

Email & Web Abuse – Monitoring and Investigations

Matthew Pemble

The Preliminaries

Before we start, I suppose that the first thing that ought to be said here is: you really need to get yourself a good lawyer – I am not one, good or bad. More than one if you can afford it – this area is a minefield of technical difficulties, contradictory laws and legal rights, and the usual quagmire that we always get whenever the nice clean (okay, mildly dirty grey) sheet of infosec technology meets the muddy waters of human resources and employment legislation.

Legal Bits (IANAL)

This section is only going to be truly relevant to UK readers, the following is a brief smattering of the laws and other relevant documentation you, or the previously recommended legal advisor, are going to need to consider:

- The Computer Misuse Act 1990.
- The Data Protection Act 1998.
- SI 2000 No 417: The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Information Commissioner's Employment Practices Data Protection Code, Section 3, Monitoring at Work (Draft 7 is latest publicly available).
- The Human Rights Act 1998.
- The Regulation of Investigatory Powers Act 2000.
- SI 2000 No 2699: The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Of course, there is also the relevant employment law, tribunal rules, and internal disciplinary procedures to consider, never mind, business impact, office politics and recent legal and internal corporate precedent. You, or your legal advisor, are now permitted to scream.

What do they all mean? Well, we should all be fairly familiar with the Computer Misuse Act, and the various issues with it, especially the poor definition of a computer and the not-too-great track record in achieving prosecutions. Provided that you are always dealing with computers that are owned by your organization (remembering the problems with both leasing and hosted-out machines, where ownership under the CMA may not be as simple as you think), you are unlikely to run into too many problems here. If in doubt, seek prior written permission for your activities from an "officer of the company" that owns the machines. Careful repetition of this step is likely to provide sufficient cover to deflect the majority of the ensuing blame.

Data Protection, in this case, means finding an appropriate legitimate reason to process the potentially personal and sensitive personal data involved. The Statutory Instrument allows processing without explicit permission for:

- The prevention or detection of any unlawful act and
- protecting members of the public against -
 - (i) dishonesty, malpractice, or other seriously improper conduct by, or the

unfitness or incompetence of, any person, or

(ii) mismanagement in the administration of, or failures in services provided by, any body or association.

However, the precise legal language here can be interpreted to suggest that whereas there is ample clarity regarding investigations, explicit user acceptance of monitoring may still be required. This is made further evident by the (non-binding) Information Commissioner's Code of Conduct still, at time of writing, in both draft and dispute. This specifically excludes "accessing stored information about a particular worker as part of a one-off investigation into a particular problem." Compared to the 47 pages of draft 7, the "Discipline, Grievance & Dismissal" section of Part 2 (Employee Records), is a mere three pages and the rules are hardly onerous.

The Human Rights Act 1998, although its primary purpose is the protection of us honest citizens against the manifold iniquities of the state and its servants, is relevant to us, even in the private sector, as alleged breaches of the Act can be attached to any case brought under other legislation, e.g. unfair dismissal. The two areas of primary concern to us are Article 6 (Right to a Fair Trial) and Article 8 (Right to Respect for Private and Family Life.)

The right to a fair trial, although it expressly deals with criminal matters, is expected, by case law, to have an impact on the structuring of internal disciplinary tribunals and procedures. I would say, "watch this space," but I make no pretence to expertise in that area – you had best make sure that your HR team are on top of the situation as it develops.

As far as Article 8 is concerned, the problem we have is the phrase, "Everyone has the right to respect for ... his correspondence." Specifically, the issue is any lack of indication as to whether that includes or excludes business correspondence, where the Intellectual Property Rights and the liabilities belong to the employer, or not. Best practice suggests, in the absence of strong case law, that we need to treat all

correspondence to or from a named individual, as protected by that (or both) individual's rights under the Act.

