e-SAFETY LAW AND THE "BYOD" WORKPLACE GUEST

In this White Paper, noted legal expert Dr. Brian Bandey discusses the overall threat landscape that e-Safety Law produces when the corporation permits the employees of third parties onto their premises who have their own (or carry their employer's) web-enabled device. It is common-place now to give these "guests" permission to access the corporation's Wi-Fi and Internet access in order to facilitate the business they have to hand - often referred to as guest network access or Bring Your Own Device "BYOD" schemes.

But what e-Safety legal obligations arise? Are any owed to the guest since they're an invitee into the corporations premises? Does the presence of the guest make any difference to the legal obligations owed by the corporation as employer to its employees?

Dr. Bandey pinpoints the manner in which legal obligations and liabilities (both to the guest and from the guest) attach to the corporation when granting the visitor internet access and when they bring their own device to the corporation's IT infrastructure. In doing so, Dr. Bandey makes reference to other Smoothwall White Papers available at: www.smoothwall.net/whitepapers.

EXECUTIVE SUMMARY

The Guest On Your Premises

Just because the Guest is not your Employee, you have invited them into the workplace you control. Accordingly, e-Safety Legal Obligations arise on you (the inviting Corporation) and flow to the Guest.

The Guest's Employer

Non-Compliance with your e-Safety Legal Obligations to your Guest can affect their Employer. After all, you're not doing business with the Guest *per se*, but the enterprise they're representing. Loss and damage you cause the Guest may also be loss and damage suffered by their Employer.

Your Employees

You may educate your Employees in e-Safety. You may ensure that Your Employees are not sexualising the workplace, or otherwise harassing each other using your ICT. This doesn't mean that third party employers do too. BYOD Guests are a new vector for breaches of e-Safety Law in the workplace.

Your IT Infrastructure

The corporation's IT infrastructure is a focus-point where a number of legal obligations intersect. It contains your secrets, the secrets of others, perhaps disclosed under Non Disclosure Agreements (NDA), and Personal Data (often referred to as Personal Identifiable Information) subject to Data Protection and Privacy Law. The unrestricted access of a Guest connected to your IT Infrastructure with their personal device may cause your enterprise to be in breach of NDAs, Partner Contracts and Local Privacy Laws.

Offensive and Obscene SPAM

You may not protect your Employees against offensive or obscene SPAM, but other employers do. If you have an unfiltered environment or can't filter input to a Guest's web-enabled device you may be liable.

Sexual Harassment

You can be sued by your Employees who have been sexually harassed or bullied through seeing inappropriate images on your Guest's web-enabled device.

Relationship Damage

Your Guests are the Employees of your Business Partners. Placing them in a legally hostile e-Environment (where they could sue their Employer) necessarily involves damage to your trading relationship.

Statutory Defences

Employers can use legal statutory defences when sued by an Employee who has been sexually or racially harassed, through the misuse by a Guest with their device, by taking all reasonably practical measures to avoid the act complained of. Active Supervision Technologies are one practical measure.

Technology Changes Legal Thresholds

It should be understood that the advent of accessible, affordable and reliable Active Supervision Technologies lowers the threshold of legal liability in the context of e-Safety Law in the workplace.

1. Introduction

In this Briefing Paper I will be seeking to give a high-level overview of the e-Safety Legal Obligations when an Employee of a third party is invited into a corporation's premises and is given the ability to connect to:

- the internet via the inviting corporation's ICT
- the inviting corporation's internal IT infrastructure

via an Internet enabled portable device not provided by the Employee of a Third Party Employer.

Now, the terminology of *"Employee of a Third Party Employer"* and *"Inviting Corporation"* is somewhat legalistic; even where we're discussing the Law.

So let's use some simple language in this Briefing Paper. When saying "You" – I'm directing myself to the reader who is the enterprise, company or corporation that owns or controls the premises it occupies; and that owns an Internet-connected IT infrastructure.

The premises in question that You own or control where Your Employees work – I'll call "Your Office".

So You have invited either a supplier or a customer to send one of their employees to meet with Your Employees at Your Office (it doesn't matter that the visit was initiated by them or You). I'll call that supplier or customer the "Guest's Employer".

The employee of the Guest's Employer who comes to visit Your Office – I'll call the "Guest".

I'll call your employees who are present at Your Office whilst the Guest is there "Your Employees".

Some people distinguish between the IT Infrastructure of a corporation (i.e. the applications, databases, etc.) and the ICT (being the means to send e-mails, access the Internet, using VOIP etc.). For the purposes of this Briefing Paper I intend to bundle those together and since they're under your control, I'll call them "Your IT".

