ECommerce

Computer Science Tripos Part II

International Perspectives on Internet Legislation

Easter Term 2013

Richard Clayton

These lecture notes were specially prepared for the Cambridge University Computer Science "ECommerce" course, Easter Term 2013.

richard.clayton@cl.cam.ac.uk

Outline

- Data Protection & Privacy
  - EU Data Protection
  - US Privacy Laws
- E-Commerce
  - copyright infringement
  - deep linking
  - brands and other web-page issues
  - politics and terrorism
- Crime and policing
  - international policing
  - extra-territoriality &c

The slides give the broad outline of the lectures and the notes ensure that the details are properly recorded, lest they be skipped over on the day. However, it is at least arguable that it will be far more interesting to take notice of what I say off-the-cuff rather than relying on this document as an accurate rendition of what the lecture was really about!

Also, please note that "IANAL" (I am not a lawyer). Consult a professional if you wish to receive accurate advice about the law!

Further Reading

- Most of the relevant statutes available online
  - many court judgments now also appearing online
  - reading acts of parliament is relatively straightforward (judgments vary in clarity!)
  - however, law is somewhat flexible in practice, and careful textual analysis may disappoint
- Wealth of explanatory websites
  - often solicitors (and expert witnesses) seeking to show their expertise
- IANAL! (although I am sometimes an expert)

The text of all relevant UK statutes are published at:

`http://www.legislation.gov.uk`

On the website you will find most statutes – starting with five that predate Magna Carta – with complete coverage from 1988 onwards. Consolidated versions of statutes (albeit with some complex exceptions and limited application of the most recent changes) are also available, along with an indication as to which sections are currently in force.

The site also holds the text of statutory instruments, with partial coverage from 1948 and a complete set from 1987.

Data Protection Act 1998

- Overriding aim is protect the interests of (and avoid risks to) the Data Subject
  - differs from US "privacy protection" landscape
- Data processing must comply with the eight principles (as interpreted by the regulator)
- All data controllers must "notify" (£35 or more) the Information Commissioner (unless exempt)
  - exemptions for "private use", "basic business purposes" (but not CCTV) : see website for details
- Data Subjects have a right to see their data

✶ The Data Protection Act 1998 is now fully in force. The text of the Act is online at **http://www.legislation.gov.uk/ukpga/1998/29/contents** and there is a wealth of advice on the Information Commissioner's site at:

http://www.ico.gov.uk/

✶ Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than in the 1984 Act. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

✶ Exemptions from notification are complex – see the website for details

✶ Data Subjects may be charged (but not more than £10) for access to data. Many organisations will incur costs that are far higher than this.

US Privacy

- US approach is sector specific (and often driven by specific cases) For example:
  - privacy of mail (1782, 1825, 1877)
  - privacy of telegrams (state laws in the 1880s)
  - privacy of Census (1919)
  - Bank Secrecy Act 1970 (requires records kept!)
  - Privacy Act 1974 (regulates the Government)
  - Cable Communications Policy Act 1984 (viewing data)
  - Video Privacy Protection Act 1988 (purchase/rentals)
  - Telephone Consumer Protection Act 1991 (DNC in 2003)
  - Driver's Privacy Protection Act 1994 (license data)
- Specific rules for phone calls & email
  - CAN-SPAM & Do-Not-Call (2003)
  - may be joined by "do not track" ?

✶ The US does not have the same idea of Data Protection as does Europe, but it does have a formal notion of privacy, and a patchwork of Acts addressing disclosure of personal information in specific sectors.

✶ The Privacy Act applies many of the Data Protection principles to the Federal Government (but not to private industry, and there are significant exceptions).

✶ The Video Privacy Protection Act was passed following Judge Robert Bork's video rental records being released when he was being considered for appointment to the Supreme Court.

✶ There is an overview of all the various statutes at:

http://www.cdt.org/privacy/guide/protect/laws.php

HIPAA

- US Federal Law (Health Insurance Portability and Accountability Act 1996)
- Sets standards for privacy and security
  - Personal Health Information (medical & financial) must be disclosed to individual upon request, and when required by law or for treatment, payments etc (but info must be minimized where appropriate)
  - all disclosures must be recorded
  - must record, eg, that patients to be called at work
  - security implies admin, physical & technical safeguards
- Requires use of a universal (10digit) identifier

✶ At the heart of HIPAA is a "Privacy Rule" that it takes a 25 page PDF to summarise!

