



Outcomes of E-Safe Education Ltd's review of image transgressions

June 2009

This document may not be reproduced or published in whole or part without the express permission of E-safe Education Ltd.

Contents

Objective	3
Overview	3
Scope	3
Data source	4
Categorisation approach.....	4
The data set	5
Media Sources	5
Summary	6
Interpretations	7
Contact information	7

Objective

“The objective of the review was to determine the degree of vulnerability, if any, of children and young people being presented with, or gaining access to inappropriate imagery through a school’s ICT provision.”

Overview

Between the period of December 2008 and June 2009, E-Safe Education Ltd undertook a review of all data that had been reported through to its e-safe education managed service, hosted e-safety services and a customer evaluation programme. The forensic data examiners at E-Safe Education Ltd reviewed the detected image transgressions¹ in order to better understand how and where potentially harmful, pornographic or potentially illegal imagery² might typically present itself on an end user’s school computer.

Scope

The e-safe education solution has the ability to detect images within the browser as well as offline sources such as desktop office applications and even remote devices such as USB drives and DVDs when plugged into a computer. The solution can be set to respond in various ways depending upon the requirements of the school or college. These range from passive recording, i.e. warning the user with a personalised message; actively interdict the image and replace it with a benign image or redirect the user to a warning page that explains the Acceptable Use Policy i.e. if the number of unacceptable images exceeds five on a single page.

A second image detection engine actively checks for images that are viewed in any application outside of the web browser and responds in a similar way to the core engine. This detection engine is optimised to analyse images that do not contain any text references. It analyses images for amounts of flesh tone, body mass, clothing or hair, limb structure and whether a head is present. Consequently, there is an increased chance of images being reported that ultimately prove to be acceptable i.e. a popular singer posing in a bikini. The specialist reviewing the images would determine whether the image was unacceptable based upon pre-defined standards.

Given that the objective was to evaluate what was happening with non-internet browser based images, the scope of the data review was focused on the latter process of image detection i.e. looking specifically at images without text.

The decision to analyse this aspect of the image detection was taken as it was clear that the e-safe education solution browser detection engine was

highly effective in detecting and interdicting images, therefore adequately mitigating the associated risk of an image being viewed by a user. Its proven ability and accuracy to detect and interdict any transgressing images was already acknowledged³. Furthermore, once detected, an establishment's filter engines were updated to restrict access to identified URLs where inappropriate web content resided.

Data source

The data reviewed consisted of some 308,467 transgressing records of images derived from approximately 6000 devices⁴ installed in a range of primary schools, secondary schools, Pupil Referral Units, and Looked After Children computer devices. The process operated in a manner that ensured that E-Safe Education customers' data confidentiality was not breached. No reference was made to individual users or devices. A process of categorisation detailed exactly how and what was actually being detected.

For the purpose of the review, specific attention was paid to some 32,400 image transgressions that were positively identified as being recorded solely outside the internet browser. The media sources section, further down this document, details examples of where images would typically be detected.

Please note: as a matter of course, every transgression recorded by the e-safe education solution was, and is, reviewed personally by an expert forensic data examiner.

Categorisation approach

The definition of what is an inappropriate image can generate much debate as it is subjective for a number of reasons. Some examples cited in the public domain to support this view centre on the potential effect and impact of offensive imagery. This may be based upon the user's personal development and level of maturity. This complex area is explored in detail in a comprehensive research study published in November 2006⁵.

An example of this might be an image contained in a popular 'lads magazine' of a risqué image of a popular model in the public eye. Depending upon the school's ethos or outlook, this type of issue might be addressed in one school's Acceptable Use Policy very differently from another school with a similar demographic footprint. The process undertaken by E-Safe Education's examiners identifies whether an image detected as a transgression, meets or exceeds the baseline definition of an unacceptable image⁶, reports the transgression to the nominated contact enabling the establishment to execute its policy and procedures. Images considered as pornographic within an academic environment are deemed as extremely unacceptable (unless utilised in PSHE specific activities perhaps) and

extreme pornography is covered by legislation²; Either way, both are most likely to be extensively covered within a school or Local Authority's policies and procedures.

The data set

From the identified transgressing data originating from outside the internet browser, 3150 images contained data that was defined as meeting or exceeding the baseline of an unacceptable image⁶ or pornography. It was evident that none of these images had either a word or contextual phrase reference that could, or would have triggered an alert through a contextual word/phrase package if it was installed on the PC.