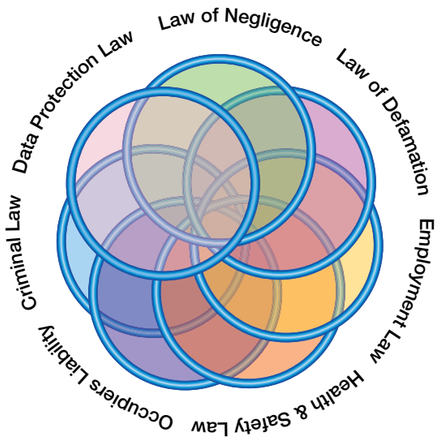
Finally there's the internet-enabled and portable device the Guest brings with them – I'll call that the "Device".

In this Briefing Paper I'll be considering two principal scenarios. Firstly, e-Safety Legal Obligations that arise which are owed to your Guest at Your Office as he or she connects to Your IT using their Device. Secondly, I'll consider the e-Safety Legal Obligations which are owed to your employees arising from the presence of the Guest with their Device at Your Office.

Before doing so, I'll sketch out the variety of well-understood Laws that intersect over this area. I'll also explain why what the Guest does, is also the act of the Guests Employer. In addition, what Your Employees do or suffer is Your act or suffering.

2. The e-Safety Law BYOD HazardSphere™

More specifically, in the context of this Briefing Paper, there are a number of overlapping Doctrines of Law which intersect over the activities concerned with the e-Safety. These apply to Employees and Guests as the Guest brings and uses their Device at Your Office. Below is a sketch diagram to illustrate such an intersection, the centre of which is a turbulent area and hazardous for the unwary or uninformed.



The Law of Negligence is concerned with Your Duty of Care to your Employees and your Guest.

The Law of Confidentiality is not only concerned with Your secrets but the secrets of others that have been disclosed to you in confidence (for example – under a NDA).

Employment Law and **Equality Law** governs Your interaction with Your Employees, their rights to a safe, non-discriminatory and non-harassing workplace and their right not to be the object of discrimination.

Health and Safety Law places legal obligations on you to keep Your Employees and visitors safe, and to risk assess their activities and workplace.

Occupiers Liability Law goes hand in hand with Health & Safety Law. It places legal obligations on You with respect to the safety of Your Office.

Criminal Law, perhaps suprisingly, has a place in the e-Safety Law paradigm. Some digital materials are illegal to possess or distribute electronically and often (regularly) make their way into the workplace.

Data Protection Law places obligations on You as to how You store and process data that can indentify living persons.

All of the above areas of Law are in play when a Guest is at Your Office interacting with Your Employees and Your IT using their Device.

The behaviour of Your Employees towards the Guest whilst at Your Office (their Acts and Omissions) will automatically make You legally liable. Although the Guest's Employer is similarly legally liable to You for the Guest's acts and omissions whilst at Your Office; You are also liable to Your Employees in respect of the Guest's behaviour (or misbehaviour). This is all bound up with what the Law calls the "Doctrine of Vicarious Liability". That will require some 'bare bones' explanation – which I've set out in the section below.

smoothwall®
Web Filtering + Security

3. Understanding the Employer's Liability for the Acts and Omissions of its Employees

What is Vicarious Liability?

In broad legal terms, employers are responsible for what their employees do, and what they fail to do, in the course of their employment. This is, as I have said above, known as the Doctrine of Vicarious Liability. It follows that any misdeeds committed by workers in the course of their employment can lead to legal claims being successfully taken against the employer by the injured party.

The legal theory of Vicarious Liability even extends to workplace bullying, harassment and inappropriate sexualised behaviour. Employers are liable for workplace harassment even if they were not in any way negligent. With a new generation of workers entering the workplace who are used to texting, instant messaging and e-mailing using their personal devices; misbehaviour using them is likely to arise.

Previously Employees had to prove that the Employer was negligent in not stopping misbehaviour taking place and that it had caused them psychological or emotional damage. The Law has changed on this point for some time now. It means that companies can be sued even if the company cannot be expected to have known about the bullying, harassment and inappropriate sexualised or discriminatory behaviour. This law is certainly wide enough to include the use of Explicit Images and E-Mailing via personal devices as vehicles for e-misbehaviour.

Vicarious Liability is the no-fault liability where the ***Blameless Employer*** is ***liable*** in law for the acts of the ***Blameworthy Employee***.

We **know** digital pornography on hand-held Devices and E-Mails sent from them are instruments used to bully and harass in the workplace and sexualise it.

