

>THE LEGAL RISKS OF UNCONTROLLED IM USE

>WHITE PAPER ORIGINALLY PREPARED BY BLAKE LAPHORN
TARLO LYONS; REVISED AND UPDATED BY JONATHAN
NAYLOR, EMPLOYED BARRISTER (2009)

>CONTENTS

ARE YOU AWARE OF THE LEGAL RISKS AROUND IM?	>1
WHY IM PRESENTS A RISK	>2
IM - TOO TEMPORARY TO CAUSE LIABILITY?	>2
SO WHAT EXACTLY ARE THE RISKS?	>3
WHY MONITORING IM USAGE IS ESSENTIAL	>6
IM SECURITY SERVICES CAN ADDRESS YOUR CONCERNS	>6

>ARE YOU AWARE OF THE LEGAL RISKS AROUND IM?

MOST ORGANISATIONS HAVE BEEN SLOW TO ASSESS THE LIKELY IMPACT OF IM ON THEIR CORPORATE RISK PROFILE.

Instant Messaging (or "IM") is one of the newest forms of electronic communication and it is rapidly gaining ground as a form of mainstream business communication. Your organisation may have embraced IM wholeheartedly, perhaps installing enterprise versions of IM and opening up its gateways to business associates using public IM networks. While many businesses are aware of the possible benefits of IM, such as its ability to promote real-time communication amongst work colleagues and customers, most organisations have been slow to assess the likely impact of IM on their corporate risk profile, and therefore have no agreed policy on its use.

This state of affairs is similar to that experienced by organisations as the adoption of e-mail became widespread. Carefully documented procedures designed to protect the organisation in terms of quality control and legal risk were not adapted fast enough to take into account the new means of communication, and consequently many were horrified to discover that e-mail represented a huge chink in their security and compliance armour.

Alternatively, you may be reading this white paper out of curiosity, comfortable perhaps that your organisation forbids IM use, or at least that no one within your organisation is using it at work. If you are within this category, you are probably experiencing a false sense of security. A recent survey by the International Data Corporation found that IM is set to overtake email as the preferred method of business communication by the second half of 2010. A younger workforce is adept at using IM and such usage is likely to continue to grow. IM tools are sophisticated and may enter networks, notwithstanding the fact that firewalls are in place, or obvious ports locked down.

Whether your organisation is an early adopter of IM as a business tool, is dragging its heels in coming to terms with IM use, or is simply basking in blissful ignorance, it needs to understand the legal implications of IM and to take swift action to mitigate the potential legal risks of IM use. After all, this is a tool that has inherent risks, such as security and record-keeping issues, which so concerned the White House of President Obama that staff use of IM has been banned (despite the President's well-known approval of technology such as the Web and Blackberries).

>WHY IM PRESENTS A RISK

In the work context, the majority of those using IM for work purposes are likely to be employees of the organisation. The liability of the employing organisation for the acts of its employees is called vicarious liability, and this arises when unlawful acts (rather than criminal acts) are undertaken in the course of employment.

It is not always straightforward to determine which acts of employees will be found to be in the course of employment, but there are strong policy reasons that often drive courts to find an employer liable. Put bluntly, an employer is more likely than an individual to have the financial resources or insurance necessary to be able to properly compensate someone who has suffered damage as a result of an employee's actions. In general, anything an employee does at work or for work purposes can be found to be in the course of employment, unless the offending act is so far removed from the work responsibilities that the employee appears to be (as the courts somewhat quaintly put it), "on a frolic of his own".

A key consideration is that an employer can be liable for the acts of its employees, even if the acts have been expressly forbidden. From this we can conclude that an employer will not necessarily escape liability arising from IM use, even if a) the use of IM is forbidden, or b) the IM software used was not provided by the employer. This is why employers need to take the risks arising from IM seriously, even if they have a policy of forbidding its use, or simply no policy at all.

>IM - TOO TEMPORARY TO CAUSE LIABILITY?

Some organisations take the view that IM leaves no trace, and therefore there is no record of any wrongdoing. This reasoning is flawed for several reasons. Firstly there is a history facility in IM products, which keeps a record of IM conversations. Secondly, even if the history facility is switched off at the sender's end, the recipient may have a copy. Those who have been involved in the IT industry since the early days of e-mail will remember that when e-mail was first introduced, there was a common belief within organisations that e-mail was similarly temporary in nature, whereas now most people appreciate that this is emphatically not the case.

In the recent Employment Appeal Tribunal case of **Netintelligence Limited –v- Ms JS McNaught UKEAT/0057/08** IM records were used in evidence, highlighting the willingness of courts and tribunals to consider such messaging in the same way that they would a letter or email.