Media Sources

Given that all of the images highlighted throughout this research were detected outside of the internet browser, it was determined that a useful exercise would be to determine how these images were most likely to have been brought onto a computer. E-Safe Education believes this is pertinent, particularly as internet filtering is quite often seen as the 'weak link', sometimes unfairly, in computer-related e-safety matters.

After thoroughly inspecting each transgression record, it was determined where each image transgression was most likely to have originated at the point of recording. The following source categorisations were utilised:

- Generic O/S integrated image viewers
- Generic O/S integrated image editing applications
- Multiple professional image editing applications
- Multiple downloading/File sharing software application
- Professional presentation applications
- Word Processing applications
- Portable Document viewers
- Locally installed email readers/viewers
- Folder/Directories on a local file server
- Folder/Directories on a local hard disk drive
- Folder/Directories on a Mass storage device Hard Drive
- Folder/Directories on a Mass storage device Pen Drive
- Folder/Directories on a Mass storage device Digital Camera
- Folder/Directories on a Mass storage device Mobile Phone
- Folder Directories via Inexpensive Media device CD/DVD

Please note: Whilst this is not an exhaustive list, it demonstrates the significant areas of potential vulnerability in a school.

Summary

Upon reviewing the research data, there were several points to note and indicators that could be evolved into recommendations for educators and policy makers.

Aside from the fact that there is still a significant number of images that successfully present themselves on-screen through an internet browser despite a filtering provision in place, there is the ability to manage the risk of exposure to web-based material through comprehensive image interdiction.

It is clear that inappropriate imagery is present on systems used by minors under the age of 18 and that there needs to be controls and processes in place that identify the situation and rectify the problem through education and positive behavioural modification.

Educationalists, Local Safeguarding Children Board members and policy makers need to acknowledge that there are multiple points of entry for inappropriate material and whilst this research focuses on imagery, there should be an acknowledgement that other materials are likely to be accessed through these same routes.

Those who safeguard children need to recognise that the technology that they may currently deploy may address some of the e-safety issues. However, reliance on these technologies should not be absolute as they may present a false sense of security.

The data review reveals that a significant percentage of transgressing images (deemed unacceptable and inappropriate for users under 18 to have sight of) are passed through to school networks despite the fact that:

- every single record of transgressing data was reviewed and classified with established protocols for escalation to a school's senior management team when necessary
- all senior educators were trained on how the Managed Service would feed back data into their pastoral, behavioural and escalatory procedures
- as an end user transgressed, they had been presented with a tailored warning explaining why it was inappropriate and what the consequences of continued transgressions might be

In conclusion, this research highlights that any e-safety provision that is implemented needs to be sufficiently resourced to ensure that all of the reported data is reviewed. For educators and policy makers, it needs to be recognised that the technologies utilised in an e-safety provision must be comprehensive. As a pre-requisite, it must be able to detect inappropriate

and unacceptable imagery from both within the internet browser and from any other source on a PC that is likely to be utilised by an end user.

As the research was reviewing data in a controlled environment where a significant amount of data had been recorded, it is highly likely that, in an unmanaged environment, there is a significantly higher chance of incidences of unacceptable and inappropriate images occurring in schools that deployed similar measures as utilised within the managed service provision.

Interpretations

¹ A transgression is a term that defines the reporting of an incident by the automated detection systems of the e-safe education client monitoring solution. Until the transgressing data is evaluated by either a forensic examiner, expert in detection and evaluating the latest e-safety threats, impartiality is maintained until the reported data is either confirmed as an act that has violated the prevailing Acceptable Use Policy or that it is deemed a “false positive” which is benign data.

² Illegal imagery, as defined by the latest revision of legislation found at:

<http://www.justice.gov.uk/docs/extreme-pornographic-images.pdf>

³ The graphic interdiction engine was evaluated independently by a sovereign nation’s government agency and they rated technology as 96% effective in detecting pornography within the browser.

⁴ The approximation of the 6000 devices is stated as the system records all devices with the clients involved and it is acknowledged that during the course of the review, a small number of machines may have been replaced or re-imaged by an establishment’s technical staff.

⁵ This refers to the ‘Report on internet usage and the exposure of pornography to learners in schools’ by Iyavar Chetty and Antoinette Basson

⁵ The definition of an unacceptable image is one that depicts partial or full nudity, imagery of a person in a state of undress that is deemed sexual or provocative. Other image types in this scenario could be that of a real image of an actual sexual act by persons or person or depicted in animation, images of violent acts, obscene depictions or those that intimate sexualisation.

Contact information

For any questions or clarifications regarding this document should be directed to: ManagedServices@esafeeducation.co.uk