The Legal Risks of Web and Email

ABSTRACT

Access to Web and email are essential for any business to be successful. However, there are a large number of potential legal risks that organizations need to be aware of and ensure that they put in place effective policies and procedures to minimize these risks.

There are obvious and hidden legal risks that can cost an organization money or inflict reputational damage. This white paper provides a brief outline of some of the main risks faced by employers when dealing with employee use of the Internet and email.
INTRODUCTION

Employee Internet and email access are indispensable applications for today’s successful business organizations. However, the inherent risks of employee Internet and email use are not always fully understood and, as a result, businesses put themselves at risk of potential legal liability. Knowing what these risks are will allow you to best prepare to avoid them.

This white paper provides a brief outline of some of the main risks faced by employers when dealing with employee use of the Internet and email.

Please note that this white paper is for indicative purposes only and does not constitute legal advice. You should seek legal advice before acting on any of the information contained in this white paper.

VICARIOUS LIABILITY

An employer will generally be liable for the acts of employees during the course of employment. This is through the concept of vicarious liability, a legal principle that imputes liability on employers for wrongful acts of their employees, if committed in the course of employment or even if sufficiently connected with employment.

The scope of vicarious liability has been proven to be very wide, and potentially any act connected to employment will attract liability for the employer. This could include actions on the Internet, sending or receiving emails and using any IT infrastructure or services that you allow your employees to use for work purposes, even when employees use them in an unauthorized way.

HARASSMENT IN THE WORKPLACE

The Internet hosts a wealth of inappropriate content such as pornographic material or Websites that incite hatred based on characteristics such as race, sexual orientation or religion. Such content can be distributed throughout the workplace with just a few clicks, for example by emailing links or downloaded content.

Viewing or distributing such content in the workplace is commonplace.

This may, however, lead to claims of harassment, discrimination or unfair dismissal by employees not involved in the accessing or distributing of such content. As an employer, there is a ‘duty of care’ to provide a safe working environment free from all types of harassment. Under the Equality Act 2010, harassment is defined as “unwanted conduct related to a relevant protected characteristic, which has the purpose or effect of violating an individual’s dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual.”

Sharing inappropriate content could lead to an employee bringing action based on the employer’s failure to maintain a safe working environment free from harassment or even that such conduct amounts to discrimination. This may be the case even if the content was not specifically aimed at or even distributed to a particular employee.

Any complaints regarding inappropriate content in the workplace should be taken seriously and dealt with following the organization’s disciplinary procedures.

IN PRACTICE

Sue is an office worker. She works in an open workspace, which she shares with several other colleagues. Her male colleagues frequently display pornographic images on their computer screens, and sometimes distribute them amongst each other. The fact that pornographic material is being viewed in Sue’s workspace may amount to harassment or even sex discrimination. If Sue’s employer does not deal with the situation, she may be able to resign and claim for constructive dismissal.
OBSCENE CONTENT

Emailing or distributing material that goes beyond pornographic which is likely to “deprave and corrupt” may, under the Obscene Publications Act, be a criminal offence. Worryingly, the viewing and downloading of this type of material in the workplace is not as uncommon as may be thought. This can result in employers being involved in criminal investigations, criminal prosecutions, negative publicity and the resultant, sometimes irreparable, reputational damage.

HEADLINE NEWS: DISGRACED AGRICULTURAL COLLEGE

Students and staff at an Agricultural College were arrested for downloading extreme pornographic material. The story featured on the front page of a Sunday tabloid with the headline “You Muck Spreaders – Farm college staff and students in porn scandal.”

DEFAMATION

Internet access allows speedy dissemination of information through applications such as email, and access to message boards, blogs and social networks. However, your employees should be careful what they write in emails or online about other individuals or organizations as unguarded comments may attract expensive defamation litigation. Defamation is the publication of a statement, presumed to be untrue, which has the effect of lowering the subject of the statement in the estimation of right thinking members of society.

Emailing or posting to a Website or blog is regarded as publication. As emails can be shared easily and quickly with a large number of recipients, the scope of potential damage from publication of a defamatory statement is wide. As an employer, you may be liable for what your employees write in an email or online.

HEADLINE NEWS: A WELL KNOWN SUPERMARKET

£10,000 was paid in settlement to a police officer who alleged this supermarket had published defamatory remarks about him. This was after a member of supermarket staff circulated a warning, via internal email, that the off-duty officer was involved in defrauding the supermarket in a “scam”, after he returned some items complaining about the quality. The email contained a detailed description of the officer. The officer was alerted of the email upon visiting the supermarket in his professional capacity.