**AN EMPLOYER
CAN BE LIABLE
FOR THE ACTS OF
ITS EMPLOYEES,
EVEN IF THE
ACTS HAVE BEEN
EXPRESSLY
FORBIDDEN.**

There is also the argument that in fact records of business transactions should be kept, and IM records of transactions are as much a record of business transactions as any other type of record. An organisation needs records as evidence to defend its legal rights: either by taking a claim or by defending a claim, and neither course of action is likely to be as successful or straightforward if vital evidence of transactions conducted by IM are not kept. Organisations in the public sector are required to keep good records of their activities under the s46 Code on Records Management, which was issued under the Freedom of Information Act 2000.

Further obligations also apply to those in the financial sector. Under amendments that were made to the Financial Services Authority Conduct of Business regime in March 2009, firms that buy and sell shares, bonds and derivatives will have to keep records of telephone and electronic communications (including IM exchanges) for six months. This new obligation is part of an attempt by the FSA to detect and deter market abuse.

>SO WHAT EXACTLY ARE THE RISKS?

The risks are exactly the same as those arising from e-mail misuse:

- **Harassment**

Employers are obliged to provide a safe place of work, and this includes reasonable protection of employees from the harassment of other employees or third parties such as customers or suppliers. If an employer fails to provide a safe place of work, then an affected employee can claim that this is a breach of contract, sufficient to entitle the employee to treat the employment relationship as at an end ("constructive dismissal"). A constructive dismissal, if established, is a type of unfair dismissal and the ex employee can claim damages arising from the loss of the employment. Where there is also a sex or race discrimination element to the harassment, the individual can claim potentially unlimited damages, presenting an additional risk to the employer. Unmonitored IM can provide a harasser with the ideal environment to conduct his harassment without detection.

- **Breach of confidentiality**

Confidential information is often kept confidential because it has some commercial value. Financial institutions were some of the first organisations to identify the risks of IM, when they discovered that whilst traders found the instantaneous communication incredibly helpful in their fast moving employment, some employees found it an equally useful medium for disclosing confidential information without having to go through the stringent controls imposed on their e-mail systems. Business plans and customer lists are just examples of the categories of information that might be disclosed.

- **Infringement of Intellectual Property Rights**

Copyright protects documents that are original (in the sense of not being copied) where effort has been invested in their creation. Copyright protects the economic value in that investment of effort. It is a breach of copyright not only to copy documents without the permission of the copyright holder, but also to issue copies to the public. Most organisations hold documents that are subject to copyright that is owned by a third party, as well as their own documents subject to copyright. Whilst most organisations would suffer a loss arising from the disclosure of their own valuable documents, an even bigger risk lies in allowing the disclosure of the documents of others, as the copyright holder can then launch an action for damages against the employer. In many cases IM will provide an unmonitored route for unlawful disclosure of copyright documents, not to mention an avenue for the sharing of unlawful files.

- **Data Protection**

Your organisation is likely to be a data controller under the Data Protection Act. A data controller is the organisation that controls the manner in which and the purposes for which personal data is processed. The data controller is responsible for compliance with, and primarily liable for, breaches of the Data Protection Act. The data controller has to take appropriate organisational and technological measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Part of compliance with principle 7 will involve measures to prevent unauthorised or unlawful processing by IM. Also IM provides viruses and other malicious code with a new route into an organisation. Viruses and malicious code will cause destruction of, or damage to personal data, and so this new route must not remain unmonitored.

Again, financial institutions face particular challenges in this area. The Financial Services Authority recently fined a stockbroking firm £77,000 for failing to implement sufficiently robust data protection measures to safeguard customer details from identity fraud¹. The FSA concerns included the failure by the firm to address the risk posed by staff access to IM. While there was no evidence that customer details had been lost or stolen, the FSA found that employees at the firm were not aware of the risks involved in IM use.

¹http://www.fsa.gov.uk/pubs/final/merchant_13jun08.pdf

THERE ARE SEVERAL SITUATIONS WHERE AN ORGANISATION MAY BE FORCED TO DISCLOSE IM RECORDS.

- **Freedom of Information**

If documents are disclosed to a public authority that is subject to the Freedom of Information Act 2000, that public authority is obliged at law to disclose information in documents that it holds if a request is made, notwithstanding that the information originates from a third party. This presents a risk to private sector (and indeed public sector) organisations in that disclosure to public authorities involves a loss of control over the public disclosure of their information. If IM is used for work purposes, documents may be disclosed with little thought, or with the mistaken idea that IM communications are somehow outside the normal legal regime. Although there are exemptions that allow public sector bodies to withhold information of third parties where release would be commercially damaging, these exemptions will not apply if withholding the information would not be in the public interest.

