

Social and Legal Issues in Informatics

MSc Management – IS and Services Science

Governance and Accessibility

Giovanna Di Marzo Serugendo

Giovanna.Dimarzo@unige.ch, room B 235, 022 379 00 72

(Some slides provided by Roger Johnson, Birkbeck College,
University of London, UK)

Overview

Government's rights (RIPA)

- To intercept electronic information

Internet Censorship

Citizens' right

- To access the Internet

Employer's rights

- To monitor employees

Digital Evidence

Governance

"The **use** of institutions, structures of authority and even collaboration to **allocate resources**, **coordinate** or **control activity** in society or the economy."

<http://en.wikipedia.org/wiki/Governance>

Accessibility

“Degree to which a system is usable by as many people as possible without modification”

<http://en.wikipedia.org/wiki/Accessibility>

Usually related to disabilities

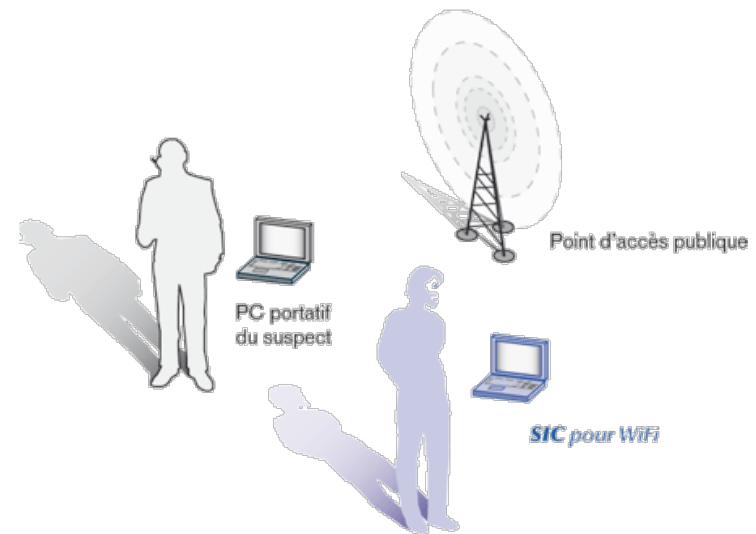
Here we are concerned with

- Employee / Citizens' rights wrt Internet information

Government's Rights

Regulation of Investigatory Powers Act (RIPA) 2000

- UK law
- Interception of communications
- Covert Monitoring of citizens
- Tribunal jurisdiction



RIPA - Purpose

The main purpose of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights.

These powers are:

- the interception of communications;
- the acquisition/disclosure of communications data;
- intrusive surveillance (on residential premises/in private vehicles);
- covert surveillance in the course of specific operations;
- the use of covert human intelligence sources (agents, informants, undercover officers);
- access to encrypted data.

For each of these powers, the Act will ensure that the law clearly covers:

- the purposes for which they may be used;
- which authorities can use the powers;
- who should authorise each use of the power;
- the use that can be made of the material gained;
- independent judicial oversight;
- a means of redress for the individual.

<http://www.opsi.gov.uk/ACTS/en2000/2000en23.htm>
<http://www.opsi.gov.uk/ACTS/acts2000/20000023.htm>

RIPA – 5 Parts

Interception of Communications and the Acquisition and Disclosure of Communications Data

- Unlawful to intentionally intercept communication without lawful authority by means of public service (postal service, telecommunication service)
- Unlawful to intentionally intercept communication by means of a private system without system's owner consent
- Lawful if both sender and recipient have given consent
- Lawful if in interest of national security
- Lawful if for preventing or detecting crime
- Lawful if for safeguarding the economic well-being of the United Kingdom

Surveillance and Covert Human Intelligence Sources

- Statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities of covert surveillance, agents, informants and undercover officers.
- Regulates the use of these techniques and safeguard the public from unnecessary invasions of their privacy.

RIPA – 5 Parts

Investigation of Electronic Data Protected by Encryption etc

- Provisions to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal use of encryption.
- Introduces a power to require disclosure of protected (encrypted) data.

