Proactive Monitoring of Illegal Content access in Schools
IT Usage Monitoring (Education) Pilot Project

August 2016

Contents

Background

In April 2006, SWGfL, facilitated by its managed service partner RM, implemented proactive monitoring across its network, identifying any user in a school attempting to access illegal child abuse images online. The pioneering project was instigated by SWGfL in collaboration with RM, Avon and Somerset Police and North Somerset Council following a series of local events and national

strategic changes. These local events highlighted the growth in use of the Internet to access child abuse including

- Priest is jailed for child porn (Sept 2004) - http://news.bbc.co.uk/1/hi/england/somerset/3624550.stm
- Teacher jailed after child porn find (July 2003) - http://news.bbc.co.uk/1/hi/england/devon/3106639.stm
- Abuse teacher caught through website (June 2003) - http://news.bbc.co.uk/1/hi/england/wiltshire/2997926.stm

Coupled with these local events, in 2004 following the public inquiry lead by Lord Laming into the murder of Victoria Climbie (2000) the Every Child Matters [1] programme introduced major policy reforms around child safeguarding for agencies and authorities. It was clear that the online protection of children required significant transformation.

In 2006, as it still is today, the 'taking, making, distributing and sharing of an indecent photograph of a child' [2](or mis named child pornography) is an offence[3], carrying a tariff of up to 10 years imprisonment.

The Internet Watch Foundation (IWF[4]) was established in 1996 'to fulfil an independent role in receiving, assessing and tracing public complaints about child sexual abuse content on the internet' and in 2004 launched the 'Child Sexual Abuse Images and Content URL List'[5] which it provided to its members.

The IWF URL list was largely used by providers to simply block access to websites identified by IWF as containing illegal child sexual abuse content, highlighted by BT in 2006[6].

Anyone with an interest in making, producing or distributing images of child sexual abuse may present a threat to the safety or wellbeing of children. Exclusively operating in within the 2,500 south west schools, SWGfL and partners determined that simply blocking access to child sexual abuse images (which was already active) was insufficient and would be an advantage to identify when access to this online material was attempted. The Proactive Monitoring project was initiated.

[1] https://www.education.gov.uk/consultations/downloadableDocs/EveryChildMattersSummary.pdf
[2] http://www.cps.gov.uk/legal/h_to_k/indecent_images_of_children/
[3] Section 1 of the Protection of Children Act 1978 (PCA 1978); and Section 160 of the Criminal Justice Act 1988 (CJA 1988)
[4] https://www.iwf.org.uk/
[5] https://www.iwf.org.uk/members/member-policies/url-list
[6] http://www.theregister.co.uk/2006/02/07/bt_cleanfeed_iwf/

Project Outline and Scope

RM [7](SWGfL Managed Service provider and IWF member) was already blocking access to any and all websites identified by IWF by implementing the CAIC URL list, but if an attempt was made a simple filter page would be presented to the user.

The Proactive Monitoring Project built on this by automating a daily (overnight) analysis of all URL requests processed by SWGfL (ie every webpage that every user across every school requests) against the IWF CAIC URL list. The result was the identification of a user attempting to access child sexual abuse content from within a connected south west school. This simple analytical process revolutionised the central identification of potential threats to the safety and wellbeing of children across the region. It has been likened to finding a needle in an digital haystack of needles

Given the function and legislation (see Annex 1),clearly this monitoring activity required notification and formal approval from users and in June 2005 the process of informing 2,500 schools commenced. The process to obtain formal approval from 2,500 headteachers took 9 months to complete, concluding in March 2006.

Proactive monitoring across the entire SWGfL network commenced on 1st April 2006.

Pilot Status

Following discussions in 2007 to both extend the benefits to other areas of the UK as well as regulate the extent of monitoring; the project was adopted by the Home Office and lead by CEOP. The project was afforded pilot status by the Home Office to enable the activities to continue.

The scope of the pilot project was to perform monitoring was limited to educational establishments and specific territories.

Alerting Process

The process to manage alerts received much attention and central involvement from law enforcement. SWGfL has seconded specialist police officers from Avon and Somerset Police's Internet Child Abuse team to provide the liaison and management of the alerting process. Following the completion of the overnight data comparison process a daily report is produced and issued. If a match is found, ie the comparison process determines that a user has requested a website listed on the IWF CAIC list, the report lists the school from which the access was requested as well as the time. This information is then acted upon, instigating the usual law enforcement response and potentially investigation

[7] http://www.rm.com/

Pilot Project Output

Since instigating proactive monitoring, 12 alerts have been raised resulting in law enforcement action. Whilst most resulted in action being taken, it is not deemed appropriate to include case details, below is a summary of the cases

Caution	1
Charged	1
Insufficient evidence	6
Not in public interest	2
False positive	2

Conclusions

The pilot project is considered a success, in that technology and information has been effectively and efficiently utilised in the interests of the safety and wellbeing of children; threats to their safety have been removed. The process has not generated undue false positives that could compromise the capability of law enforcement to respond. The system has not required any additional burden on schools or colleges.

Recommendations

The capability for proactive monitoring of attempted access to illegal online content in schools should be extended to all UK schools and to any agency or organisation who works with children

Annex 1 - Lawful Monitoring in the Workplace

Aim

To outline the legislation that regulates the monitoring by employers of their staff whilst in the workplace.

Background

With the use of internet and external email networks within the workplace, employers are concerned with monitoring the activities of their employees. In certain circumstances the employer could be held to be vicariously liable for the actions of their employees done in the course of duty and can be held responsible as the owner operator of the email system. Policies around monitoring in the workplace have grown with the growing interest in employers of monitoring and surveillance.

The Law

Monitoring in the workplace is a regulated activity. Employers who do monitor activities of employees on intranet, internet and telephone systems must have regard to the legislation and comply with all its obligations. This legislation includes the following:

1. The Data Protection Act 1998
2. The Regulation of Investigatory Powers Act 2000
3. The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
4. The Human Rights Act 1998

Guidance has also been produced by the Information Commissioner's Office: The Employment Practices Data Protection Code: Part 3: Monitoring at Work

The Data Protection Act 1998

This Act confers an obligation on employers to tell staff when monitoring is taking place and why. There is also the obligation to ensure that any monitoring is fair and lawful to employees whilst being proportional to the aim which the employer seeks to achieve.

Covert monitoring can only occur when one of the exemptions apply.

RIPA

Interception of emails, telephone calls and Internet access will only be permitted where the employer has reasonable grounds to believe that both the sender and recipient have consented.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

These regulations allow employers to intercept communications that are relevant to their business without the express consent of their employees but only in limited circumstances, e.g.:

- To ensure compliance with regulatory rules
- To protect the security of internal systems
- To investigate any unauthorised use of systems
- To prevent and detect crime

Employers are expected to make all reasonable efforts to ensure staff using their systems know that interceptions such as those mentioned above may occur.

The Human Rights Act 1998

Employers must comply with this legislation and interpret it consistently with the European Convention of Human Rights. Article 8 provides for a qualified right of respect for private life and therefore any interference with this must be justified on grounds of necessity and proportionality and in accordance with the law.

The Employment Practices Data Protection Code: Part 3: Monitoring at Work

This Code is not legally binding but produced as guidance and best practice. It does appear to go further than the Regulations mentioned above and stresses the importance of the individual's privacy over routine and untargeted monitoring.

Conclusion

This is a short note merely outlining the legislation and regulations that aim at ensuring lawful business monitoring occurs in the workplace.