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

✶ The official site explaining HIPAA is at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Sarbanes-Oxley

- US Federal Law (Public Company Accounting Reform and Investor Protection Act of 2002)
  - introduced after Enron/WorldCom/etc scandals
- Public companies have to evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting
- Auditors required to understand & evaluate the company controls
- Companies now have to pay much more attention to data retention and data retrieval

✶ Sarbanes Oxley (SOX) is a complex collection of provisions, that are intended to restore confidence in corporate America following some very high profile scandals that cost investors billions.

✶ Drawing on analysis on why those scandals occurred, there are now specific rules about conflict of interest for auditors and security analysts.

✶ Senior executives in public corporations must take individual responsibility for the accuracy and completeness of financial reports and they have new requirements to report personal stock transactions.

✶ The requirements on effective internal controls have been implemented through the Public Company Accounting Oversight Board (PCAOB), and in essence through the major accounting firms. Where existing accounting systems were chaotic, manual or decentralised, costs have been high, which has led to considerable criticism.

✶ There is some evidence of smaller firms avoiding stock market listings in New York to reduce their costs, and the SOX regime is regularly being tinkered with to try and avoid excess expense.

✶ For the text of the law see:

http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

Security Breach Disclosure

- California State Law SB1386 (2002) updated by AB1950 (2004)
  - must protect personal data
  - if disclosed then must tell individuals involved
- Now taken up by 46 (of 50) states & talk of a Federal Law (for harmonisation)
  - early on had a dramatic impact, now (100 million disclosures later) becoming part of the landscape
  - no central reporting (so hard to track numbers)
  - some disclosures look like junk mail!
- EU already has sector-specific provision for telcos/ISPs and may extend this during the revision of the Data Protection Directive

✶ For a list of all the various state laws (there is similar language in all of them, but all sorts of complex differences) see the NCSL website:

http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

✶ The EU included a security breach disclosure requirement in the reworking of the Telecoms Directives. It applies to telcos and ISPs (but NOT to "information service providers") where there is a security breach affecting information held for "the provision of electronic communication services".

✶ For the UK transposition of the new regime see "The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011", SI 2011/1208:

http://www.legislation.gov.uk/uksi/2011/1208/made

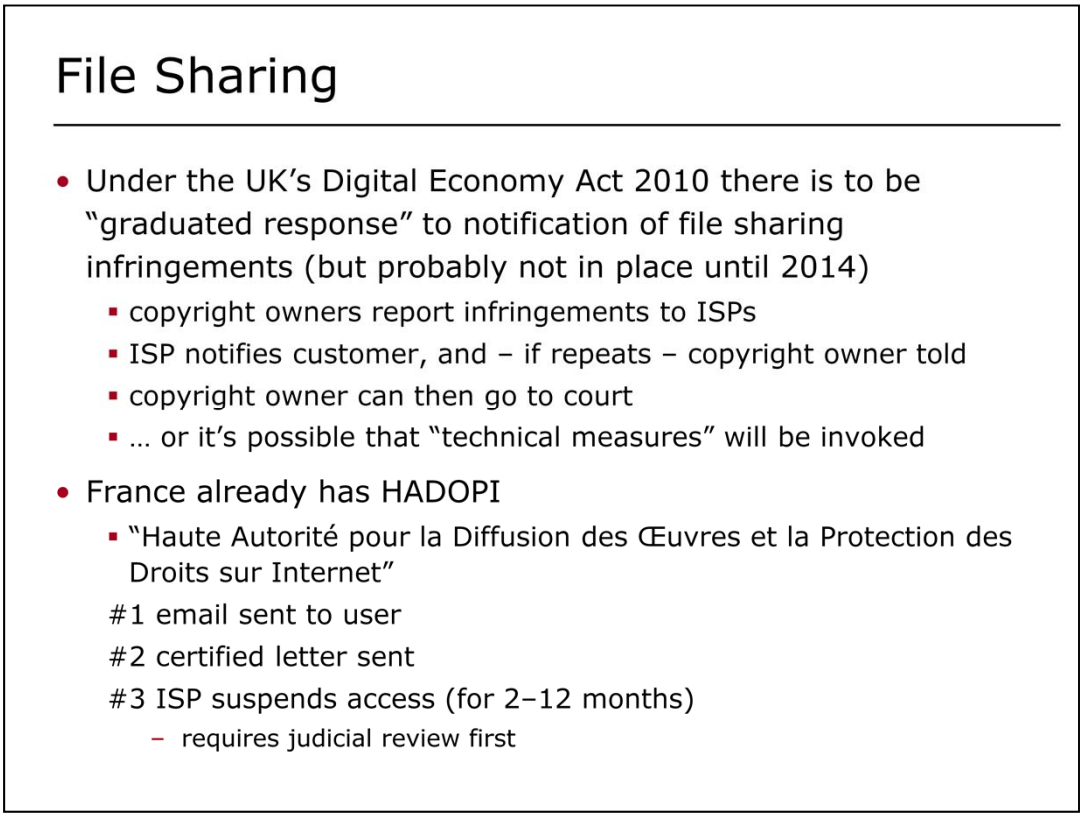
Note that if you lose personal data you have to tell your national authority (in the UK the ICO). If you think it adversely affects the personal data or privacy of a user of subscriber then you must tell them. If you don't the regulator can force you to do so. Note that you have to report a breach even if the data was encrypted and hence there wasn't really a breach at all !