The interception of such misuse is the **ONLY** defence available in law.

Are there Defences to Vicarious Liability in this Context?

Vicarious Liability is the no-fault liability where the Blameless Employer is liable in law for the acts of the Blameworthy Employee.

We know digital Pornography and E-Mails are instruments used to bully and harass in the workplace.

The new generation of Active Supervision Technologies[1] permit, for the first time, the prevention of sexual and racial harassment through digital means.

1 In this Briefing Paper, the term "Active Supervision Technologies" means Computer Software Technology which: (i) reads or views Internet based traffic; or (ii) reads or views the content of computer display peripherals (whether the computer is offline or online); and, if such traffic or content meets certain criteria: (a) prevents the intended recipient's access to it; or (b) prevents the display of the content; or (c) automatically generates alerts or reports in respect of such traffic or content.

smoothwall®
Web Filtering + Security

4. e-Safety Law Obligations Owed to the Guest

Digital Supervision – Safeguarding the Guest

> Only Digitally Supervising and the Guest will provide you with a Legally Effective Defence to loss and damage suffered by the Guest when their Device connects with Your IT.

Do You allow Your Guests to physically roam Your Office unhindered and unsupervised? Do they go where they want, when they want, on their own? Are they permitted to interact with Your assets – Employees, Your IT?

Well, from a legal point of view, why do You not permit that?

Legally, You do not permit that because:

- You must ensure that they're not harmed or injured by anything in Your Office which may be harmful or toxic – of which the Guest would be normally unaware;
- You need to ensure that they do not have access to Your Confidential Information;
- You know that you need to provide a Workplace for Your Employees which is not hostile and therefore need to supervise Guest Behaviour;
- You need to ensure that they do not leave behind in Your Office (even as an ill-considered joke) something harmful to your business[2];
- You must ensure Your Employees behave appropriately to the Guest.

The Legal Obligations that fall upon you in the real world, also fall upon you in every respect of a Guest's 'virtual presence' at Your Office.

Only Digitally Supervising the Guest will provide you with a legally effective defence to loss and damage, that may be suffered by the Guest when their Device connects with Your IT.

What is "Digital Guest Supervision"?

In order to satisfy Your e-Safety Legal Obligations to Your Employees; you may have implemented Active Supervision Technologies[3].

You may have done this not only to ensure Your Employees will not be inadvertently exposed to the toxicity of the internet (pornographic or sexualised SPAM, inappropriate image material) but also to identify, and where possible interdict, e-Misbehaviour by members of staff, one to the other.

The Guest can be exposed to the dangers of the internet and the e-Behaviour of Your Employees in just the same manner when they connect their Device to Your IT – with your permission.

Firstly in this context then – the Law requires you to enter upon a sensible and reasonable Risk Assessment exercise with respect to the Guest using their Device at Your Office. What hazards could they encounter? What reasonable steps could You take which would reduce the risk in those hazards?

Secondly – You are obliged to implement the findings of such Risk Assessment.

Digital Guest Supervison – in other words is the exercise of control, supervision and management of the Guest's Device (both input into and output from) whilst connected to Your IT.

In this way You substantially satisfy your e-Safety Legal Obligations.

2 There have been reported incidents where visitors to an office, who know the employees there very well through the course of their employment, have left behind sexually suggestive joke items, pornographic photographs in desk drawers (to be found by the 'victim' of the joke later, or inappropriately suggestive notes of admiration.

3 Briefing Papers specifically focussed on the Risk and Exposure Employers face when their Employees misuse their ICT and focussed on the e-Safety Legal Obligations owed to the Employee by the Employer which are complimentary of this Briefing Paper, are available from Smoothwall.

From What are You Protecting the Guest?

SPAM

A great deal of SPAM is rude, lewd or may contain indecent images. The Guest has a right not to work in a hostile workplace where their health is negatively affected. SPAM can create a hostile workplace as easily as any form of sexual or racial discrimination.

In a situation where the Guest originates from an environment where Active Supervision Technologies are highly tuned, their encounter with lewd or pornographic SPAM whilst at Your Office connected to Your IT may very well be actionable.

Inadvertent Content

The internet contains an incredible quantity of inappropriate content. The vast majority of this content is filtered by employers as a reasonable practical step in ensuring the workplace safety of their employees.

In Law, the Guests Employer's obligations to the Guest are replicated on you with regard to their workplace experience of Your Office.

You might consider increasing the filtering activity of Your Active Supervision Technologies when they are used by the Guest. Another way of putting this non-technically is to say that You should 'turn up' Your filtering policies for a login to Your IT by the Guest.

