

# Cyberliability — "Oh What a Tangled Web We Weave"

*Alyn Hockey, Director Product Futures, Clearswift  
and Mark Smith, Solicitor, Morgan Cole*

The Information Commissioner's draft Employment Practices Data Protection Code, dealing with monitoring at work, has caused a stir among employees and employers. The draft, stressing the need, in most cases, to tell workers when and why monitoring is taking place, brings to light the sensitive debate of employer responsibility versus employee privacy and the challenges that lie ahead.

Over the last two years, the growth of the Internet and email has kept the subject of employees' rights vs. corporate security under an increasing political, media and legal spotlight. As email and Internet monitoring grow, the number of disciplinary actions continues to increase, leaving individuals unclear about their rights to privacy in the workplace. The struggle to balance the individual employee's right to privacy and security with the organization's responsibility to protect its own intellectual assets has become increasingly intense as new legislation seeking to address this is resulting in new and complex compliance challenges for business.

There is a mass of UK and European legislation that must be taken into consideration. We've listed most of the relevant legislation in this article. There is also relevant federal and state legislation along with cases of precedent in the US. To further complicate matters, in the US there are market-specific regulations in certain vertical markets. In this article we touch on just two of these — the Securities and Exchange Commission regulations (finance) and the US Health Insurance Portability and Accountability Act of 1996 (healthcare).

## Relevant UK law

The starting point is the concept of 'vicarious liability'. This means an employer can be liable for the wrongful actions of its employees if performed in the course of their employment. The concept also covers activities that are

incidental to the employment (even if the method adopted is forbidden). Vicarious liability is a basic principle of employment law and underpins the majority of risks to organizations in this area.

The **Obscene Publications Act 1959** (OPA) defines obscene material as that which is likely to 'deprave and corrupt'. Whether material falls within this definition is not clear-cut. Certainly some material accessible on the Web could be considered obscene. There are criminal penalties under the OPA.

Offences under the OPA are committed upon 'publication' of the material, which includes electronic publication e.g. emailing obscene material. The **Telecommunications Act 1984**, supports this by making illegal the use of a public telecommunications system to send material that is 'grossly offensive or of an indecent, obscene or menacing character'.

The **Protection of Children Act 1978** deals specifically with indecent material concerning children. The threshold of 'indecent' is much lower than that of 'obscenity' under the OPA. The offence is committed by possessing such material (publication is not required). This would also include receiving the material in an email attachment. Therefore, businesses not only need to consider what is contained in outgoing email but also the content of incoming email.

UK **defamation** law protects the reputation of both individuals and corporate organizations. If untrue statements are made that would 'lower the individual or organization in the estimation of

right-thinking members of society' a claim may be brought. This includes libel (a more permanent statement which would cover email and Web defamation) and slander (a transient statement).

In determining the amount of damages awarded to someone who successfully sues for defamation, consideration is given to the size of the audience of the defamatory comment. A key risk associated with defamation in this context is that each repetition of the statement may be a fresh defamation. The ease with which a vast audience could be reached with email is obvious and so the damages awarded could potentially be very large. In addition, the damage to the reputation of the business may be substantial.

The **Sex Discrimination Act 1975**, **Race Relations Act 1976** and **Disability Discrimination Act 1995** prohibit **discrimination** on grounds of sex, race and disability. Electronic communication systems may be used by employees to send offensive or discriminatory messages to or about other staff. The presence of downloaded pornography or offensive material in a workplace may leave companies open to claims of harassment.

Businesses should be aware that there is no ceiling on the compensation that can be awarded for a successful sex, race or disability discrimination claim so the costs could be significant. Future legislation will outlaw discrimination on grounds of sexual orientation, religion and age.

## Monitoring

The extent to which employers can monitor their employees use of email and the Internet is governed by legislation. The following is relevant:

Under the **Regulation of Investigatory Powers Act 2000** (RIPA) interception of communications without lawful authority is an offence. 'Communications' will include email and Web access systems, if they are connected to a public telecommunications network.

