



Pinsent Masons

Hacking and the Law

John MacKenzie

john.mackenzie@pinsentmasons.com

Introduction



- About Pinsent Masons
- Hacking
- The Law
- Individual rights and responsibilities
- Employee rights and responsibilities
- Directors' duties
- Questions

About Pinsent Masons



- Pinsent Masons is a full service commercial law firm
- 240 partners, a total legal team of around 900 and more than 1,500 staff in the UK and internationally.
- Pinsent Masons ranks in the top 15 of UK law firms and in the top 100 of law firms globally.

- OUT-LAW offers businesses both free services and added-value services, on-line and off. All the legal help you need on IT, e-commerce, privacy, intellectual property, software, telecoms, security, cybercrime, tax, employment, companies...



OUT-LAW.COM



IT & E-COMMERCE LEGAL ADVICE & SUPPORT FROM INTERNATIONAL LAW FIRM PINSENT MASON'S

About **OUT-LAW**

Services

OUT-LAW News**OUT-LAW** Guides

Case Studies

Fun

Links

Contacts

OUT-LAW offers businesses both free services and added-value services, on-line and off. All the legal help you need on IT, e-commerce, privacy, intellectual property, software, telecoms, security, cybercrime, tax, employment, companies...

FREE LEGAL NEWS BY E-MAIL

We track the main legal developments every day. [Register](#) for a free weekly summary or see [news of this month](#) or [archive news](#).

NCP Issue noted on our Palm PDA's

FREE CONSULTATION

Businesses around the world, from individuals to multinationals and governments, have contacted OUT-LAW for help with legal problems or questions. Get **free initial guidance** from specialist lawyers.

FEATURES

- ▶ OUT-LAW has a new data controller
- ▶ Get an OUT-LAW News Ticker on your site - FREE
- ▶ OUT-LAW Compliance: Get your site checked
- ▶ Data Protection and FOI training services

FREE GUIDES

Our wide range of popular [Guides](#) explain complex laws in terms that are easy to understand - and they're kept up to date.

SERVICES

- ★ Extranet services - contracts tailored to your business
- ★ Trade mark your brands
- ★ More legal services at [Masons.com](#)

FAVOURITE CONTENT

- ▶ Free confidentiality agreement
- ▶ Free internet and e-mail policy
- ▶ Disabled access to web sites under UK law
- ▶ The UK's E-commerce Regulations



FREE SUBSCRIPTION
Get your hands on the new OUT-LAW magazine. News, views and commentary on the issues affecting the world of IT law.

Are your web sites conditions of use legal notices up to scratch?
We'll help you to comply with the e-business laws

SEARCH

Hacking



- **Hacker***: [originally, someone who makes furniture with an axe] n.
 1. A person who **enjoys exploring the details of programmable systems** and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.
 2. One who **programs enthusiastically (even obsessively) or who enjoys programming** rather than just theorizing about programming.
 3. A person capable of appreciating hack value.
 4. A person who is good at programming quickly.
 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.)
 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
 8. [deprecated] A **malicious meddler** who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. See cracker.
- *Hacker Dictionary

Common Terms



Cracker

Phreaking

Phishing

Spoofing

Bot nets

Spyware

Malware

Adware

Homeware

Compare: Warez d00dz get illegal copies of copyrighted software. If it has copy protection on it, they break the protection so the software can be copied.

The Law



- The Computer Misuse Act 1990
- Data Protection Act 1989
- The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
- The Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- Council of Europe Cyber Crime Convention
- Common Law offences and the Civil Law

The Computer Misuse Act 1990



Not necessarily external control

It is the access that is “unauthorised”, not the method of access

- It is the access that is “unauthorised”, not the method of access
- (a) he causes a computer to **perform any function** with intent to secure access to any program or data held in any computer;
- (b) the **access** he intends to secure is **unauthorised**; and
- (c) he **knows** at the time when he causes the computer to perform the function that that is the case.
- **2.—(1)** A person is guilty of an offence ... if he commits an offence under section 1
- (a) to commit a ... applies; or
- (b) to facilitate ... (whether by himself or by any other person);

Knowledge is an essential aspect of any conviction under the CMA

Cor

Clearly consent would end any question of a crime – but what of contract terms?

1990

Notice the definition of intent



3.—(1)

- (a) he does any act which causes an **unauthorised communication** of the contents of any computer; and
- (b) at the time when he does the act he has the **requisite intent** and the requisite knowledge.

(2) ... the requisite intent is an intent to ...—

- (a) to **impair** the operation of any computer;
- (b) to **prevent or hinder** access to any computer; or
- (c) to **impair** the operation of any such program or data.

