PROFESSIONAL COMPUTING

Lecture 2: Legal Perspectives

Dr. Mark Lee | *m.g.lee@cs.bham.ac.uk*
School of Computer Science, University of Birmingham
Autumn 2014

Disclaimer

- Dr. Lee is a :
  - Award-winning lecturer of Computer Science*
  - (not bad) banjo player
  - (pretty good) morris dancer
  - But is not a lawyer (and has not even played one on TV)
  - Caveat Emptor!

* not that I want to talk about this …

Question

A fellow student wishes to model how viruses spread by creating a benign computer virus to be spread via email

Upon infection, the virus asks the user for consent to 1) replicate itself 2) send back confirmation to the student 3) to self delete itself within 7 days of infection.

If the user does not give consent, it instantly disinfects the computer and deletes itself without sending any data or changing any files.

Is this a good idea?

What is the Law?

- This can be a philosophical question …
- “A set of laws which can be enforced by a court”
- Jurisdiction – the geographical area governed by a single set of laws
  - Federal law versus State Law in the US
  - We’ll focus on English law but …
  - Jurisdiction is often not obvious in computer use.

- The Law is more than just a set of “rules”
  - Different systems of courts.
  - Different rules concerning how appeals are made.
  - Different rules about how new laws work with old.

Criminal versus Civil Law

- Criminal Law
  - Designed to protect “society” from wrong doers
  - Police investigation and arrest
  - CPS proceeds with prosecution
  - *“Innocent till proven guilty”*
  - Guilty beyond reasonable doubt

- Civil Law
  - Settling disputes between *people*
  - But companies can become people
  - Litigation must be brought by one of the parties of the dispute (the plaintiff) against another (the defendant)
  - Both parties must present arguments
  - Decision based on “*balance of probabilities”*
  - Usual objective is to obtain damages (money) or injunction (court order)

  - We’ll mostly be concerned with Civil Law in this module

Two examples

- An e-commerce site uses third party software for encryption. Unfortunately the encryption software has a security loophole allowing it to be easily cracked.

- Case 1: the encryption software is developed by a security company who licences it for use to other companies.
- Case 2: the software is cut and pasted from some old lecture notes from an introductory lecture on computer security which explains the loophole…

- A user using the site finds that their bank account details are shared with a criminal gang who swiftly takes their savings.

Who is liable?

Tort

- In Common Law, a Tort is a civil wrong
- The action might not necessarily be illegal (or criminal) but some how has caused harm which can be re-addressed through the courts
- Torts are usually re-addressed through damages awarded
- Negligence
  - Duty of care
  - Dereliction of duty
  - Tortfeasor directly caused the injury
  - Plaintiff suffered damage
  - Proximate Cause
- Nuisance
- Defamation

A brief history of English Law

- ~1086
  - System of Common Law
  - Law is essentially precedent plus common sense by judges
  - Central authority is the court of the King
  - Equity & the Court of Chancery

- 15th century
  - legal power moved from King to Parliament
    - Legislation by political bodies

- 19th century
  - Courts reorganised to combine common law and equity.
  - Legislation becomes more important than common law or equity

Legislation

- A “Legislative Act of Parliament” (or statute) can create, amend, repeal any new or existing law
- Any statute overrules any previous act or precedent (but not court decisions)
- Body of law is regularly reviewed by the Law Commission

- Process
  - Bill is drafted (usually under supervision of government minister)
  - Bill introduced in House of Commons or Lords (but usually passed by both)
  - Several stages of reading and amendment
  - Bill becomes an Act following Royal Assent

European Union

- EEC established in 1957
- Single European Market established in 1992
- Council of the European Union and European Parliament have legislative powers
- Attempts to harmonise laws of the member states
- Growing influence on English Law

- Regulations – directly enforceable by Parliament and English Courts
- Directives – instructions for member states to alter their laws
- Decisions – specific decisions on states, enterprises, individuals

European Convention on Human Rights

- Drafted in 1950, signed 1953
- Generally a “good thing”
- Allows individuals an active role in International Law

- Of particular interest to us:
  - Article 5 Liberty and Security
  - Article 7 Retrospectivity
  - Article 8 Privacy
  - Article 10 Expression

  - Today’s lecture notes might be out of date next year …

Hacking Facebook

- Gareth Crosskey (21, Sussex) hacked a US citizen's facebook account and gained access to an email account in Jan 2011.
- Breach was reported to Facebook who reported it to the FBI
- The FBI traced hack to the UK and then informed UK police
- Crosskey was charged under the Computer Misuse Act (1990,2004)
- Due to evidence presented, Crosskey pleaded guilty and was imprisoned for 12 months in May 2011

http://www.theregister.co.uk/2012/05/17/facebook_account_hacker_jailed/

R v. Gold & Schifreen (1988)

- Gold & Schifreen used home computers and modems in 1984-85 to gain unauthorised access to BT's Prestel viewdata service.
- At a trade fair, Schifreen noted the username and password of a Prestel engineer (22222222, 1234)
- Gained access to personal mail to Prince Phillip among others
- Charged under Forgery and Counterfeiting Act (1981) as defrauding BT using a "false instrument" – the internal condition of BT's computers after it had processed the lifted password.

- Tried and fined £750 & £600 respectively.