Scrutiny of Investigatory Powers and Codes of Practice

- Ensures that there will be independent judicial oversight of powers where necessary.
- Establishes a Tribunal as a means of redress for those who wish to complain about the use of the powers.
- Provides for the Secretary of State to issue Codes of Practice covering the use of the powers covered by the Act.

Miscellaneous and Supplemental

- Amendment to other acts

Regulation of Investigatory Powers Act 2000

(Examples courtesy of JISC)

Example 1

Mr A, a private detective, installs a home-made phone tap on a British Telecom line to intercept Mr B's telephone calls.

This interception is intentional and without lawful authority. It is a criminal offence.

Example 2

Mr A, a private detective, installs a home-made phone tap on a line in the internal phone system of the University of Bumbleside, which is connected via a PBX switchboard to the British Telecom network, to intercept Mr B's telephone calls.

This interception is intentional and without lawful authority. It is a criminal offence.

Regulation of Investigatory Powers Act 2000

(Examples courtesy of JISC)

Example 3

Mr C, a staff member of the University of Bumbleside Computer centre, illicitly uses system privileges on the University computer network, which is connected to the Internet via JANET (the UK's Education and Research Network), to intercept interesting emails sent by Mr D, a member of the University. Mr C does not have the express or implied consent of the person with a right to control the relevant private telecommunication network (the University).

This interception is intentional and without lawful authority. It is a criminal offence.

Example 4

Mr C, a staff member of the University of Bumbleside Computer centre, acting on a memo from the Vice-Chancellor of the University uses system privileges on the University computer network, which is connected to the Internet via JANET, to intercept interesting e-mails sent by Mr D, a member of the University. Mr C has the express or implied consent of the person with a right to control the relevant private telecommunications network (the relevant officer of the University).

This is not a criminal offence. However, unless the relevant officer of the University has lawful authority to require the intercept, Mr D may be able to sue the University.

Regulation of Investigatory Powers Act 2000

Example 5

The University of Bumbleside Alumni Office wishes to conduct phone solicitations of former students (who have consented to their data being used for this purpose). It monitors staff phone calls to Alumni to ensure that staff adhere to correct procedures, including data protection rules, and for future staff training purposes.

Both staff and Alumni should be informed that calls may be monitored and /or recorded.

Example 6

The University of Bumbleside suspects that certain user accounts are being used to commit computer misuse offences. It monitors user accounts that display suspicious behaviour.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines and reinforced by registration documentation, login warnings and stickers on equipment.

Regulation of Investigatory Powers Act 2000

Example 7

The University of Bumbleside has reason to believe that its computer facilities are being misused to send unsolicited commercial emails. It monitors user accounts it suspects of being used to send such messages.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines, and reinforced by registration documentation, login warnings and stickers on equipment.


Example 8

The University uses certain logging mechanisms to ensure the efficient functioning of its email systems. The logging mechanisms allow authorised staff to access and monitor the use of user accounts as an incidental part of that logging.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines, and reinforced by registration documentation, login warnings and stickers on equipment.

Government Spied on 500,000 UK Citizens Last Year

PatrioticResistance1 27 videos



0:27 / 2:46 360p

211 views

<http://www.youtube.com/watch?v=zsCHhTba7Yw>

Internet Censorship

Internet Censorship

- “Control or suppression of material an individual can **publish** or **access** on the Internet”
- Difficult to put in place:
 - ◆ Information can be found from web sites hosted outside a specific country
- http://en.wikipedia.org/wiki/Internet_censorship

Blocking Methods

- IP Blocking (preventing access to server with specific IP address)
- URL filtering (look for keywords in the URL)
- Packet filtering (don't give back packet if contains specific keywords)

Internet Censorship

China

- Censored content (download/upload):
 - ◆ China-related political/social issues; pornography, criminality
- “Great Firewall of China”
 - ◆ Proxies filtering content by blocking IP access
- http://en.wikipedia.org/wiki/Internet_censorship_in_mainland_China

USA

- Freedom of speech is restricted to protect minors
- Control of content
- USA Patriot Act / Interference with Human Rights

UK

- Child Pornography
- Cleanfeed BT Service (blocks access to identified sites)
 - ◆ Target: all ISP to implement Cleanfeed-style of blocking
 - ◆ Child abuse website database
 - ◆ <http://publicaffairs.linx.net/news/?p=497>
 - ◆ <http://www.iwf.org.uk/media/news.archive-2004.39.htm>

Internet Governance

“Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.”