- **Defamation**

A defamatory statement is an untrue statement that tends to lower the reputation of an individual or organisation in the minds of right thinking individuals. An organisation can be exposed to liability for defamatory statements published by IM as much as it can be exposed to such liability for defamatory statements published by e-mail. The publication does not have to be external for defamation to have occurred.

- **Regulatory Requirements**

Where organisations are subject to regulatory requirements in relation to their communications, those requirements will apply to IM communications as much as to e-mail communications. Companies regulated by the Financial Services Authority should ensure that standard wording used on their e-mail is replicated on instant messages if used in the business context and that staff are aware that the regulations apply as equally to the content of instant messages as to any other form of communication. Where an organisation chooses to use disclaimers on their e-mails, these should be reproduced on all instant messages.

IM SECURITY SERVICES PROVIDE ADVANCED FUNCTIONALITY SUCH AS LOGGING OF ALL IM CONVERSATIONS

>WHY MONITORING IM USAGE IS ESSENTIAL

It is much better to monitor communications to ensure that corporate communications are of an acceptable quality and content than to have to deal with embarrassing and financially damaging situations later. There are several situations where an organisation may be forced to disclose IM records:

1. IM records are subject to disclosure in legal proceedings, and must be preserved when litigation is contemplated. Court rules on disclosure of electronic documents make it clear that searches for relevant documents should be stringent and even “deleted” documents should be disclosed if they can be recovered. An argument that searching for IM records will be too onerous, particularly when the software is held on your own systems, is unlikely to be successful.
2. IM records must be disclosed as electronically processed documents if they contain personal data and the subject of that personal data makes a subject access request.
3. They also must be disclosed pursuant to any request for them made under the Freedom of Information Act 2000. There are stringent penalties for attempting to amend documents that are to be produced as evidence, and it is a criminal offence to destroy, alter or delete documents with a view to preventing their disclosure under a Freedom of Information Act request.

>IM SECURITY SERVICES CAN ADDRESS YOUR CONCERNS

MessageLabs hosted IM Security Services (IMSS), is an IM security solution designed specifically for businesses that see the value in IM, but want to eliminate some of the risk associated with public IM services (such as Yahoo Mail, AOL AIM and Microsoft’s Live Messenger). IMSS provides advanced functionality such as content control, malicious link blocking and logging of all IM conversations. These logs can then be imported into an archive system for quick and easy retrieval in the event of legal disclosure requirements.

The legal risks associated with uncontrolled IM use need to be taken seriously by organisations of all sizes. Taking preventive measures is better than applying a cure after the fact. Having a company policy on IM use is essential, but it cannot protect your organisation to the same extent as a dedicated IM security service, such as IMSS. IMSS proactively prevents wrongdoing by controlling who uses IM and how they use it. The fact that some kind of monitoring is in place will, in many cases, provide a defence to actions brought on as a result of use of public IM systems.

For more information about how the MessageLabs hosted IM security service could help your business address the legal risks of unmonitored IM use or to register for a free trial visit:

www.messagelabs.co.uk/trials/free_imss

>WWW.MESSAGELABS.CO.UK
>INFO@MESSAGELABS.COM
>FREEPHONE UK: 0800 917 7733

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 20 7291 1960
Fax +44 (0) 20 7291 1937
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Culliganlaan 1B
B-1831 Diegem
Belgium
Tel +32 (0) 2 403 12 61
Fax +32 (0) 2 403 12 12
Support +44 (0) 1452 627 766

>DACH

Feringastrasse 9a
85774 Unterföhring
Munich
Germany
Tel +49 (0) 89 203 010 300
Support +44 (0) 1452 627 766

>AMERICAS

>HEADQUARTERS

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Tel +1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>CENTRAL REGION

7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA
Tel +1 952 886 7541
Fax +1 952 886 7498
Toll-free +1 877 324 4913
Support +1 866 807 6047

>CANADA

First Canadian Place
100 Kings Street West,
37th floor
Toronto, ON M5X 1C9
Tel+1 646 519 8100
Fax +1 646 452 6570
Toll-free +1 866 460 0000
Support +1 866 807 6047

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel +852 2528 6206
Fax +852 2111 9061

>AUSTRALIA

Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia
Tel +61 2 8208 7100
Fax +61 2 9954 9500
Support +1 800 088 099

>SINGAPORE

Level 14
Prudential Tower
30 Cecil Street
Singapore 049712
Tel +65 6232 2855
Fax +65 6232 2300
Support +852 2111 3658

>JAPAN

Bureau Toranomom 3rd Floor
2-7-16 Toranomom Minato-ku
Tokyo 105-0001
Japan
Tel +81 3 3539 1681
Fax +81 3 3539 1682
Support +852 2111 3658