets

CLOUD CONTRACTS

So…..

- What is the customer of cloud services most concerned about?
- What is the supplier's perspective?
- What is an 'SLA'?
- What happens in the event of breach?