[WGIG 2005]

Internet Governance

Working Group on Internet Governance (WGIG)

- United Nations Working group
- set up after the World Summit on the Information Society 2003 (WSIS)
- <http://www.wgig.org/>

Issues

- Infrastructure (Domain Name System, IP addresses)
- Security, safety and privacy (spam and cyber crime)
- Intellectual property and international trade (including copyrights)
- Development Issues (particularly developing countries)

Citizen's rights

Web access favours

- Freedom of speech
- Freedom of access to information

Governmental Restrictions

- Regulation of Freedom of information
- Internet Censorship

Interference with Human Rights

- Freedom of Speech
- Access to information

Citizens' Rights

European Charter of Rights of Citizens in the Knowledge Society -
e-Rights Charter ([see ppt presentation](#))

- 1. Promote **Internet access for all** and foster the effective use of and the public's trust in **technologies** and **public services** based on new technologies
- 2. Strengthen the fundamental right to **education** in the Knowledge Society, enabling people of all ages and sectors to take part in and benefit from the development of the Knowledge Society
- 3. Provide **access** to user-friendly and understandable **public information**
- 4. Ensure transparent **public administration**

E-Rights Charter

CHAPTER I. Rights to Access

- 1. Every citizen of the European Union will have **access to the Internet through Public Internet Access Points**, preferably via a broadband network
- 2. Every citizen of the European Union must be guaranteed the **security and privacy of any personal data** managed through online public services

CHAPTER II. Rights to Education and Training

- 3. Every citizen of the European Union will have the **right to acquire the basic skills** for an effective use of services and information through ICT
- 4. Every citizen of the European Union will have **access to personalised assistance** when accessing public and ICT-based equipment and facilities
- 5. Every citizen of the European Union will have **access to lifelong e-learning platforms** to benefit from all the available resources generated by communication-technology facilities and thus take part in the knowledge society

E-Rights Charter

CHAPTER III: Rights to Online Information

- 6. Every citizen of the European Union will have access to the best quality information produced by public administrations
- 7. Every citizen of the European Union will have access to online information regardless of disabilities

CHAPTER IV: Rights to Online Participation

- 8. Every citizen of the European Union will be ensured the right to participate through ICT platforms in the decision-making processes of his or her local government
- 9. Every citizen of the European Union will receive public administration feedback on any online consultation results

See City of Glasgow signing charter (also: Barcelona, Gdansk, Brno, Lyon, Tampere, ...):

<http://www.glasgow.gov.uk/NR/rdonlyres/1B4BE881-9540-49A4-AE66-9C04886BCD52/0/echarterelectronic.pdf>

www.telecities-prague.cz/download/e-rights-en.pdf

Employer's rights

Misuse of computer by employee

- Downloading prohibited material (pornography)
- Defamation, Breaches of Data Protection Act
- Hacking, etc.
- Employer can be held responsible
 - ◆ Even if not authorised by employer

Computer / E-mail usage policies

- Employers adopt policies
 - ◆ Describing conduct to adopt when using computers and e-mails
 - ◆ Use of computers and e-mails subject to compliance with policies
 - ◆ Make sure everybody knows the rules (training/reminders)

Employer's rights

Writing e-mails

- E-mails are written traces of communication
- E-mails can be communicated very rapidly to a large number of people
 - ◆ Private e-mails that go public may damage employer's image
 - Sexual content, discrimination content, etc.
 - ◆ Confidential e-mails disclosed to concurrent/collaborative companies
- File content can be retrieved even if file has been destroyed
 - ◆ E-mail is even worse
 - Copy available to sender + all recipients

E-mail Usage

- Be careful when writing e-mails!
 - ◆ No critics, racial, sexual, discriminatory content
 - ◆ No comments on legal dispute in which employer is involved

Employer's rights

Monitoring e-mails

- Same rules apply to phone calls, faxes, e-mails

Basic Principle (RIPA)

- Telecommunications may **not** be intercepted by employers **unless** both sender and recipient have **consented** to the interception
 - ◆ Specifying a policy allows interception!