HEADLINE NEWS: A WELL KNOWN INSURANCE COMPANY

In an out of court settlement, a financial institution paid £450,000 in compensation to a competitor after an employee circulated, on internal email, that the competitor was having severe financial difficulties.
INFRINGING COPYRIGHT AND THE RISKS OF P2P

Obtaining information through the Web is easy. But when the information that is retrieved is protected by copyright there is a risk of liability if that copyright is infringed. Examples of copyrighted works include films, music, pictures and literary works. A common misconception is that if a piece of work is on the Web you can do what you want with it. This is not the case.

The copyright owner has the sole right to copy, adapt, distribute, communicate to the public, rent or lend and perform in public. These are known as restricted acts, and only the copyright owner can do them. If you wanted to do a restricted act then you must seek permission from the copyright owner. Downloading or copying works such as songs, movies or news articles without permission of the copyright owner is an infringement of the copyright.

Furthermore, it is an infringement to distribute copyrighted work to others without the permission of the copyright owner. Email and shared network storage, as well as sophisticated online networks such as Peer-to-Peer (P2P), make it easy to circulate this potentially infringing content. Almost 95% of all music files shared online are unpaid for and are shared in breach of copyright, largely through P2P networks. Therefore, it is likely that at least some of your employees may partake in downloading or distributing copyrighted work and they may use company computers to do so.

Copyright infringement in the workplace may attract vicarious liability, and notoriously expensive legal proceedings for infringement. Online copyright infringement has attracted a lot of media attention in the last few years, with high profile cases such as the “Pirate Bay” case. It is likely therefore, that any organization facing legal proceedings for copyright infringement would also attract media attention.

The further risk with P2P networks is that once a file is downloaded, other P2P users can then access your computer to make copies of that file. If P2P clients are not properly configured it is possible to expose the entire contents of a computer to other P2P users, which could lead to confidential or sensitive business information being disclosed. Additionally P2P networks (and other illegitimate download sources) are known havens for malware and spyware, which further put the security of your IT systems, and the data stored on them, at risk. Leaking this confidential or sensitive data outside your organization could be a breach of the Data Protection Act, leading to significant fines from the Information Commissioner Office (ICO) and reputational damage.

IN PRACTICE: THE DANGERS OF SHARING AN ONLINE ARTICLE

An article on a Website catches an employee’s attention, and they think it is important for the rest of the company to be up to speed with the information. He decides to copy the text of the article and circulate an email to colleagues. The original copyright notice is left out of the email. This could amount to an infringement of copyright, and the company could face copyright infringement action which may involve paying monetary damages.

IN PRACTICE: DISTRIBUTING A DOWNLOADED FILM AT WORK

An employee downloads a copy of the latest movie from a file sharing site, without permission of the copyright owner, and stores it on her work PC. She then sends out an email to her colleagues letting them know that the film is available on shared network storage in the office. The employer may be vicariously liable for this infringement and again could face copyright infringement proceedings.
SECURING CONFIDENTIAL INFORMATION

Confidential information lies at the heart of most successful businesses. This could include a trade secret, client lists or databases constructed over several years. Yet when this information is stored digitally there is a risk that an employee, either unwittingly or intentionally, could copy or share this information via email or the Internet. This could have devastating consequences for any business. On top of the commercial impact, there is the risk that where the leaked information relates to a third party a claim under Data Protection legislation or for breach of contract.

THINKING POINT: HOW CAN EMPLOYEES USE A COMPANY DATABASE OF CONTACTS

An employee joins a professional networking Website. He uses the company database of clients and invites them to join his “network” on the Website. The issue that arises is this: are the contacts his to make or are they the company’s contacts? Given the amount of time and resources that a company may put into gaining clients, a use of such confidential information in this way could have devastating effects if the employee were to leave the company to work for a competitor, or even to set up business on his own, taking company contacts with him.

SOCIAL MEDIA

As social media increasingly blurs the line between work and home life, comments made by employees on social networks can have a significant impact on their employers. Whilst the use of social media can reap many benefits for an organization, misuse by employees can have some unfortunate consequences.

Harassment, discrimination and bullying in the workplace can be made easier by the use of social media networks. Harassing or discriminatory conduct online, aimed at an employee, can impact on their ability to do their job, especially when the conduct is that of a fellow employee. Employers could be held vicariously liable for conduct undertaken by one employee towards another, even when it occurs outside of working hours on social networking sites.

An employee has implied duties of fidelity to their employer and not to bring their employer into disrepute, and therefore derogatory comments about employers may justify disciplinary action and even dismissal. However this also has to be balanced with an employee’s freedom of speech. Dismissing employees based on comments or remarks on social media could attract claims of unfair dismissal, so any action must be proportionate and in line with an Acceptable Use Policy.

HEADLINE NEWS: SOCIAL MEDIA AND EMPLOYEES

The air hostess who was dismissed following comments posted about passengers.

