Wigley & Company
BARRISTERS and SOLICITORS

POLICE ON-LINE PORN BLITZ: IMPLICATIONS FOR OTHER ORGANISATIONS

May 2005

P O Box 10842 • 11-17 Bolton Street • Wellington • New Zealand • Ph. + 64 (4) 472 3023 • Fax. + 64 (4) 471 1833
also at Auckland Ph. + 64 (9) 307 5957 • www.wigleylaw.com

OVERVIEW

The Police problems with online porn look set to spread across the public sector and increase focus on the private sector too. Many organisations are not well set up to combat the office porn problem, partly because they have poor Acceptable Use Policies (AUPs) and those AUPs have not been agreed to adequately by employees.

The porn problem is part of a wider set of issues covered by AUPs including the very significant risk area of security, and other risks such as defamation, copyright, and privacy.

In this article we deal with some of the risks and solutions, focusing on both private and public sector organisations.

There is no perfect solution so there will always be risk. However, risks can be minimised by taking an optimal yet pragmatic approach.

It is very important to factor this into the wider picture. Online porn shouldn't be handled by way of a silo approach.

INDEX

1 Executive Summary

1.1 For an overview of this paper, go to: http://computerworld.co.nz/cw.nsf/UNID/47155218B4D5C8C4CC256FF40075BFCE?OpenDocument

2 Introduction

2.1 Scrutiny of porn on Police computer servers has all the signs of extending out to other Government Departments, with State Services Commissioner, Mark Prebble, getting in behind departmental audit, and improvement of relevant policies[1].

2.2 This is already an issue in the private sector too. There are signs there will be increased focus for all employers. Air New Zealand for example was required in April 2005 to temporarily reinstate four employees it sacked last November for alleged on-line porn. A full hearing of that case is due soon and it shows up some of the potential problems in this area.

2.3 Many organisations are not well set up to combat the office porn problem, which is hard to deal with in the best of circumstances.

2.4 First we'll deal with issues that apply to all employers (public and private sector). Then we will cover public sector issues.

2.5 Like all these things, there is no cookie cutter solution for every organisation. Any response including an AUP and a technology response needs to be carefully tailored to the organisation's risks and needs.

3 Online porn: only part of wider problems to handle

3.1 Well set up organisations will have on-line use policies, often called Acceptable Use Policies or AUPs. They deal not only with online porn but also other aspects such as security, privacy, copyright etc. So porn is just an example of the wider issues that organisations need to deal with by way of AUPs and other responses, such as audit, technical controls and so on. Therefore a response to porn should be part of the overall response to:

3.1.1 Security risk (which has a heavy human component, alongside technical solutions such as firewalls);

---

[1] http://www.ssc.govt.nz/display/document.asp?docid=4480

3.1.2 Copyright (for example, use and distribution at work of pirated or unlicensed proprietary software can expose the organisation);

3.1.3 Privacy (all organisations need to cover this in a policy); and

3.1.4 Defamation (for example, an organisation might be liable for its employee's defamatory statements, just as a library can be liable in defamation (subject to certain defences) for a defamatory book on its shelves).

3.2 It's important not to focus only on porn and ignore the wider picture (for example, for most organisations, security is a much bigger risk).

3.3 Often these AUPs don't cut the mustard because they are inadequately drafted and aren't properly part of the contract with the employee. We are going to focus on those issues, along with other responses such as technical solutions. As porn is part of a bigger picture, this should be treated as an example of the issues to cover in the AUP and other solutions such as computer use monitoring etc.

4 So what's the legal position on online porn in the office?

4.1 A combination of legislation covers this area, including the Films, Videos, and Publications Classification 1993 Act (FVPC), the Employment Relations Act, the Human Rights Act and the Privacy Act. For the public sector, add the State Sector Act (we deal with public sector issues below). Then there are general contract and employment law principles.

4.2 The starting point is the Films, Videos, and Publications Classification Act 1993. This outlines the circumstances in which employees and others could be prosecuted. The important point is that it is only particularly bad porn that justifies prosecution under the relevant definition. This will be in the order of child pornography, bestiality, violent sex and so on. However, much less serious porn should be stopped in an employment context.

4.3 Some deficient AUPs define what is or is not acceptable based on the relevant definition in that Act. But that is only the tip of the iceberg. There is a real difficulty in getting a definition in an AUP for what is or is not offensive. This is further complicated because what is acceptable may depend on context in each case. For example, a particular email sent to a male colleague could have a very different impact than the same email sent to a female colleague. Context is important and varying.