Your Office Culture

Your Employees may carry on their day-to-day activities in what might be called a robust, gregarious, unreserved and combative environment (which You may, or may not, encourage (tacitly or otherwise)). That does not stop certain behaviour being, in Law, discriminatory, or indeed prevent it from being harassment.

From recent case law and studying the misuse of ICT at work, it seems that the truth of the matter is this. No matter what "Acceptable Use Policies" are put into place; in the modern workplace, ICT is regularly employed to convey illicit messages, jokes, pornography and off-colour materials. This is especially because doing so no longer necessitates any face-to-face or proximate interaction between the sender and the recipient.

That which is normal for Your Employees – may simply be unacceptable and, in Law, actionable by the Guest.

Your Common Duty of Care

The Law of Negligence has certain essential attributes which indisputably fall on You. It is an important Doctrine of Law that operates very strongly between You and the Guest.

You must take reasonable care that your acts and omissions (which, of course, includes the acts and omissions of Your Employees for whom you are Vicariously Liable) do not negatively impact the Guest as you permit them access to Your IT.

Bear in mind that the Duty of Care that arises on You cannot be 'delegated away'. It cannot be avoided. it cannot be ignored. To operate in circumstances of ignorance of the law, or wilful blindness to it, affords no defence to it whatsoever.

The fact that web-enabled portable and personal devices are being used as a vector of hostility and harassment is now a given.

Your Common Duty of Care *continued*

Taking all of the above into account – You must look to Your Duty of Care that arises when Guests access Your ICT. The Duty of Care should be acknowledged, calculated and understood. Only then can appropriate measures be introduced so that this inescapable duty is fulfilled.

I will explain the action of the Law in these types of scenario in more detail as I evaluate what Your Employees might suffer at the hands of the Guest as they connect to Your IT. I do this since significant anecdotal evidence goes to show that away from the 'home' workplace, Guests may feel less 'inhibited' when at Your Office.

5. e-Safety Law Obligations Owed to Your Employees – the Guest in Your Office

Sexual Harassment by Third Parties

You will be potentially liable for sexual or sex-related harassment of Your Employees by the Guest where such harassment takes place in the course of their employment.

The Guest sending sexualised messages through to one of Your Employees using their Device would constitute this type of harassment.

However, You will have a defence to such claims provided that You have taken such steps as would have been reasonably practicable to prevent the third party from harassing the employee. You must also (usually) know that the complainant has been subject to harassment in the course of his/her employment on at least two other occasions by a third party (whether or not that third party is the same or a different person on each occasion).

Remember, Your Guest is very likely to have forged pre-existing commercial relationships with Your Employees and their conduct whilst at Your Office, connected to Your IT, may simply be a continuation or exacerbation of that situation.

Also bear in mind that the Guest may feel somewhat less inhibited when at Your Office compared to the level of professional inhibition they feel when at the office of their Employer.

There can be no doubt that the Law has serious implications for You as it gives Your Employees who are bullied or harassed at work an additional way to claim compensation from You.

We know that harassment regularly and habitually takes place in the workplace through the use of pornographic images and obscene and suggestive e-Mails (directed by the Guest at persons who they will not see on a day-to-day basis). It seems that the only avenue forward for You in mitigating these risks is to use every means, including technology, to try to intercept e-Harassment and the E-Mails or the explicit images used.

The Guest – Your Employees, Pornography and Obscene Material in General

The Guest sending Pornographic E-Mails and Attachments via Your IT

One of the most common and difficult problems You may face is the discovery that the Guest has been using their Device to access, view, download or transmit pornographic or sexually explicit material[4]. Although the possession or downloading of adult pornography is usually not a criminal offence (unless it is obscene or of a paedophilic nature), the transmission or distribution of such material is illegal.

Thus for example, an Employee who forwards a pornographic picture sent to them by the Guest through Your IT to a co-worker, or to someone outside the organisation, as an E-Mail attachment is committing a criminal offence.

Undoubtedly, the most important aspect of Your duty to Your Employees which is implied by Law is the duty to take reasonable care to ensure their safety. There are a number of common law rules which determine the extent of that duty In addition, there are certain statutory provisions designed to ensure Your Employee's safety which, if broken or not observed by You, may lead to an action for damages by an injured employee based on a breach of statutory duties.

What about Offensive or Obscene e-Mails which aren't Pornographic?

It is illegal to send indecent or grossly offensive material in order to cause the recipient distress or anxiety.

How can internet access by the Guest Amount to Harassment?

