

Cybercrime 2009: the Legal Perspective

Lilian Edwards
Professor of Internet Law
University of Sheffield
Lilian.edwards@sheffield.ac.uk

RUSI CyberSecurity Conference
October 2009
London

Categorisations of Cyber Crime

- Lloyd, quoting NCIS report 2003: *“the range of crimes that can be committed, either through or with the support of hi-tech tools is limited only by the imagination and capability of the criminals”*.
 - *Cyber-trespass* - access harms
 - *Cyber-deception/thefts* - acquisitive harms, including
 - *Cyber-piracy* - IP appropriation harms
 - *Cyber-pornography/obscenity*
 - *Cyber-violence* eg of individuals - stalking; of groups - hate speech; terrorist websites
- “New” cyber-crimes have not been too hard to slot in to substantive laws
- Porn “pseudo-photographs”, denial of service, wi-fi theft (Comms Act 2003), phishing
- Much new legislation nonetheless - eg glorifying terrorism, pedophile grooming, extreme porn

UK substantive cyber crime laws

- *Hacking*. Computer Misuse Act 1990, s 1, 2: “unauthorised access” to “program or data”
 - S 17(2) – can include altering, erasing, copying, using, reading any data or program
- *Virus dissemination*. CMA, s 3 – originally “any act which is an unauthorised modification of the contents of the computer”
- *Internet pornography* – POCA78, CJA88, CJPOA94
- *Computers as a tool for fraud*. Common Law, Fraud Act 2006 (phishing).
- “*Glorifying terrorism*” – websites – TA 2006 s 1

Issues: Denial of Service/Botnets

- Did D(D)oS fall under CMA s3?
- Issues : “modification” – impermanence of damage? (tho see s 17(7)); “unauthorised” – emails? Page requests?
- S 3 amended to “act”
- *Lennon case: ““In this case, the individual emails caused to be sent each caused a modification which was in each case an ‘authorised’ modification. “*
- Reversed on appeal 2006 – implied permission does not extend to comms *“sent for the purpose of interrupting the proper operation and use of his system.”* (spam?)

Legal issues for security professionals

- Do user rights to privacy in EU/UK impede investigation?
- Yes, DPD almost certainly regards IP addresses as “personal data” – Art 29 WP and Google/Hustinx discussion
- No this is not an absolute bar to public **or** private investigatory action
 - Consent of user
 - Art 13 DPD allows exemptions to DPD rights & obligations for prevention of crime, & national security (and other reasons)
 - In UK, this crime exemption applies to private actors (eg security consultants) as well as police (cf CCTV). Not true however in all EU.
 - ISP/telco allowed to disclose – DPA 98 s 35 – where required by law or court order
 - Revised PECD may well allow ISPs/telcos across EU to process personal data for security purposes even despite DP
- *Security and DDOS/hacking tools*
 - CMA 90 amended s 3A (10/08 i/f in E&W); supply “believing..likely to be used”

The changing face of cybercrime/cyber insecurity

- ◎ Key issues are around enforcement, evidence, forensics **not** substantive law
- ◎ Cybercrime now not game played by hackers, teens and geeks (mad, sad, not bad) but serious branch of organised crime – the black hat economy.
- ◎ Heavily transnational – main crime gangs organised from Russia, Moldova, etc, only money mules etc` caught locally.
 - ◎ Lack of harmonisation on procedure, evidence, extradition – though see Cybercrime Convention, but sign up poor.
 - ◎ Lack of standing transnational policing agencies (Interpol, Europol?)
- ◎ Tools available online along with help, tutorials etc – no need to be a geek
- ◎ Heavy under reporting of cybercrime esp from industry due to bad PR (though insurance?)– mandatory security breach reporting where personal data breaches is on horizon from EC law

Policing cybercrime in UK

- Previously – NHTCU, some specialist expertise in local policing esp Metropolitan Police.
- NHTCU absorbed into SOCA.
 - *“We used to have huge expertise in IT within the NHTCU. This expertise got very efficiently removed into SOCA, which killed it” : Earl of Errol*
- Left gap for “local” e-crime enforcement – Police Central e-Crime Unit (PCeU) (sub Met Police)– 2008 - £7m initial funding.
- Child porn – hived off to CEOP; IWF for reporting/NTD.
- Financial online fraud – National Fraud Reporting Centre – 2009 (part of City of London Police). Public still encouraged to report to banks first – criticised HL Committee. Action by NFIB.
- One off transnational policing ops, expensive, time consuming, some successes eg pedophile rings, bot herders
- EU – ENISA (8m Euros, 2008)
- A standing international/EU/NATO cybercrime task force?

Future issues in cybercrime

- “Virtual” crime?
 - Attacks on virtual banks – Stross “*Halting State*”
 - Theft of virtual property – E Asian prosecutions
 - Dutch “Habbo Hotel” case
 - Are new laws really needed? Unauthorised access, unauthorised modification, fraud..
 - Likeliest problems; local police disbelief, forensics, access
- The line between cybercrime , cyber terror and cyberwar?

LAW OF CYBER CONFLICT