The RIPA contains provisions for both civil and criminal liability. Interception

will be unlawful unless it complies with one of the exceptions in the RIPA. The key exceptions for most businesses are that (1) the sender and recipient have both consented to the interception (or the person intercepting reasonably believes that to be the case) or (2) where it complies with the **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** (the Regulations).

The Regulations give businesses a lawful basis for intercepting some communications without the consent of both sender and recipient. Essentially, any business (or government department or public body) can monitor communications for several specified reasons. The purpose of monitoring must be relevant to the business.

The Regulations require that the employer should make all reasonable efforts to fully explain to employees that they will be intercepting communications. Best practice suggests that the employer should also explain why they are doing so.

The **Data Protection Act 1998 (DPA)** came fully into force in October 2001. The DPA governs the use of personal data which is any information that can be used to identify living individuals.

The DPA requires that organizations inform individuals about how their data is used and ensure that they consent to this use. The DPA imposes strict requirements on anyone processing personal data ('processing' covers a very wide range of activities from collecting and storing the information to transferring it or even destroying it). It is important to note that organizations processing personal data are required to have 'appropriate organizational and technological measures' in place to safeguard the data. Failure to comply with the DPA attracts penalties ranging from fines to criminal sanctions for directors.

The Information Commissioner (the officer overseeing data protection) will shortly issue a revised Code of Practice to provide further guidance — (the draft of part of which caused such a commotion recently).

The **Human Rights Act 1998 (HRA)** should also be considered with regards to monitoring. The HRA incorporates the European Convention on Human Rights (the Convention) into UK law. Article 8 of the Convention provides a general right to a private life.

It is suggested that where the monitoring complies with the legislation mentioned above and the employee has signed and returned a balanced acceptable use policy, it would prove difficult to argue that any monitoring to enforce the policy was a breach of the employee's human rights. However, the law in this area is generally too recent to have established precedents.

## Relevant European law

Under the **EU Data Protection Directive**, EU citizens are afforded equivalent protection of personal data across Europe. Companies across Europe are responsible for the personal data they hold on individuals e.g. employees, clients and customers and must process personal data in a fair and lawful way. Companies which use central data centres outside of Europe must make special agreements to avoid breaching the Directive.

The **Cybercrime Treaty** was adopted on 8 November 2001 and is the first international treaty recognizing the impact of cross-border Internet crime and establishing objectives to deal with Internet crime including copyright infringement, computer related fraud, child pornography and violation of network integrity. Additional protocols will make any publication of racist and xenophobic propaganda via computer networks a criminal offence.

The **European Convention on Human Rights** guarantees certain fundamental human rights, including the right to a private life and to freedom of expression. Companies are responsible for protecting their employees' fundamental rights and freedom.

The **Telecommunications Data Protection Directive 1997** provides that

Member States must ensure confidentiality of communications and prohibit listening, taping, storage, interception or surveillance of communications unless consent is given by users or when legally authorized. Member States may authorize interception by businesses if it is needed to provide evidence of business communications.

The Treaty of Rome, the EU Equal Treatment Directive and the EU Equal Treatment Framework Directive govern the law on **discrimination** in Europe.

## Relevant US law

In the US, as in Europe, there are a number of laws, and cases of precedent, which define the general cyberliability landscape. However, a successful email policy can give an employer the right to read every email by dealing with the privacy issues raised by the Common Law right of privacy, state privacy laws, the Fourth Amendment and the Electronic Communications Privacy Act (ECPA) of 1986. Other federal legislation which pertains to Cyberliability includes:

- The Telecommunications Act of 1996
- The Communications Privacy Act of 1986
- The Civil Rights Act of 1964
- The National Labor Relations Act
- The Copyright Act
- Senate Bill 771
- Economic Espionage Act of 1995

In the case of *Smyth v Pillsbury Co.* in 1996, the court ruled that employees cannot reasonably expect privacy from email sent at work, despite the Common Law right to privacy. In cases where a written email policy has been in place, employees have a smaller chance of proving the reasonable expectation of a right to privacy.

