PROFESSIONAL ISSUES
The Internet
defamation, pornography, spam

MICHAEL FOURMAN

Owning information
Misleading information
Stolen information
Illegal Information
Private information
Unwanted information
Dangerous information

Every country has laws governing what can be published or publicly displayed.

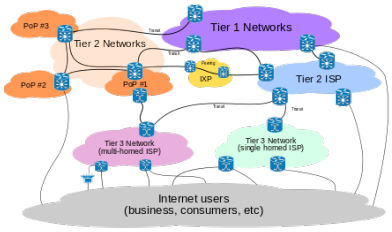
Typically, such laws address **defamation**, that is, material that makes unwelcome allegations about people or organisations, and

pornography, that is, material with sexual content.

They may also cover other areas such as political and religious comment, incitement to racial hatred or the depiction of violence.

14.2 The role of the ISP
do they possess information?
do they publish information?

- mere conduit
- caching
- hosting



14.3.1 Criminal law

Suppose a person X commits a criminal offence in country A and then moves to country B. Can country A ask that X be arrested in country B and sent back to A so that he can be put on trial? Or can X be prosecuted in country B for the offence committed in country A?

extradition
extraterritorial jurisdiction

The international convention on cybercrime

In 2001, the Council of Europe approved a draft convention on 'cybercrime'.

It deals with child pornography on the internet, criminal copyright infringement, computer-related fraud and hacking.

There is an additional protocol relating to incitement to religious or racial hatred, to which signatories to the protocol may also sign up.

14.3.3 Civil law There are some parts of the civil law where the position is reasonably clear cut.

Any contract that involves parties from more than one country should, and usually will, state explicitly under which jurisdiction (that is, which country's laws) it is to be interpreted.

Where intellectual property law is concerned, there are international agreements to which most countries are signatories so that there is a common framework, even if it can be very difficult to enforce the rights in certain countries.

In many cases, the plaintiff will have some choice about where to take action. Very often the decision will be taken on practical grounds – there is little point in taking action in a country in which defendant has no legal presence or few assets and it is probably unwise to take action in a country where the legal process is well known to be lengthy and expensive.

Defamation

- Defamation Act 1996 (+ 2002 regulation)
  defences
  not author, editor, or publisher
    - or
      took reasonable care in publication
      and
      did not know, or have reason to believe that what he did caused or contributed to
      publication of a defamatory statement
- The Defamation Act 2013 creates a new statutory defence for publishers to claim that allegedly defamatory statements constituted, or "formed part of", comments "on a matter of public interest" and that they "reasonably believed that publishing the statement complained of was in the public interest".

Under the Defamation Act (2013), a statement can be said to be defamatory if its publication "caused or is likely to cause serious harm" to individuals' or businesses' reputation.

However, only if businesses have suffered, or are likely to suffer, "serious financial loss", can they bring a claim of defamation against commentators.

The authors of defamatory comments can avoid becoming liable for damages if

they can show "that the imputation conveyed by the statement complained of is substantially true" or,

if the comments took the form of an opinion, that the opinion is one which "an honest person could have held the basis of any fact which existed at the time the statement complained of was published; anything asserted to be a fact in a privileged statement published before the statement complained of".

Authors shown not to have held the opinion themselves will lose their right to rely on this 'honest opinion' defence.

Section 5 of the 2013 Act provides a new defence for the operator of a website where a defamation action is brought in respect of a statement posted on that website if it was not the operator who posted the statement.

The rationale for the defence is that any defamation claim in this context should be between the claimant and the poster of the statement in question.

the defence is defeated if the claimant shows that:

1, it was not possible for the claimant to identify the person who posted the statement;
2. the claimant gave the operator a notice of complaint in relation to the statement; and
3. the operator failed to respond to the notice of complaint in accordance with the Regulations.

- Defamation Act 2013
  http://www.5rb.com/wp-content/uploads/2014/03/The-Section-5-Defamation-Act-2013-Regulations-Cumbersome-and-of-Questionable-Benefit.pdf

It is submitted however that of those who do, some will be quick to appreciate the potential ease with which the defence can be made … if the identity of the poster is anonymous to the complainant and the website operator alike.

A rise in abusive posts, automatic removal of material which may not be genuinely defamatory, and actions taken against the operator rather than the poster represent somewhat uncomfortably both the potential consequences of the Regulations and the very mischief these were drafted to address.

Pornography law in the UK

- Obscene Publications Acts 1959 & 1964 (+1994 for electronically-stored data)
  - **publication** likely, **taken as a whole**, to tend to deprave and corrupt those who are l**ikely to see or hear** … it
- Protection of Children Act 1978
  - **possession** of indecent material **involving children**
- Criminal Justice and Immigration Act 2008
  - **possession** of 'extreme pornography'
  - http://www.cps.gov.uk/legal/d_to_g/extreme_pornography/

Section 42 of the Criminal Justice and Licensing (Scotland) Act 2010 provides for a new offence criminalising the the possession of extreme pornographic material.
It came into force on 28 March 2011.

criminalises the possession of obscene, pornographic images which explicitly and realistically depict:

an act which takes or threatens a person's life
an act which results or is likely to result in a person's severe injury

rape or other non-consensual penetrative sexual activity
sexual activity involving (directly or indirectly) a human corpse

an act which involves sexual activity between a person and an animal (or the carcase of an animal)

http://www.gov.scot/Resource/Doc/925/0114212.pdf

Deleting images

Possession is defined in Scots law in terms of a person having knowledge and control of an item.