Uncontrolled internet access routinely leads employees into misbehaviour which is, in legal terms, **sexual harassment**. For example, in one case that went to Court, a female employee who worked in an open-plan office saw sexually explicit material which her male colleagues regularly downloaded from the internet and displayed on their workstation monitors. This downloading was not part of their employment but was conducted for their personal 'enjoyment'. She resigned and sued her employer for sex discrimination and sexual harassment.

Even though the activities she complained of were not directed at her personally, and despite the fact she had not previously raised any complaint with management, she won her case.

The Court said that the working environment was hostile to her as a woman due to the sexually explicit material being circulated. In this real-life situation, if the employer had implemented Active Supervision Technologies the pornography may have been blocked. A valuable employee would have been retained and training initiated for those trying to download pornography. Even if the porn filter had let the images through – the employer may very well have had a **total legal defence.** That is that they had taken all reasonable and practical measures to prevent the harassment.

You need to take reasonable and practical measures to prevent the Guest from this type of downloading or visualisation via Your IT which may negatively impact Your Employees.

4 Please do not consider this statement farfetched. Employees (who feel substantially inhibited behaviourally at work) regularly do this. Don't imagine that a Guest won't – especially if they're with You for a few days or more.

How are You to Blame for this type of Guest Behaviour?

All of the Law dealing with discrimination makes You legally liable for Your Guests, whether or not the actions in question were done with Your knowledge or approval.

This means that You cannot escape liability by:

- pleading ignorance of the fact that harassment was being suffered by an employee.
- arguing that there was no intent to cause offence to the person affected.
- blaming Your Employee for failing to complain formally to management about the alleged harassment.

Often the employees who is suffering the harassment may not come forward to a member of management to complain. Where unacceptable e-Mail content or images are concerned, they often feel particularly embarrassed about what is happening to them. Some Employees fear that they will not be believed or taken seriously, or worry that a complaint will just cause problems for themselves.

How do You defend Yourself?

The Law says that the responsibility lies squarely with You to take all reasonable steps to prevent discrimination (including harassment) from occurring.

To use the Legal Defence against a case where You are being sued for harassment and discrimination through the actions of the Guest, You must show that You have taken **all reasonably practical measures** to prevent it.

Active Supervision Technologies are the newest reasonably practical measures which **MUST** be taken. Without them – Your use of available Legal Defences is more likely to fail completely.

6. Unauthorised Guest Access to Confidential and Personal Identifiable Data

Let's not forget that You will own confidential and sensitive information. Information which, if unintentionally disclosed to the Guest via their access to Your IT, might cause considerable loss and damage. This will include, for example, product information (both present and future), unpublished financial data, profit projections, competitor assessments and so on.

You may also hold information about others; employee information, medical details, supplier data and information supplied under obligations of confidence. A comprehensive list would be lengthy indeed. Your Corporate Officers will owe Your stakeholders a 'duty of care' (in some jurisdictions a Statutory obligation, in others a Common-Law obligation) to take all reasonable precautions to ensure the security of such information.

Security breaches occasioning the loss of data can cause a whole raft of legal difficulties: from breach of contract, to fines under Data Protection Law, uncapped damages due to the release of third party secrets and so on and so on.

The Duty of Care owed by officers to their stakeholders, the corporation's duty to those persons whose personal information it holds, and the contractual obligations it owes with respect to third party confidential information – all compel You to exercise an appropriate level of expertise, care and prudence in the selection of a technologically secure computing environment through which the Guest accesses Your IT.

You must deploy suitable Firewall Technology to ensure that Your essential Confidential and Personal Information remain invisible and inaccessible to the Guest.

7. Conclusions – The Law, BYOD and Disclaimers

BYOD has become a business fact – in the same manner in which e-Bullying, e-Harassment and e-Pornography have become a fact of business life. From a legal perspective it is clear that BYOD in the enterprise or corporation should not go unsupervised, unmoderated or uncontrolled.

The obligations that fall on the host of their guest (in the context of this Briefing Paper) cannot be avoided or delegated other than by accessing pre-existent legal defences. Active Supervision Technologies are the reasonable and practical route to that those defences.

It is also regularly argued that if You cause Your Guest to sign a disclaimer and accept the risk inherent in e-Contact with your staff – that will do. It will not.

Your staff are entitled to rely on You to protect them. Your Guest similarly relies on you. Their Employer relies on you. Your stakeholders rely on you to control and secure your confidential information. Data Protection authorities and regulators insist on you taking appropriate technological steps to safeguard the personal data of others.

It is hoped that this Briefing Paper can at least serve as an entrée to the matrix of risks and risk management that the corporation is now newly exposed – by BYOD.

Copyright Information