The ECPA prohibits unauthorized interception of messages and the unauthorized retrieval of electronic communications. In the case of *Steve Jackson Games Inc. v the US Secret Service* in 1994 the court ruled that this Act applied to email.

## Banking & finance regulatory compliance

Today's financial institutions face many regulatory requirements pertaining to their communications with the public, record keeping, trading practices and supervision of staff. Leading the regulatory charge in the world is the US Securities and Exchange Commission (SEC), closely followed by regulatory bodies from other developed countries, including the UK's Financial Services Authority.

Each year the SEC brings between 400-500 civil enforcement actions against individuals and companies for insider trading, accounting fraud and providing false or misleading information about securities and the companies that issue them. All major investment banks, mutual fund companies and commercial banks that engage in securities employ staff and deploy technologies to ensure their compliance with applicable regulations. The rise in financial institutions' usage of email has required the reinterpretation of regulations written when paper communications were the order of the day, to reapply them in this new context.

Compliance is required with regulations, amendments and clarifications

published by SEC, the National Association of Securities Dealers (NASD) and the New York Stock Exchange (NYSE). These regulations cover a vast array of banking activities, including the use, management and archive of corporate email.

The manual checking of emails is impractical and politically and legally incorrect. Software solutions will be deployed to provide compliance mechanisms. We should expect other developed countries to codify their regulatory requirements in this area, and here again software will be the key to achieving compliance.

### Protecting patient privacy

US healthcare organizations today face an urgent regulatory and management challenge: their need to comply with the various requirements of the US Health Insurance Portability and Accountability Act of 1996 (HIPAA). This landmark legislation mandated wide-ranging regulations for privacy, security and electronic transaction standards for individuals' healthcare information. Organizations covered by

the regulations include hospitals and other healthcare providers, physician offices, health plans, public health authorities, life insurers, information systems vendors, medical service organizations and universities, who have until 14 April 2003 to adapt their policies and tools to comply with HIPAA.

A recent US survey revealed that 14% of physicians send patient-specific clinical information by email. A further 39% said they would also do this, if email privacy could be guaranteed.

Central to the HIPAA is its Privacy Rule, which establishes the circumstances under which individuals' health data must be kept private; and the accompanying proposed Security Rule mandates various tactics for achieving this.

HIPAA calls for civil and criminal penalties for non-compliance, including fines of up to \$25 000 for multiple violations of the same standard in a calendar year, and fines of up to \$250 000 and/or imprisonment for up to 10 years for knowing misuse of individually identifiable health information.

# Fighting Fire with Fire: Automated Network Vulnerability Assessment

*By Adil Pastakia, managing director, Qualys, UK*

By responding to automated hacker attacks with automated vulnerability assessment, IT groups level the battlefield. In so doing, they take proactive steps to protect their networks, customers, data assets, and business continuity.

Not too long ago, most hacker attacks targeted high-profile organizations such as banks and governments. Times have changed, and now every Internet-connected network is vulnerable, whether it has thousands of IP addresses or just one. Why? Automated

tools make it easier to quickly identify and exploit network exposures, so more people can become hackers. And they're doing more damage because the new generation of threats are self-replicating and more virulent than ever.

As a result, prevention has become a top priority for IT groups of all sizes. For companies with global E-commerce operations, for example, protecting Internet-facing devices is crucial for business continuity. And for companies that maintain confidential customer or patient data online, it's essential to protect privacy, prevent fraud such as identity theft, and safeguard research data from destruction or manipulation by hackers.

But with limited staff resources, how can IT groups prevent network attacks without diverting resources from other projects? Increasingly, the answer is vulnerability assessment, the process of identifying network and device vulnerabilities *before* hackers can exploit them. And since hackers rely increasingly on automation, companies can fight fire with fire by