In normal circumstances, deleting images held on a computer is sufficient to get rid of them – i.e. to divest possession of them.

An exception would be where a person is shown to have intended to remain in control of an image even though that person has deleted it, for example, where a person has the capacity through skill or software to retrieve an image.

Participation in consensual acts

An additional defence has been created for those who appear in extreme pornographic images as direct participants in the act or acts portrayed.

In order to benefit from the defence, the accused must prove that they directly participated in the act or acts portrayed … and

that the act(s) did not actually take or threaten to take a person's life, did not actually result, and
was not likely to result in a person's severe injury,
did not actually involve nonconsensual activity and
did not involve sexual activity with a real corpse or real animal.

Spam UK

- EC Directive on Privacy and Electronic Communications (2002/58/EC)
  UK Privacy and Electronic Communications (EC Directive) Regulations 2003
- Unsolicited email can only be sent to individuals if
  they have previously given consent.
  reveal address of sender
  provide for removal 'easily and free of charge'

Spam USA

- CAN SPAM (2004)
  Controlling the Assault of Non-Solicited Pornography and Marketing
  - Unsolicited email can be sent to individuals if
    the recipient has not previously denied consent.
    and the sender provides physical address for removal
  - Exemptions:
    religious messages;
    political messages;
    content that broadly complies with the marketing mechanisms specified in the law; or
    national security messages.

In 2004 less than 1% of spam complied with the CAN-SPAM Act of 2003

A student member of the BCS, who has been given poor marks by one of his lecturers, writes a blog alleging (falsely) that the lecturer has accepted bribes from other students to increase their marks.

What legal and professional codes apply to the student's situation?

Under the heading Professional Competence and Integrity, section 2f states that you shall "avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction." This is the primary way in which the Code of Conduct relates to the situation.

However it is arguable that the conduct in question also infringes two clauses of section 4, Duty to the Profession:

a) [you shall] accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute, and
b) d) [you shall] act with integrity and respect in your professional relationships with all members of BCS and with members of othe professions with whom you work in a professional capacity.

Peter is a cricketer. He has suspicions that a team mate, Fred, is involved in some 'match fixing' as part of a betting group. In this case he believes that bets are being placed on which ball Fred will get out on. Rather than raise it with Fred or the team captain, Peter makes a comment on a social media site accusing Fred of this action. Peter believes that only his friends will read this comment but it is shared publicly. Fred disputes the accusation and is intending to take legal action.

Explain the law of defamation as it relates to Peter's actions.

What responsibility do the social media site or internet service provider that Peter is using have?

Defamation means making a statement that will damage someone's reputation, bring them into contempt, make them disliked, etc.
The author and publisher can both be held liable. Fred could therefore sue Peter and the social media site. This action by Peter would appear to imply dishonesty without any appropriate evidence. It would therefore be considered libel and Fred could sue both Peter (the author) and the social media site (the publisher).
Peter's claim that it was just intended for his friends is irrelevant; it is still libel, unless, of course he could provide evidence to show that the claim is true.
The social media site would be considered the publisher. As such, Fred could sue them, but they could claim that they cannot monitor everything. However, if Fred complained to them and they refused to remove the allegation, then they would be liable. The internet service provider (ISP) is protected by the E-Commerce Regulations 2002, provided they take down the libel expeditiously if they are made aware of it.

Explain the law relating to the sending of 'spam' to individuals within theEuropean Union. (8 marks)

How does this law differ from the corresponding law in the USA?

The European Union law relating to the sending of 'spam' is implemented in the UK through the Privacy and Electronic Communications (EC Directive) Regulations 2003.
Unsolicited e-mail can be sent to individuals (as opposed to companies) only if they have previously given their consent.
It is unlawful to send unsolicited e-mail that conceals the address of the sender or does not provide a valid address to which the recipient can send a request for such mailings to cease.
If an email address has been obtained in the course of selling goods or services, the seller may use the address for direct mailings, provided that the recipient is given the opportunity, easily and free of charge, with every message, to request that such mailings cease.

In the USA, it is legal to send spam provided that
* the person sending the spam has not been informed by the recipient that they do not wish to receive spam and
* the spam contains an address that the recipient can use to ask that no more spam be sent.

The security department of a bank has discovered that one of the bank's programmers has made unauthorised modifications to a programme he has been maintaining; these modifications divert a very small percentage of the value of each transaction into an account belonging to the programmer's mother.

How do the provisions of the Computer Misuse Act 1990 relate to this scenario?

Under the UK Computer Misuse Act 1990, it is a criminal offence to knowingly gain unauthorized access to a computer system. However, in this case, the employee's access was authorised.

Under the Act, it is a more serious criminal offence to gain unauthorized access with intent to commit or facilitate commission of a further criminal offence. The theft of funds would be a further criminal offence but this part of the Act does not apply because the access was authorised.

Under the Act, it is a criminal offence to modify computer materials without authorization. The bank employee has modified computer programs without authorization and so can be found guilty under this section.