Exception

- Telecommunications (Interception of Communications) Regulations 2000
- Interception is allowed in certain limited circumstances
 - ◆ Related to the business / Be on a system provided in connection with business
 - ◆ Establishing existence of facts
 - ◆ Detecting crime
 - ◆ Compliance with regulatory standards
 - ◆ Investigating unauthorised use of system (breach of company's rules)
 - ◆ Staff quality control and training
 - ◆ Protecting system from viruses / Backing up – rerouting emails

Employer's rights

Employer must notify **users** that interception may take place

- Employee: in staff **policy**
- Outsiders: through e-mails and fax disclaimers

Use of intercepted communication

- Under Data Protection Act

Information Commissioner Code on **monitoring at work** (2003)

- Monitoring only when there is a real business need
- Methods used: not intrusive in employee's privacy
- Employees are entitled to some privacy at work
- Employers should avoid opening e-mails
- Employees should be aware of monitoring, its reasons, and the methods used
- Covert monitoring: for crime only
- Monitoring done by Security/Human Resources (not direct manager)

Employer's rights

Private e-mail (general usage)

- Private e-mails allowed
- Conditions:
 - ◆ short messages / sent during break time
 - ◆ Private vs Official Company E-mails should be differentiated
 - Signature format or different e-mails

Web site access

- Policy prohibiting access to unauthorised sites
- Use of filtering / blocking systems
- Employers can dismiss staff for excessive surfing

Birkbeck Policies

Birkbeck College Policies

- Computing Regulations
- E-mails
- Security
- Data Protection
- Personal Web page
- <http://www.bbk.ac.uk/ccs/policies/index.html>

University of Geneva Policies

UniGe Policies

- Computing Regulations
- E-mails
- Security
- Data Protection
- Personal Web page
- <https://memento.unige.ch/tm12>

Encryption

Switzerland

- Development, manufacturing and use of cryptographic software is not subject to limitations
- Import/Export of cryptographic software subject to Import Certificate

France

- Prohibited until 1996 (consider war weapon)
- Allowed up to 128 bits (1999?)
- Since 2004, liberalisation of encryption techniques
- <http://www.techno-science.net/?onglet=glossaire&definition=6143>
- http://gilc.org/crypto/crypto-survey-99.html#_Toc450793211 (survey, 1999)

Digital Evidence

Digital evidence

- Probative information stored or transmitted in digital form
- That may be used at trial
 - ◆ E-mails
 - ◆ Digital photographs
 - ◆ ATM processing
 - ◆ Accounting programs / Spreadsheets
 - ◆ Web browser histories, ...

Issues

- Authentication (e.g. may be easily modifiable)
- Readable format
- Must be properly acquired

Digital Forensic Investigation

Digital investigation

- Searching for information on a computer
- Any user does digital investigation when searching for files

Digital forensic investigation

- Special case of a digital investigation
 - ◆ Procedures and techniques used allow the results to be used for trials
 - Are illegal photographs stored on a computer?
 - ◆ Need to ensure that the state of the computer is preserved or need to use trusted tools
- Investigation may modify state of computer!
 - ◆ Preservation
 - Preserve the "crime scene" so that the evidence is not lost
 - ◆ Make copy of memory, power the computer off, make copy of hard disk

http://www.digital-evidence.org/di_basics.html
Copyright © 2006 by Brian Carrier

References

J. Holt: *Avoiding Employment Problems*. Ch. 4 in *A Manager's Guide to IT Law*. J. Holt, J. Newton (Eds), pp. 38-43, BCS. 2004.

Report of the Working Group on Internet Governance. Château de Bossey. June 2005. <http://www.wgig.org/docs/WGIGREPORT.doc>