4.4 This means that it is not desirable to take a prescriptive approach to defining what is or is not acceptable in an AUP. While a more flexible approach will in itself create risks (in terms of figuring out whether something is or is not acceptable in a work context) the other solution (such as something based around the censorship legislation) won't work.

4.5 The Employment Relations Act and employment law principles are of course important because they determine when a wayward staff member can be disciplined (ranging from warnings through to dismissal). The employer has to go through normal processes including treating the employee fairly. Rare will be the case where immediate dismissal is justified.[2] Warnings are likely to be needed before that happens.

4.6 Of course, when considering employment law aspects, the starting point is the employment contract and any AUP already in place.

4.7 A well drafted AUP will greatly help the employer in dealing with online porn problems, including by giving clarity around what is and is not acceptable, and what happens as a result.

4.8 Some organisations take the option of stating in the employment contract or AUP that personal use of the internet is banned outright. If that happens, the organisation would need to insist this happens. The reality is that virtually no organisation would fully discourage personal use of the internet. Any organisation like that would be an unpleasant place in which to work. An outfit that has a "*no personal use*" policy in place, but then tacitly permits it, simply doesn't have a leg to stand on when problems arise (that is, in relation to "*no personal use*").

4.9 AUPs must reflect the reality and organisations should walk the talk. That doesn't mean taking disciplinary action in every case. There must be room for discretion, and in some cases the evidence won't be strong enough. More about that below.

4.10 The Employment Relations Act has provisions around sexual harassment which can expose employers to claims by employees. The organisation can end up being liable to staff who receive porn from colleagues and clients.[3]

4.11 Under the Act, sexual harassment involves three aspects: (a) conduct of a sexual nature; (b) the behaviour must be "*unwelcome or offensive*"; (c) there must be "*a detrimental effect on the employee's employment, job performance, or job satisfaction*".

4.12 Employers can be liable to employees where there is sexual harassment (including, for example, inappropriate emails of a sexual nature from a male to a

---

[2] In a different area, there is useful authority on this point in *W&H Newspapers v Oram* [2002] ERNZ 448.

[3] There are similar remedies under the Human Rights Act, which enable employees to pursue a claim not only employment rights but also by way of the Human Rights Commission and Human Rights Review Tribunal.

female colleague) even where a relatively junior staff member is the perpetrator.[4]

4.13 As an example of the risks around sexual harassment, employers can get in a real tangle where an employee maintains that she is being harassed, and the alleged perpetrator denies it. The employer owes duties of good faith, and other duties, to both employees. It must tread carefully in dealing with the situation.

5 What to do about the Acceptable Use Policy?

5.1 The employee should be clearly bound by the AUP. The risk is too large, as to porn, security, copyright, defamation, etc, for the organisational handling of this to be inadequate.

5.2 Because requirements change (for example it may be desirable to update the AUP to reflect new security threats and technology risks), the AUP should stand alone from the employment contract itself and be able to be updated relatively easily.

5.3 This means that the employment contract should have clear reference to the AUP and the ability to update it. However the risk of just having an AUP referred to in an employment contract, without doing anything more, is far too big for organisations. Yet that's what often happens. The policy lurks somewhere in a manual or on the intranet. That might be acceptable if the risks covered by an AUP are minor. But they are not. When a dispute arises, it's important that the employer reduces the risk that the employee can argue that, for example:

5.3.1 He or she never saw the AUP;

5.3.2 The AUP that the employer says was there in fact wasn't (this is a real problem as organisations often don't keep adequate track of what AUP was in place at what time).

5.4 In our experience, these risks are dismissed too quickly. It's important to look at this from a Court or Employment Relationship Authority perspective. Here are 2 examples:

5.4.1 In the Air New Zealand case noted above, 4 of the 8 employees have won temporary reinstatement to their jobs pending full hearing around porn use allegations. One of the reasons for this is uncertainty around

---

[4] Sections 103(1)(d), 108, 111, 116, 117, 118 and 123(d) of the Employment Relations Act deal with sexual harassment. The degree of risk and the appropriate response from the employer depends on whether the perpetrator is (a) more senior in the organisation (particularly a supervisor of the recipient of the harassment) or (b) a fellow employee or client (in which case there is a warning process to be followed). There are separate regimes for (a) and (b) respectively.