Copyright Material

- US has the DMCA "safe harbor" so that hoster is immune until notified then must remove; but user may "put back"
  - DMCA is very prescriptive about take-down
  - but if you follow the rules then removal is straightforward
  - put-back timescale is not immediate (idea is to allow complainant to move dispute to the court system)
- EU has eCommerce Directive and a "hosting" immunity
  - hoster immune until they have "actual knowledge"
  - related immunities are "mere conduit" and "cacheing"
- User Generated Content might qualify for hosting immunity
  - or it might not!
- L'Oreal v eBay – ECJ ruling May 2011
  - only affects "commercial" use of trademarks
  - eBay (who bought AdWords) can be pursued for infringing sales

✶ The Digital Millennium Copyright Act (1998) criminalises production or shipping of digital rights management (DRM) circumvention devices. It also sets up a scheme for dealing with copyright infringement on the Internet. ISPs are immune until notified, via a specific address that they must publish, and then they must remove infringing material. When there is a dispute the poster can have the material replaced, but must submit to the jurisdiction of a court who will decide the case. Note that infringement notices must meet specific requirements and be made "under penalty of perjury".

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ304.105.pdf



✶ In the UK, Parliament passed the Digital Economy Act (in rather a hurry) in April 2010. Where there is infringement via file sharing the rights owners will be able to require ISPs to communicate with their customers to tell them of their wrongdoing. The ISP must reveal the existence of persistent offenders, and the rights holders can then apply to the court for an order to have their names and addresses revealed. This is sometimes called "graduated response" or "three strikes". Much of the detail will be set out in secondary legislation that will be appearing over the next year or so.

Deep Linking

- Deep Linking is the term for pointing at specific pages on another website rather than the top level.
- Courts generally rule against this when "passing off"
  - 1996 Shetland Times v Shetland News (UK) settled
  - 1997 TicketMaster v Microsoft (US) settled
  - 2000 TicketMaster v tickets.com (US) allowed [since clear]
  - 2006 naukri.com v bixee.com (India) injunction
  - 2006 HOME v OFiR (Denmark) allowed [not a database]
  - 2006 SFX motor sports v supercrosslive (Texas) injunction
- Google News is a popular target
  - 2007 Copiepresse Press v Google (Belgium) forbidden
    - appeals, but settled out of court in 2012
  - legislation possible in DE, and maybe cases in FR, BR etc

✶ Shetland News had headlines that pointed to stories within Shetland Times site. There was an interim injunction forbidding this (because the headlines were copied verbatim), but it settled before trial with the News agreeing to cease their previous practice.

http://www.netlitigation.com/netlitigation/cases/shetland.htm

✶ Microsoft's "Sidewalk" site linked direct to events on Ticketmaster's site. They settled out of court and the deep links were removed.

http://www2.selu.edu/Academics/FacultyExcellence/Pattie/DeepLinking/cases.html

✶ Tickets.com were linking into TicketMaster when they didn't handle an event, and the judge said it wasn't a copyright breach because there was no copying.