RIPA is less of a problem. Skirting viciously around the controversy regarding Part 3¹ and the arrangements for scrutiny and tribunals in Part 4, we essentially have two main parts of the Act. Part 1 neatly brings together the various previously existing bans on interception of communications and extends those to the modern electronic age. It also provides regulations for Law Enforcement and similar personnel getting warrant or other approval to breach the bans and what can then be done with the information gained. Part 2 covers intrusive surveillance and covert human sources – not something that is common in the corporate environment.

However, RIPA does not give much indication as to what corporates, who cannot get a warrant from the Secretary of State, can do, except for limited exceptions for public telecomms providers. This is left to the Statutory Instrument with the appallingly long title, normally abbreviated to “The Lawful Business Practice Regulations. “In a nutshell, this makes it reasonably clear, that as long as both parties to a communication over your private telecomms facilities are informed of the possibility of monitoring², monitoring is probably legal. This is easy enough for a phone call, or even a website access, but a whole lot harder for email. It must be stated here that the draft Information Commissioner's guidance, as currently written, interprets RIPA and the LBPR somewhat more tightly than I have.

Why?

Given all of the above, should we bother? Why can't we just let our staff get on with doing their jobs, and only worry about it once we have a reasonable suspicion that something is wrong? Fundamentally, the two components to the answer are “vicarious liability”; the responsibility all employers have for the actions of their employees at work, regardless of whether those actions are authorized or even in the interest of the

employer; and the unfortunate fact that, up and down hierarchies and across industry sectors, specific employees continually demonstrate that they are not worthy of the level of trust that we would require.

Obviously, and this is not anything that I wish to labour here, we need to monitor for viruses and other malware. No-one, please remember this, can control what they are sent by email. To a more limited extent, the increasing use of spoof and spelling-error domains, pop-up windows and window bombs³, mean that it is not entirely simple to control your Web surfing. The most notorious example of this must be the number of entirely innocent, and rather less so, students of United States political science who have ended up at rather than .gov.

On a personal note, several years ago, I had been asked to look at the issues around upgrading off-site hosting for a customer who was then hosted with host4u.net. Being bounced (username and password required⁴) from the www site, I made the flying, and completely incorrect, assumption, that this was the site for existing customers and that the marketing site would be on the equivalent dot com. That was a mistake – “Kara's Pleasure Palace”, I seem to remember.

However, regardless of error, all organizations do have a limited but notable fraction of users who will deliberately and maliciously abuse the systems, provided to them for work purposes, to display offensive material (racist and sexist, as well as simply pornographic.) All organizations have a duty to provide a safe working environment for their workforce, and this includes freedom from harassment and similar behaviour⁵. At the worst, users downloading or trading in paedophile material may cause the organization, corporately, to be committing a criminal offence by the storage of such images on email or file servers, or within your back-up systems.

Anybody using corporate facilities to duplicate copyright material may, even if the material is for “personal” use, cause the employer to be sued as

an adjunct. Often, the employer would be adjointed simply because they are likely to have more money than the employee.

Statements made by email can be dangerous from the point of view of defamation. The famous Western Union/ Norwich Provident, settled for £450 000, is the classic UK example, illustrating how careful you need to be about the text content of data traffic. Leakage of sensitive corporate data is relatively trivial with modern connectivity – a competitor could even establish an HTTPS bulletin board, to allow their collaborators inside your organization to securely post data, undetectable by keyword or context filtering devices. Inexperienced staff can also accidentally commit you contractually, by careless statements in email.

Finally, if you needed any more encouragement, consider the costs to you, as the employer, in loss of time and in network (and, more especially) internet bandwidth. I have seen 4 megabyte Powerpoints scurrying backwards and forwards across the Internet, with no discernable business benefit, and staff copying entire DVDs across the corporate LAN. These events can cause serious impact to the normal business operations, even if it is just additional data transfer costs.

Policy

It is vital, if you are considering monitoring and investigations, to have an acceptable use policy⁶. The only thing that can be safely assumed, at least until we have more HRA and RIPA case law, is that you are able to take action to protect yourself against employees who are acting in criminal breach of the law. However, much of the activity we are looking to detect and suppress is civil law, breach of standards or merely time-wasting. Accordingly, an Information Security Policy, including a strong Systems Acceptable Use policy, with specific regard to Web and email issues and including a statement regarding monitoring, is a very sensible foundation on which you can build.