Impair, prevent or hinder – clearly directed toward the disabling of systems – but what of the use of spare capacity?

(3) The intent need not be directed at—

- (a) any particular computer;
- (b) any particular program or data or a program or data of any particular kind; or
- (c) any particular modification or a modification of any particular kind.

Data Protection Act 1989



- The seventh principle
- Having **regard to the state of technological development** and the **cost of implementing** any measures, the **level of security** appropriate to-
-
- (a) **the harm that might result** from such an occurrence of unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
- to be protected.

But when, and judged by whom?

May seem vague, but it is a concept familiar to Health and Safety lawyers

Plainly an assessment on a case by case basis, but if harm arises, then a claim for damages could follow

The Telecommunications (Lawful Business Practice) (Interception and Access) Regulations



You just can't! – Civil penalties (damages) possible if you do

Billions of e-mails pass through business mail servers – these are the circumstances in which you can monitor

Investigatory Powers Act

It is **unlawful to intercept electronic communications** unless the interception has been authorised.

The Investigatory Powers Regulations set out circumstances in which a **business can lawfully intercept emails** and telephone calls made on their own systems.

- routine access to business communications,
- monitoring standards of services and training,
- combating crime and unauthorised use of systems.
- Central to the Lawful Business Practice Regulations and the draft code is the need for email and internet access in the workplace - **consent**.

Without consent it is unlawful – the so called “legitimate” spyware software is unlawful



Record Everything Your Employees Do On The Internet.

Spector CNE (Corporate Network Edition) will record all employee Internet and PC activity, automatically archive these recordings to a centralized server and allow you to review the recordings remotely across the network.

SpectorSoft named a 2004 Inc 500 Company



SpectorSoft has been named as one of the 500 Fastest Growing Private Companies in America by Inc. Magazine. The ranking covers annual growth rate spanning a four-year period from 2000 to 2003.



Spector CNE is the Corporate Network Edition of Spector Pro - winner of the PC Magazine Editors' Choice Award for Best Activity Monitoring Software.

A New Definition for "Internet Monitoring"

Until Spector CNE, Internet monitoring meant recording web sites your employees visited and perhaps blocking them from certain web sites.

Have a Question?
Call us Toll-Free at:
1-888-598-2788

Spector CNE adds a whole new dimension to Internet monitoring. Now you can record everything your employees do online, including instant messages, chats, emails sent and received, web sites visited, applications launched, files downloaded and keystrokes typed.

Spector CNE combines Spector Pro, winner of the prestigious PC Magazine Editors' Choice award, with corporate network installation, configuration and deployment capabilities.

The result provides businesses with the most advanced monitoring software suite ever offered. Now, at the touch of a button, Spector CNE can be remotely configured and installed FROM any computer on the network TO any computer on the network, and the recordings can be viewed from any PC on the network.



Monitor multi-computer activity and track Internet usage
Record, calculate, and analyze application running time

Product | Awards | What's New | Screenshot | Download | Buy Now! | FAQ | Support | Forum | Site Map



Track4Win v2.2 is available NOW! Award-winning Product! Free to Try!

Track4Win can monitor all computer activity and Internet use. It can automatically track visited website addresses, and log work time on each application. Track4Win customers range from Fortune 500 companies to small business start-ups, and from system administrators to parents.

[Track4Win Enterprise 2.2 has been released [read more...](#)]

Key Features

- Multi-user monitoring (office/corporate LAN and remote WAN):
 - Track4Win can monitor all computers on a computer network at the same time. So you can run Track4Win on either a single PC or networked PCs.
 - No additional hardware required. You can use any computer to monitor other workstations.
- Real-time monitoring and Internet tracking
- Time tracking for all software applications
- Web site address and web page title tracking
- **Stealth installation and invisible running**

Screenshot

Download

Buy now

**Track4Win
Professional**

Privacy and Electronic Communications



What does this mean? In the conditions of use – as a pop-up – in a front page banner?

Information should not be stored or accessed on the user's equipment unless the user is:

Is this not a browser issue?