"possible failure of the respondent to sufficiently induct and train the applicants in the company's policies and protocols regarding internet use and disclosure of personal passwords".[5]

5.4.2 An employee maintained that he had not seen a key memorandum to all staff, which was closely tied up with the AUP and reinforced the points made in it, as he was away from the office on leave at the time.[6]

5.5 An important practical and legal question is: *"How should the employee acknowledge acceptance of the AUP?"* The safest is handwritten signed acceptance of the AUP (or an actual copy of the AUP). People often ask the question: *"Why would getting something signed in hand writing be better than comparable acceptance on-line?"* Important to consider is how this would stack up in a dispute, when the employee is alleging that he or she has not signed up the AUP. It is almost always possible for a forensic specialist to detect whether or not handwriting is from the employee or someone else. Of course, in the vast majority of situations it will never get to this because the employee will accept that it was his or her signature. When someone click accepts however (whether or not with a key such as a username/password combination) all that is proven that someone has presented as Joe Bloggs, not that this is Joe Bloggs himself. This is a fundamental issue and problem of on-line authentication generally.

5.6 However there are also problems with the offline way of doing things (for example getting documents hand signed). Often mistakes are made (which would not happen on the computer) in the way the document is signed (so they lose their enforceability). Also, it's common, particularly in a large organisation, for such documents to go missing. And there is the practical reality of getting hundreds or thousands of employees to hand sign documents in a large organisation, as against the relatively straight forward step of doing this on-line. Things will change as technology develops, but we suggest the following possibilities in what is just as an important area as the contents of AUPs themselves: the way in which employees buy into them:

5.6.1 **New employees**: they hand sign the employment contract so it is very simple to get them to hand sign the AUP at the same time. Organisations typically have good systems for retention of employment contracts (and that makes retention of the hand signed AUP straight forward too).

5.6.2 **Introduction of new AUPs and changes to AUPs in relation to existing employees:** We deal below with whether and how this can be done, given that new or changed AUPs change the relationship with

---

[5] *Bisson & Others v Air New Zealand* (Employment Relationship Authority (Christchurch Office)) CA 43/05; 4 April 2005.

[6] *Allerton v Methanex* (2000) 5 NZELC (Digest) 98,610

employees. Subject to that, ideally these changes will be accepted in handwriting. In a small organisation that would be best as it is easy enough to do. In a large organisation (employing hundreds or thousands of staff), on balance it may be safer to use a click accept process ideally linked to a username/password in a way that can be established later.

5.7 Importantly, the original documents (or a clear electronic archived record) should be retained for easy reference in case things turn sour. It is easy enough to overlook these things when setting up systems. These points are commonly overlooked. It is another thing in two or three years time to try and unravel what happened, and prove a case against an employee, when electronic/paper records are poor (in our experience this is a particularly common problem).

5.8 It's also important to emphasise that any solution will not be perfect and will involve some compromise and balance in terms of solutions. For example, having a click accept approach with a large organisation may in practice be the only solution (and may in fact be a safer approach on balance). But it will also mean that there is a risk that some people will get off the hook when they might not otherwise do so. Each organisations needs to look at its own needs and decide what to do from there.

6 Reinforcement of the AUP

6.1 The array of issues dealt with in the AUP means that there should be sufficiently frequent reminders. There are various solutions to this ranging from periodic reminders by email through to pop up click accept of the AUP each time the computer is used (some organisations do this although that does seem to be cumbersome).

6.2 All of the risks handled in the AUP together amply justify ongoing training in this area. Probably the most important reason for this is security, which increasingly calls for strong training of staff. Training on security can have bundled with it training as to the other aspects covered by the AUP including porn.

7 "Walking the Talk" Going Forward

7.1 The AUP should not just be filed away and left. The organisation does need to walk the talk including steps noted above such as training, audits and so on. One issue, which pervades the employment area generally, is consistency of approach. Inconsistent approach (or a sudden blitz) has been raised in a number of cases in this area[7]

[7] See for example *Allerton v Methanex* (2000) 5 NZELC (Digest) 98,610. *Clark v Attorney-General* [1997] ERNZ 600 and *Howe v The Internet Group Limited* (Ihug) 1999 1 ERNZ 879.

7.2 For legal and practical employment reasons, the employer should generally strive for a measure of consistency. However there is always room for variation. That may often be forced by the practical and evidential realities of a particular case and the circumstances of the particular employee. As one of the on-line porn cases emphasises, the justice of an individual case takes priority of overall corporate policy.[8]

8 Amendment of the AUP

8.1 An important thing is to reserve the right to amend the AUP to respond to various threats, technology developments and so on. This should be stated in the employment contract and the AUP and a process for doing this should be specified. The employer is required to deal with the employee in good faith, and in view of that, and general contract principles, the employer can't always unilaterally impose those changes without approval from the employee. It is also arguable that before such changes are made, the employer would need to consult with the employee, particularly where the changes are major.