http://www.politechbot.com/docs/ticketmaster-tickets-2000-03-27.txt

✶ The aggregator naukri was enjoined from linking deep into the naukri jobs site (they were essentially presenting classified of their own).

http://dqindia.ciol.com/content/industrymarket/focus/2006/106032304.asp

✶ Real estate site bolig.ofir.dk was linking into a database of houses for sale at Home. The court overturned a previous DK ruling saying that search engines by "ordinary practice" provided deep links into websites.

http://www.edri.org/edrigram/number4.5/deeplinking

✶ Supercrosslive linked to a live audio webcast at SFX. This was seen as copyright infringement. Worth noting that supercrosslive was a litigant in person.

http://cyberlaw.stanford.edu/packet/200702/providing-unauthorized-link-live-audio-webcast-likely-constitutes-copy

✶ The Belgian newspapers objected to Google News who provided headlines and small snippets of their stories.

http://www.webpronews.com/topnews/2007/02/14/google-to-appeal-copiepresse-decision

http://www.futureofcopyright.com/home/blog-post/2012/12/20/legal-battle-between-google-and-belgian-publishers-comes-to-an-end.html

Framing, Inlining & Linking

- Framing is being permitted for search engines
  - Kelly v Ariba (US) : thumbnails of Kelly's photos in Ariba's search engine were "fair use", and full-size "inlined" or "framed" copies were also OK
  - but don't do your own design of a Dilbert page!
- Linking is much less of a problem
  - even from disparaging site (US) Ford Motor Co case
  - but linking to bad things generally bad
- In general, framing causes problems
  - Hard Rock Café v Morton (US) "single visual presentation"
  - Washington Post v Total News (US) settled

✶ Kelly was a photographer whose site was indexed by Ariba (an early image search engine). The court held that the thumbnails were allowed under US copyright law's "Fair Use" provisions. The appeal court initially held that when they framed images that were clicked on then this infringed, but revised their opinion and later said that was OK as well.

`http://www.eff.org/cases/kelly-v-arriba-soft`

✶ United Media get upset if you create your own page (with a better layout) and incorporate Dilbert strips within that.

`http://www.cs.rice.edu/~dwallach/dilbert/`

✶ Ford failed to get an injunction to prohibit a link from the disparaging website "fuckgeneralmotors.com"

`http://www.2600.com/news/122201-files/ford-dec.html`

✶ Morton sold his interest in the Hard Rock Café, except for the Hard Rock Casinos and Hotel. However, he also built a website that sold Hard Rock items, and that sold CDs via a framed copy of the Tunes website. The court held that since it looked like a Hard Rock Hotel site, and since selling CDs was a right Morton had sold, he was in breach of agreements.

`http://www.internetlibrary.com/cases/lib_case192.cfm`

✶ Total News linked to various news websites, presenting their content within a frame (full of their logo and their adverts). They settled out of court with the media companies – with Total News getting a license to link to the sites, but without a frame. Since settled, this doesn't settle anything!

`http://legal.web.aol.com/decisions/dlip/wash.html`

Brand Names

- Significant protection for brands in domain names
  - Uniform Dispute Resolution Protocol for brand owners
  - mikerowesoft.com settled, microsuck.com survived…
  - US: 1999: Anticybersquatting Consumer Protection Act
  - US: 2003: Truth in Domain Names Act
- Using other people's brand names in meta-tags doesn't usually survive legal challenge
- Many US rulings on "adwords" now occurring; if you just buy keyword then you may well be OK, but definite risk of problems if use trademarks in ad copy, or on landing page
  - NB Google has its own rules as well
- Germany, UK, Austria following US line, France is not, but ECJ have followed the US approach which should harmonise things

✶ Most top level domains provide a dispute resolution protocol for settling domain name disputes, in particular the ICANN sponsored names have a uniform system: **http://www.icann.org/en/udrp/udrp.htm**

Trademark owners have little choice but to defend their IP, which put them in an awkward situation when a 17-year-old uses their real name:

http://ensign.ftlcomm.com/ensign2/mcintyre/pickofday/2004/january/jan019_04/mikerowesoft.html

✶ The US has specific legislation on Cybersquatting (in the UK the "One in a Million" judgment has been sufficient) and the US also criminalises "misleading" domain names for "porn" websites.