Not to say that, in the absence of such a policy, you are weaponless, however the subsequent legal discussions may be considerably more fraught. Mind you, having heard a witness at an employment tribunal admit that it was their signature on the bottom of their previous employer's Acceptable Use Policy, and then flatly deny, under oath, ever having read or even seen the policy, "legally fraught" seems to find these issues no matter how well you prepare.

Monitoring

We will need to quite carefully deliberate on what constitutes the "monitoring" aspect of the title and what constitutes "investigations." These are quite distinct, from a practical viewpoint, and certainly from the legal aspect. In my, non-legally qualified, opinion, monitoring is something that is applied either to everybody or to large blocks of staff, as normal business practice and in the absence of any specific evidence of misconduct.

There are quite specific legal differences between the two states – monitoring, for example, has no privileges under the Data Protection Act; investigations, on the other hand, has SI 2000 No 417 which, as previously stated, provides lawful reasons for processing for a significant range of investigatory means and methods.

Additionally, monitoring data may well be considered "electronic data gathered in the normal course of business practice", therefore generally admissible evidence, whereas investigations data will normally be collected and processed as an exception to practice, and will therefore need to follow forensic evidential standards in order to be admitted to court.

Email monitoring

Yes, we all know and we are endlessly told by people who really ought to think about it in a little more depth, somebody is reading all of your email. Now, I actually read quite quickly and, especially with my home email which is better publicised

than my work email and some-what less expensively protected, I get a huge amount of spam. For anyone to read all of my email would take them probably, combining work and home, about a third of a working day. To be extremely blunt about this, having a quarter of your workforce listening to the other three-quarters is not commercially viable, without considering "Quis custodiet ipsos custodes?"

Assuming, therefore, that it is not practical to read everything, it is necessary to be selective and careful about what you are considering reading. If you are concerned about leakage of trade secrets, keyword filtering may be useful, as might image filtering for preventing sending of obscene material. Five important things to consider:

- Caveat emptor. The technologies and products currently available to assist in this are far from infallible⁷. False positive and negative rates are both well above that considered acceptable in, as a directly relevant example, email anti-virus systems.
- Who is going to review detections?
- How will the privacy of individuals be best preserved until the automated flag is confirmed as a breach of policy?
- What actions are you going to take if you find breaches of policy?
- What is going to happen to the material in the meantime – block, quarantine or pass through?

I have a few favoured premises, based on my experience of running a detection and investigations unit. Firstly, the unit needs to be independent of both the disciplinary process and line management. Human Resources is a bad place to put this, as is Information Systems Technology. Group Risk, Internal Audit or Group Information Security are all better places, each with their own advantages and peculiarities. The correct choice will be very dependent on the culture and current structure of your particular organization.

Systems need to be built to strip and mask user IDs until policy breach is confirmed. Remember, this is a workflow

system – we do not need to rely on this for our forensic evidence: that can be recovered from other systems once the subsequent investigation is under way. Removing any person identifiers, combined with a good audit trail and checks, should help prevent the monitoring team from assisting their friends escape detection and ensuring that the grade or position of the people involved is not considered at this stage of the process.

Material required for further investigations should not be kept within the monitoring system, but should be transferred to a separate investigations database. Material not required, either as a false positive or for policy reasons, should be purged, as soon as reasonably practical. However, you do need to make sure that the system is also capable of providing automated reports to support Data Subject access requests under the DPA. These are likely to be a common feature of Employment Tribunal and court actions, as well as straightforward employee and customer requests.

In terms of cutting down on the amount of material needing manual review, there is one useful trick I have uncovered. As far as offensive material goes, the stuff seems to come in waves, with a two or three month cycle where there is a volume change and the "old favourites" cropping up from time to time. Therefore if you have a formalised grading system for images, a specific file recognition system, using hashing and other metrics will allow automatic grading of easily more than 85% of the emails. Coupled with a good boundary selection algorithm, you should be able to bring the total volume down to something manageable within a decent sized team.