Appeal

- Appeal to Criminal Division of Court of Appeal
  - Lack of evidence that defendants had intended material gain
  - Evidence that BT didn't really take security seriously
  - Not really a case of Forgery and Counterfeiting

- Acquited by Lord Justice Lane
- CPS appealed to the House of Lords

- House of Lords upheld the Acquittal –
  - "The Appellants' conduct amounted in essence, …, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for legislature rather than the courts." (Lord Brennan)

Computer Misuse Act (1990)

- Three Offences
  - Unauthorized access to a computer;
  - Unanthorized access to a computer to commit a serious crime; and
  - Unauthorized modification of the contents of a computer.

  - A person is guilty of a crime if either they or the computer in question is in the UK at the time of the offence.

Unauthorized Access Offence

Section1

- A person is guilty of an office if
  - He causes a computer to perform any function with intent to secure access to any program or data held in any computer;
  - The access he *intends to secure* is unauthorised; and
  - He *knows* at the time when he causes the computer to perform the function that this is the case.

  - Punishable by a fine up to £5000 or 6 months imprisonment

Key points:

Knowledge & intent

Attempt is sufficient

No requirement of damage done.

Intent to do serious crime

- Section 2 covers unauthorized computer access to commit a more serious crime.
  - E.g. a blackmailer might hack into email to gain evidence of an affair etc.
  - It is not necessary for the more serious crime to be carried out … as long as intent to do so can be shown.

- Punishment is up to five years imprisonment or an unlimited fine.

Unauthorized Modification

- A person is guilty of an offence if
  - he does any act which causes an unauthorized modification of the contents of any computer; and
  - At the time when he does the act he has the requisite intent and the requisite knowledge.
- Requisite intent covers:
  - To impair the operation of any computer;
  - To prevent or hinder access to any program or data held in any computer; or
  - To impair the operation of any such program or the reliability of any such data
- Maximum penalty is 5 years or unlimited fine.
  - Spreading a virus
  - Encrypting files and demanding a ransom for revealing the key
  - Redirection of browser home pages etc etc.

Review of CMA (2004)

- All Party Review of the Act
- Plus input from professional bodies (e.g. BCS)

- Added an additional offence “impairing access to data”
  - Mainly motivated by DoS attacks

- Increased tariff for unauthorised access from 6 months to two years
  - A sign to show this is a serious crime
  - Now a crime which is extraditable under UK law …

- Despite this, the UK has had relatively few prosecutions under the CMA
  - 32 & 26 successful in 2006
  - 10 prosecutions in 2010
- http://www.theregister.co.uk/2012/05/18/uk_hacking_prosecutions_decline/

Police and Justice Act 2006

- 2004 All Party Intergroup proposed further amendments
- P & J 2006
  - Section 35. Unauthorised access to computer material
  - Section 36. Unauthorised acts with intent to impair operation of computer, etc.
  - Section 37. Making, supplying or obtaining articles for use in computer misuse offences (books? Security tools?)
  - Section 38. Transitional and saving provision

- Following News International Phone Hacking
  - Current discussion about explicit reference to mobile phones with browsers and to what extent these are covered.

Issues surrounding CMA

- Common view is that the real issue with computer crime is a lack of resources for investigation and prosecution rather than a lack of laws
  - Phising for instance is better dealt with as a case of Fraud
- Unfortunately “Fraud” is a unclear term in English law.
  - “Conspiracy to defraud”
  - 8 different types of “deception”
  - Can a computer be deceived?
  - Review is on-going.

- Some instances of DRM might be liable under CMA

Gary Mckinnon

- Scottish citizen (born 1966) & mid-level system admin
- Between 2001 & 02 hacked into 97 US military and Nasa computer systems
  - Claimed to be looking for evidence of UFOs and Free energy suppression
  - Diagnosed with mild autism/aspergers
- The US claims
  - deleted files, copied passwords, closed servers for 24 hours and posted jokes on
  - government websites and BBS
  - Investigation has cost $700,000 plus
- Extradition
  - Interviewed by UK police in August 2002
  - Indicted by Federal Grand Jury in Virginia in November 2002
  - 7 counts of computer misuse, each carrying a ten year tariff
  - 2003 Extradition Treaty with the US does not require the US to provide any evidence of wrong doing
  - Potential of a **70 year** sentence
  - US prosecutors have said that if the charges are uncontested then McKinnon will face a sentence of 36-47 months.
  - Won approval for judicial review of case in 2009 – but this review held the extradition to be legal.
  - Further Judicial Review granted in 2010 due to concerns about suicide risk if extradited.
  - October 2012 – Home Security blocked Extradition to the US
- December 2012 – CPS decided not to prosecute due to difficultly in evidence being located in the US.
- http://freegary.org.uk/ (which now links to Gary's SEO business …)

Summary

- This lecture gave a (very) brief overview of English Law
- English law has historically been based on precedent
- But Legislation has increased
  - This is inevitable due to technological change
  - Most criminal activities are best dealt with as forms of more traditional crime.
  - But some aspects of computer crime are difficult to fit this
  - Computer Misuse Act
- Civil law is probably more relevant to most …
- Copyright, breach of contract, privacy, libel etc. are mostly dealt as civil issues