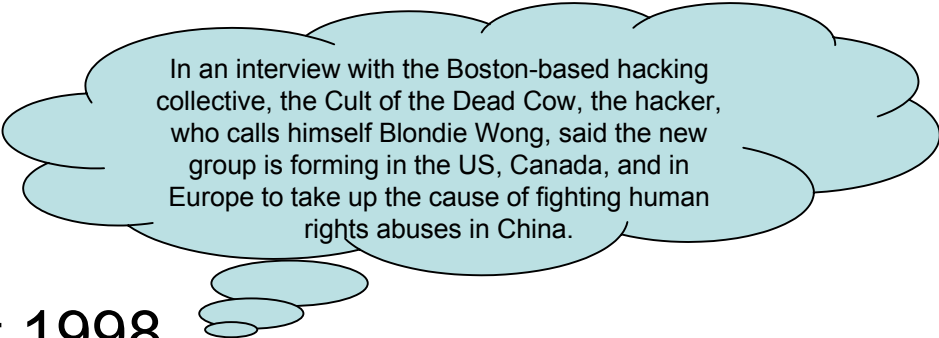
- Given **clear and comprehensive information** about the purpose of the storage of, or access to, that information; and
- Given the **opportunity to refuse** the storage of access to that information.

- Where loss has been suffered there is a right to bring a civil claim

Difficult to envisage what loss could be caused – but the right is there

- Information Commissioner can use the DPA under the

Europe



In an interview with the Boston-based hacking collective, the Cult of the Dead Cow, the hacker, who calls himself Blondie Wong, said the new group is forming in the US, Canada, and in Europe to take up the cause of fighting human rights abuses in China.



- Human Rights Act 1998
- Applicable to public authorities
- ARTICLE 8

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- Council of Europe Cyber Crime Convention
 - does not itself create substantive criminal law offences or detailed legal procedures. Parties agree to ensure that their domestic laws criminalise several categories of conduct

Common Law offences



- Theft
 - Theft of materials, but not information (in Scotland)
- Fraud
 - The intention to deceive – covers most forms of online crime
- Malicious mischief
 - Where the Crown can think of nothing else
 - Eg – denial of service attacks
- Civil wrongs – negligence... (oops!)
- Other Laws:
 - If there is a possibility of several things going wrong, the one that will cause the most damage will be the one to go wrong
 - Any given program, when running, is obsolete.
 - Don't get caught

Case Studies



- The individual
 - He wants to test his bank's security measures to gain access to his own account
 - He browses the web
- The employee
 - With no policies in place he is challenged about a personal e-mail
 - He is then sacked
- The director
 - With a mission critical system in place, they suffer a factory shut down as the server, and back-up, fall over.
 - No anti-virus, system overloaded, spam being sent from unprotected server.

Individual Rights and Responsibilities



- Testing the Bank
- the **access** he intends to secure is **unauthorised** – Computer Misuse Act
- However – if he impairs the operation of the Bank system
 - Criminal liability – malicious mischief – deliberate damage
 - Civil liability – negligence
- Possibly an enormous exposure
- Browsing the web
- Cookies received contrary to the Computer Misuse Act?
- the **access** he intends to secure is **unauthorised**
- to **perform any function**
- What terms does he actually read?
- What about read receipts?

Employee Rights and Responsibilities



- Personal e-mails
 - No entitlement to monitor
 - Require informed consent
- Monitoring creates a stressful environment
- Data protection requirements
- Evidential complications
- Sacked employee
- Can they access the office system?
- “I only wanted my...”
- No – “to **perform any function** ...[and] the **access** he intends to secure is **unauthorised**”

Directors' Duties



- Fiduciary duties to the company
- What is reasonably obvious to the ordinary Director – with that Director's skills and experience
- Data Protection
- Health and Safety?
- Criminal liability?
- Negligence:
 - Inadequate firewall
 - Inadequate virus protection
 - Damage to company reputation (spam)
 - Liability under the DPA, fine, censure
 - ISO 17799 – treats IS as a management function

The hacker's liability



- Loss flowing naturally from the wrong
- The loss is foreseeable
- The loss is reasonable
- The loss is not too remote

- Replacement system costs
- Loss of profits
- Management time

- Vicarious liability of the employer of the casual hacker?

A bit of reality



- It is unclear what proportion of hi-tech crime is attributable to serious and organised criminals, as distinct from individual criminals or mere thrill-seekers.*
- SDEA Headquarters are located at the Osprey House Complex, Paisley, which also accommodates the National Criminal Intelligence Service (NCIS) Scottish Office and HM Customs and Excise (HMCE).
- There are between 6 and 9 police officers dealing with “hi-tech” crime...

*<http://www.ncis.co.uk/ukta/2003/threat08.asp>

Some more reality...



- The biggest targets for criminal activities are financial institutions
- Financial Institutions **cannot** be seen to have insufficient security
- They would rather invest in technological defences, than sue
- Most sensible hackers will operate from other jurisdictions,
- The government, and especially the military, will track you down!

Questions?