About the author

Matthew Pemble is an experienced security architect, auditor and investigator. Having left the military for the purgatory of consultancy, he has finally escaped to run the Security Compliance team for a major

international bank. Qualified as an engineer, penetration tester and forensic analyst, he is now in charge of a small team at putting in to practice many of the views expressed in these articles.

References

¹Government, or Law Enforcement, access to plain text of encrypted data and /or the encryption keys themselves.

²As in robot woman on end of telephone, "this call may be monitored for training and security purposes."

³Never mind more malicious html such as 1-pixel resized, and therefore unnoticed by even the most alert user, pornographic, or worse still, jpegs!

⁴Nowadays, it just comes back with a HTTP 403 (Forbidden) error. The dot com is blocked by our corporate filter under "Sex", so probably hasn't changed much!

⁵The UK Employment Equality Act 1998, states that an employee is entitled not to be discriminated or harassed in the course of their employment on the

grounds of gender, marital and family status, sexual orientation, religion, age, disability, membership of the travelling community and race. Harassment is defined as including, "the circulation of written words, pictures or other material which a person may reasonably regard as offensive"

⁶The draft IC guidance mandates this as one of their benchmarks.

⁷Oh, and in case this is news to anyone, some sales people are known to stretch the truth.

BASEL II: Heralding the Rise of Operational Risk

David Porter, Head of Financial Services Risk, Detica

Basel II - a growing concern

The media coverage around the Basel II Accord is steadily growing, as financial institutions engage seriously with the details of compliance. Basel II is one of the biggest financial shake-ups in recent times, which will eventually lead to new rules and regulations for banking globally. Banks will need to have their processes and systems in place by the start of 2007, which is when the Basel Committee on Banking Supervision plans to implement the Accord.

The purpose of Basel II is to ensure that financial institutions manage risk so that they have the capital to cover exposure to debt. Basel II will be regulated by the FSA in the UK and through CAD-3 on a European basis. Banks will have to carry out a fundamental review and overhaul of their processes and systems in order to achieve compliance. Technology will be at the core of their strategies to meet Basel II requirements. Estimates of the investment needed to comply with the new Accord vary widely, with little consensus evident currently. What does seem certain is that significant technology investment will be required, amounting to hundreds of millions of pounds in the UK financial services industry alone.

The rise of operational risk

It is interesting how the management of Basel II programmes has fallen mainly into the hands of those in charge of operational risk who are now receiving full backing from top management. This perhaps reflects the desire by banks to get a stronger grip on operational risk, credit risk being a more mature modelling discipline. Indeed, operational risk appears to be entering a golden age. Its profile has been raised — "We must get a key risk indicator (KRI) for this" and similar risk vocabulary is now being used at board level — and greater awareness is starting to trickle downwards through the corporate culture.

Basel II is enabling those involved in risk to finally get risk management to permeate corporate culture and decision-making

processes. What was always viewed as "nice to have but we can't afford it right now" is no longer the case. The goal of 'designing-out' risk, whenever any new product, process or system is developed, is becoming a realistic proposition.

Those who work in risk are no longer seen as a nuisance factor or pointing the finger. Instead, they are increasingly viewed in meetings as being there to help and are becoming the glue that is bringing together formerly disparate islands of decision-making and data storage.

Programme management and cultural shift

Basel II is more than just a very large project. Like CRM, it is a complex business change programme, comprising a series of inter-dependent projects that need to be orchestrated effectively. A programme must be structured and managed using best practice principles and techniques in order to ensure that it delivers successfully, i.e. on time, within budget and to the right quality.

Basel II should be viewed in conjunction with all other programmes, be they compliance-driven, marketing-driven or otherwise. It may be possible to combine different programmes, or sub-elements of programmes, into one programme. One example is the overlap between Basel II and International Accounting Standards (IAS). Another is the potential overlap with tactical anti-money laundering and anti-fraud initiatives.