http://www.nominet.org.uk/disputes/caselaw/index/million/

http://www.law.cornell.edu/uscode/html/
uscode15/usc_sec_15_00001125----000-.html
uscode15/usc_sec_15_00008131----000-.html
uscode18/usc_sec_18_00002252---B000-.html

✶ Rescuecom Corporation v. Google, Inc. settled US issue of "use of trademarks", but to a problem it needs to be used "in commerce" to be a problem and create "consumer confusion". I , ECJ ruling in March 2010 found similar position, and gave substantial immunity to Google, albeit rather less to the advertiser. For a extended discussion of the current situation and some worked examples:

http://www.floridalawyer.com/press/2010/12/
google%E2%80%99s-adword-policies-and-
trademark-law-across-international-boundaries/

Politics & Terrorism

- Mainstream politics is following the extremists onto the web
  - especially Obama's fundraising (but Howard Dean did it first)
- Many issues arise on content
  - defamation, incitement, anti-terror laws
- Raising money raises lots of issues for political parties, for example in the UK:
  - need to know identity if amount over £200
  - need to report if over £5000 (or even £1000)
  - need to identify "permissible donors"
  - raising money for terrorism forbidden (!)

✶ For information about fund-raising for UK political parties see:
http://www.electoralcommission.org.uk/party-finance

International Policing

- Foreign police priorities differ (as do laws)
  - specialist advice is wise before attempting to engage them
- Police do not usually operate across borders
  - Interpol mainly a fax distribution centre
  - although we now have the European Arrest Warrant
- Convention on Cybercrime
  - aka Budapest Convention
  - Russia & others have objected to cross-border aspects
  - recently a "Commonwealth Cybercrime Initiative"
- Problem for searches of remote/cloud systems
  - once police become aware must use MLAT
  - MLAT allows the diplomats to consider the issues
  - but it often makes glaciers look quick

✶ There are attempts to harmonise cyber legislation, such as the 2001 Convention on Cybercrime

http://conventions.coe.int/treaty/en/treaties/html/185.htm

This also sets out a framework for cooperation with 24x7 contact points, but it does not provide any mechanisms for aligning strategic objectives, let alone allowing police to operate across jurisdictional borders.

✶ The Commonwealth initiative:

http://www.commonwealthigf.org/wp-content/uploads/2011/10/Commonwealth-Cybercrime-Initiative-Version-11.1.pdf

Extradition

- Gary McKinnon
  - accused of hacking 97 US military/NASA computers (2001-2002)
  - took until 2012 before extradition ruled out
- Richard O'Dwyer
  - student at Sheffield Hallam University
  - ran TVshack.net (and then TVshack.cc), hosted in Sweden
  - accused of copyright offences in New York state
  - faced extradition, but initial judgment was appealed
  - in Nov 2012 agreed to a deferred prosecution arrangement
- Gambling, non-banks &c => no US holidays!
  - extradition can be slow, but grabbing you at an airport is not
  - being a backroom boffin supporting serious crime can be a serious offence (see the UK's Fraud Act 2006 & Serious Crime Act 2007)

✶ Gary McKinnon

http://spectrum.ieee.org/geek-life/profiles/the-autistic-hacker/

✶ Richard O'Dwyer

http://www.bbc.co.uk/news/uk-england-south-yorkshire-17472142

✶ David Carruthers was arrested at Dallas Fort Worth airport whilst changing planes on a flight from the UK to Costa Rica. He was CEO of an online gambling firm (illegal in the US) and after several years of house arrest was sentenced to 33 months in January 2010.

http://news.bbc.co.uk/1/hi/business/5204176.stm

http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/6963081/Betting-executive-jailed-for-racketeering.html

Review

- Important to understand the difference between the European Data Protection regime & US privacy laws
  - however, much common ground and ideas like security breach notification gaining traction worldwide
- Much still to be finally settled on the web, but the broad outlines are quite apparent and there is case law (albeit perhaps still being appealed, so pay attention to dates on articles) for a great many situations, so a search engine will assist you in understanding what to ask a lawyer…
- Governments now grok computers and the Internet and are getting into data retention, traffic analysis &c in a major way

Ignorance of the law excuses no man; not that all men know the law; but because 'tis an excuse every man will plead, and no man can tell how to confute him.

John Selden (1584-1654)