The gay senior police officer, who posted explicit information about his gay lifestyle and pictures of him in his police uniform at a London Underground station. He received disciplinary action and was denied a promotion.

The supermarket employee who posted on a social networking forum obscene remarks about his employer, and subsequently was dismissed.

The bookstore employee who was sacked for blogging about his bad days at work and satirizing his “sandal-wearing” boss.

CONTRACT BY MISTAKE

Not all contracts have to be formal written documents. The briefest of negotiations by exchange of emails may be enough to satisfy a conclusion of a contract as long as the elements of offer and acceptance are present. This may cause problems when an unauthorized employee accidentally contractually binds a company to a commercial transaction. Further problems arise if emails relating to a contract are accidentally deleted, as it may be difficult to prove your position with no evidence.
CASE LAW: HALL V CONGOS

Hall, an employee at Congos, had not filed an expense claim within the deadline set out in his contract of employment. He emailed his line manager to ask if it was okay to submit a late claim. The line manager replied with the briefest of emails – “Yes, it is okay” – and his electronic signature. This was enough to vary the terms of Hall's employment, and the late expense claim was held to be valid and Congos had to pay the expenses.

CASE LAW: BAILLIE ESTATES LTD V DU PONT (UK) LTD.

DuPont sent Baillie an email with an attachment document for its commercial proposal on pricing and delivery for a printing machine. Baillie replied with an email saying “Go ahead”. To this Du Pont replied “It's on its way. See you tomorrow. Thanks again.” It was concluded that with the exchange of just these three emails, a binding legal contract had been entered into. The Judge commented that even though a disclaimer was attached to an email, there was an intention to be bound to contract. Furthermore, the email disclaimer did not necessarily apply to attachments.

RISKS FROM BRING YOUR OWN DEVICE (BYOD) POLICIES

More and more companies are allowing, and encouraging, employees to use their own computer, tablet or other mobile device to complete work-related tasks. BYOD again blurs the line between work and private life, and employees may be more lax about how they use Internet and email when using their own device. Monitoring what your employees are doing on their personal devices during working hours may be difficult, so a clear policy on what is and is not acceptable must be in place before employees bring in their devices. As the device is being used in connection with employment the principal of vicarious liability may apply.

There have been many reported faux-pas of portable computing devices containing sensitive data being left in public places. BYOD policies increase the risk of incidents like these, as it does make it harder to monitor which information is on which device. Lost devices can cause embarrassment and losses in terms of time and money, but more seriously there may also be Data Protection implications.

REMOTE AND MOBILE EMPLOYEES PRESENT THE SAME RISKS

Remote or mobile employees pose similar risks. An employee may feel detached from the workplace and therefore undertake more risky online conduct. These employees pose the same risk as employees in the workplace, and as an employer you may still be liable for their online conduct. Before an employee commences remote working, a full assessment of possible risks should be conducted.

HOW TO MINIMIZE THE RISKS OF WEB AND EMAIL

There is a framework of law that sets out how an organization can monitor employee use of Internet and email systems, including the Data Protection Act, the Regulation of Investigatory Powers Act and the Lawful Business Practice Regulations, as well as the Human Rights Act. The lawful authority to monitor employees comes from the Lawful Business Practice Regulations, provided monitoring is for one of a number of specific purposes and that every reasonable effort to inform employees that their communications may be monitored.

The best way to inform your employees is by creating and distributing an Acceptable Use Policy (AUP), which sets out what use of Internet and email is acceptable, why the employer is monitoring and how use will be monitored. The least intrusive means of monitoring should always be used, and there should be an identifiable goal of monitoring e.g. reducing personal emails. The policy should also be linked to disciplinary procedures as this allows the employer to take disciplinary action when the AUP is breached.

A sophisticated content filtering system for Web and email can help implement AUPs, allow usage to be proactively monitored and can ensure that potential breaches are highlighted through detailed usage reports.
ABOUT BLOXX

Bloxx provides Web and E-mail filtering solutions to thousands of organisations around the globe. We have an in-depth understanding of the unique challenges faced by educational establishments. Bloxx uses unique patented Tru-View Technology (TVT) to analyse and accurately categorise webpages being requested in real-time. With unsurpassed flexibility in deployment, Bloxx Web filtering lets you quickly and effectively roll out 1-to-1 learning programmes and easily manage BYOD Web traffic.

Available as hardware and virtual appliances, Bloxx filtering easily scales to meet your current and future requirements and our dedicated web reporting appliances ensure you can store years of traffic logs. In addition, our unique approach to licensing lets you decide the most cost-effective approach for your deployment which means you don't end up paying for expensive licenses you don't actually need. To find out more about Bloxx content filtering and security, email info@bloxx.com, visit www.bloxx.com, or chat to us on Twitter or Linkedin.