8.2 Of course, changing an AUP does involve changing the nature of the relationship (and therefore, potentially, some of the employment contract terms) as between the employer and the employee. This should generally be possible as a matter of contract, but there are employment law issues on top. First we'll cover contract aspects, and then deal with the employment law overlay. As a matter of contract, the ability to change the contract unilaterally in this way boils down to a question of degree. A recent case (*Barton v Air New Zealand*[9]) confirms that some changes can be made unilaterally. However it is unlikely that wholesale changes could be made. As a matter of contract, the sort of tweaking of AUPs that might take place to reflect developments such as new threats, technology and so on, may well be acceptable from a contractual perspective.

8.3 We turn now to the employment aspects. Employers always have some ability to make changes in the employment relationship such as changing to a degree the nature of the job, to respond to operational needs. This will always boil down to a question of degree. So far in this story, employers have some leeway in changing and updating policies to reflect changes.

8.4 However, particularly where significant changes to an AUP are planned, or an AUP is being introduced for the first time, an employer should consider whether

---

[8] *Allerton v Methanex* (2000) 5 NZELC (Digest) 98,610.

[9] See our article: *Queen's Counsel Battles Air New Zealand: Can a Supplier Unilaterally Change Contract Terms?* at http://www.wigleylaw.com/assets/_Attachments/QCBattlesAirNewZealand.pdf

it would be prudent to provide this in draft first to the employees for comment,[10] and possible change in the light of any comments.

9 Contents of the AUP

9.1 Describing what is or is not acceptable in a sufficiently flexible way – and not using the censorship legislation definitions – is obviously important as we note above. Expanding this to cover related areas of sexual harassment and other communications between staff members will be important.

9.2 A contentious area is the degree to which an employer should be able to look at a staff member's emails and other material stored on the server. If nothing is said about this, often the Privacy Act will be sufficiently flexible to enable employers to vet personal material when problems arise. But there will always be fuzzy areas and therefore risk. It is far better to confirm that the employer (and particular nominated people) are allowed to review all emails (business and personal) and other material on the servers. The Privacy Act and employment law would require that any review is done relatively judiciously and carefully, but the right to do this should be firmly retained including for random audits and for checking when problems are suspected. The risk for employers not only as to porn but other aspects such as defamation, copyright, security etc, is too great to do otherwise.

9.3 The organisation should consider how it frames its ability to review personal emails, depending on the type of operations it undertakes, its culture, and issues around personal privacy in respect of individuals as against the organisation's needs and the reality that personal communications etc are being handled on office computers. However, as noted above, even if a wide ability to review personal material is enabled, implementation by way of specific reviews should be undertaken carefully, by the appropriate people in the organisation (who may well be specified in the AUP) etc.

---

[10] The legal obligations in relation to consultation in this area are not entirely clear. Section 4 of the Employment Relations Act provides that there is a duty on the parties to an employment relationship to deal with each other in good faith. This duty is "*wider in scope than the implied mutual obligations of trust and confidence*" and "*requires the parties … to be active and constructive in establishing and maintaining a productive employment relationship in which the parties are, among other things, responsive and communicative …*". While the only specific reference in section 4 to an obligation to consult the employee relates to redundancy scenarios, arguably there remains a duty (or, at least, it is prudent to consult) to employees to consult before introducing changes to an AUP. It may be good employment and practical sense to do so, even if it adds some complication to the process. It is of course one way in which attention can be drawn to the AUP which is a good thing from an implementation perspective, as well as a legal perspective. For a fuller overview of obligations in relation to consultation see the April 2005 NZLS Law Society, *"Employment Law for Non-Specialists"*. See also *Coutts Cars Ltd v. Baguley* [2002] 2 NZLR 533.

10 Other responses by organisations to the online porn problem

10.1 To cover porn and other risks, organisations would be wise to implement some sort of audit and review programme to periodically check compliance, taking into account the privacy concerns noted above. This would be part of a wider program aligned with the other issues covered by the AUP.

10.2 According to a newspaper report, the Air New Zealand case referred to above illustrates the problem with some of the technology used to monitor online usage. It also illustrates the difficulties when things turn sour and employees are raising arguments and defences. The employees are maintaining that the porn arrived on their PC by way of *"pop up"* and in ways which they couldn't control. We've all had experience of getting unsolicited emails and spam like this. They go on to say that the software used by Air New Zealand to monitor access to such material records access when there has been usage less than 3 minutes. In other words, the software reports that there has been access even if, within a few seconds of receiving the unsolicited material, the employee deleted it.

10.3 In these situations there may well be other evidence. In some cases, the evidence will be relatively uncertain and an employer may decide that it is imprudent to proceed, or it may simply give a verbal warning or do something else other than moving down a more formal employment law path. No solution is perfect and the idea is to set up systems that, in practical terms, work without being too costly and overbearing. After all we are talking about employees who generally should be trusted to get on with their jobs and to use the internet for minimal personal use, without having an unduly *"big brother"* approach from the employer.

10.4 There is of course technology which restrains (but can't entirely limit) sending and receipt of illicit material. One of the problems is that this technology stops quite a wide range of legitimate material from being transmitted. We've all had experience of sending legitimate emails only to have them bounce back for some strange reason.

10.5 In view of these inadequacies in the software, we don't think the point is reached where most organisations significantly increase their legal risk because they fail to have that software in place. However, that will need to be kept under review as new software methods are introduced.[11] Note however that the answer to this issue will depend on the operations of the organisation, the sort of risks involved, and so on. For some organisations, the position may have been reached where the risk is too great from a legal perspective not to have such software in place. For example, if an organisation has a history or a particular

[11] For example, the point may well have been reached by which an organisation would be legally at risk if it does not have anti-virus software installed.

risk around sexual harassment by people outside the organisation, it may be prudent to introduce such software.

10.6 Like all these things, there is no cookie cutter solution for every organisation. Any response including an AUP and a technology response needs to be carefully tailored to the organisation's risks and needs.

11 Are there special issues for the public sector?

11.1 While organisations have reputational issues around porn, the public sector is likely to have greater "*front page of The Dominion*" concerns. This is illustrated by the hue and cry in respect of the porn on the Police servers, compared with the relatively muted response to Air New Zealand's problem in this area.

11.2 The State sector has the employment responsibilities that apply the private sector. But there are additional requirements around being a fair employer etc, under section 56 and 57 of the State Sector Act 1988.

11.3 While there is a list of specific obligations upon State Services employers and their obligations to be good employers[12], these obligations generally don't differ greatly from those owed by private sector employers.[13] However there are some specific obligations that do apply to State Service employers which might create additional obligations in the online porn area, including the requirement in section 56 to recognise the employment requirements of women. There is also the requirement in section 56(3) to ensure "*… that all employees maintain proper standards of integrity, conduct and concern for the public interest*".

11.4 The latter is further confirmed by the NZ Public Service Code of Conduct[14] issued by the State Services Commission under section 57.

11.5 In summary, the State Sector Act and the NZ Public Service Code of Conduct do create high level obligations on both employer and employee that impact on issues such as online porn including exchange of material within the office, harassment, etc. Those high level obligations don't add a great deal to the position. It's the detail that counts (that is, how State Sector agencies reflect the high level principles in material such as AUPs). When State sector agencies are drafting their own AUPs, they need to have regard to the State Sector Act (as well as other legislation such as the Employment Relations Act) and the NZ Public Sector Code of Conduct.

---

[12] Section 56(2).

[13] *French v. Chief Executive of the Department of Corrections* [2002] 1 ERNZ 325.

[14] This is at http://www.ssc.govt.nz/display/document.asp?docid=3508&pageno=1#P8_0

11.6 As we note above, the response to porn is couched within the approach to wider threats such as security. So, for example, government agencies need to have regard to public sector policies which are outline at www.security.govt.nz . For further details see http://www.security.govt.nz/sigs/chapter-8-communications-and-systems-security-management.doc#_Toc10368038.[15]

12 Conclusion

12.1 Legal and reputational problems in the online porn area for organisations have been simmering away for a while. Many organisations – public and private sector – have inadequate AUPs (and fail to make sure that properly signed up and agreed to by employees). Problems can be reduced by optimising AUPs, by introducing audits, training, etc and perhaps adding technology software solutions.

[15] The next level of Govt instructions, NZSIT 100 & 200 series, (issued by GCSB and in need of update), is being replaced later this year by NZSIT 400. NZSIT 400 will be an adaptation for NZ requirements of the Australian Government instructions ACSI-33. The link is http://www.gcsb.govt.nz/nzsit/index.htm (Thanks to Alisdair McKenzie for updating us on this).