INTERNATIONAL ELECTRONIC EVIDENCE

Edited by

STEPHEN MASON

British Institute of International and Comparative Law

Published and Distributed by
British Institute of International and Comparative Law
Charles Clore House, 17 Russell Square, London WC1B 5JP

British Library Cataloguing in Publication Data
A Catalogue record of this book is available from the British Library

ISBN 978–1–905221–29–5

Typeset by Cambrian Typesetters
Frimley, Surrey
Printed in Great Britain by Biddles Ltd,
King's Lynn

INTRODUCTION

Stephen Mason

The final AEEC Conference held at the Ritz Hotel in Madrid on 14 December 2006 provided an overview of the results of the Admissibility of Electronic Evidence in Court project, partly funded by the European Union.[1] A number of those present at the conference expressed the view that it would be good to have a European-wide law on electronic evidence for criminal proceedings (although if such a law were introduced, it should be for digital evidence, or both analogue and digital evidence). This was also noted in the booklet produced to summarize the findings of the project.[2] Perhaps these comments were made in the knowledge of the *Corpus Juris* project,[3] but had those who offered such comments been aware of the *Corpus Juris* project and the subsequent criticisms of the undertaking, they may have reached the conclusion that given the cultural and political diversity of the economic union that makes up the European Union, such supra-national plans are best left for those that wish to make the European Union Member States a single political entity. The *Corpus Juris* project produced some excellent materials that deserve to remain at the forefront of any future plan (if there is such a plan) to introduce a European-wide law on digital evidence, whether it is for criminal proceedings or both criminal and civil proceedings. The aim of the *Corpus Juris* project was to 'elaborate a number of guiding principles in relation to the protection in criminal law of the financial interests of the European Union'.[4] In essence, the project proposed a mixed regime. National and European Community elements would be combined in such a way that Member States, and not the European Union, would apply the criminal law. Eight offences with penalties were set out with the purpose of protecting the

[1] The project was undertaken between 4 November 2005 and 28 February 2007 and was undertaken by Cybex in Barcelona with financial support from the AGIS Programme, European Union, Director General Justice, Freedom and Security.

[2] *The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime* (Cybex, Barcelona, 2005) 33.

[3] M Delmas Marty and JAE Vervaele, *The Implementation of the Corpus Juris in the Member States*, Volume 1 (Intersentia, Antwerp, May 2000); Volumes 2, 3 and 4 (Intersentia, Antwerp, 2001).

[4] Delmas Marty and Vervaele, *The Implementation of the Corpus Juris in the Member States*, Volume 1 (n 3) v; see also JR Spencer, 'The *Corpus Juris* project and the fight against budgetary Fraud' (1998) 1 Cambridge Yearbook of European Legal Studies 77–105 and JR Spencer, 'The *Corpus Juris* project—has it a future?' (1999) 2 Cambridge Yearbook of European Legal Studies 355–67.

financial interests of the European Union. It was proposed to appoint a European Public Prosecutor, comprising a Director of European Public Prosecutions and European Delegated Public Prosecutors. The European Public Prosecutor was to exercise its powers of investigation throughout the territory of the European Union, which meant the powers were mostly devolved to the Member States. Judicial control was to be exercised by an independent and impartial judge, called a 'judge of freedoms' to be nominated by each Member State, and the offences were to be tried by the national courts.

Two themes dominated the study. The first considered whether the project was feasible in relation to the Member States. This meant the participants had to analyse the legal framework and points of compatibility with constitutional law, criminal law and procedure in the Member States. This study was carried out article-by-article in 15 of the Member States. The second theme concentrated on specific issues relating to horizontal cooperation between Member States and vertical cooperation between Member States and the European Union. The criminal justice systems were analysed from the point of view of the draft of the *Corpus Juris*, and the possibilities and obstacles relating to horizontal and vertical cooperation were identified. Since *Corpus Juris*, the pace quickened. An amendment to Article 280 of the EC Treaty was proposed in a Communication from the Commission, 'Additional Commission contribution to the Intergovernmental Conference in institutional reforms, the criminal protection of the Community's financial interests: a European Prosecutor'.[5] No action was taken on this paper, so the Commission adopted the 'Green paper on criminal-law protection of the financial interests of the Community and the establishment of a European Prosecutor',[6] and the Green Paper was subsequently followed up with a 'Follow-up report on the Green Paper on the criminal-law protection of the financial interests of the Community and the establishment of a European Prosecutor'.[7] The Treaty establishing a Constitution for Europe, signed in Rome on 29 October 2004, provided for the establishment of a European Public Prosecutor, and the Draft Treaty amending the Treaty on European Union and the Treaty establishing the European Community, discussed and agreed at the Intergovernmental Conference (Heads of State or of Government) meeting in Lisbon on 18 October 2007, has also provided for the establishment of a European Public Prosecutor in new Article 69i, which in turn is reinforced by the provisions of new article 69j, replacing Articles 68 and 69, requiring greater police cooperation across Member States. This is part of a wider remit, in that judicial cooperation in

[5] Brussels, 29 September 2000, COM (2000) 608 final.
[6] COM (2001) 715 final.
[7] COM (2003) 128 final.

criminal matters is expressly provided for in Article 69e, which replaces Articles 66 and 67. In particular, Article 69e(2) provides as follows:

> 2. To the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension, the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules. Such rules shall take into account the differences between the legal traditions and systems of the Member States.
>
> They shall concern:
> (a) mutual admissibility of evidence between Member States;
> (b) the rights of individuals in criminal procedure;
> (c) the rights of victims of crime;
> (d) any other specific aspects of criminal procedure which the Council has identified in advance by a decision; for the adoption of such a decision, the Council shall act unanimously after obtaining the consent of the European Parliament.
> Adoption of the minimum rules referred to in this paragraph shall not prevent Member States from maintaining or introducing a higher level of protection for individuals.

It should be noted that Article 69e(3) allows for a form of opt-out, which may be used by more Member States than those framing this text appreciate. New Article 69h aims to introduce crimes against the European Union by providing Eurojust with additional powers:

> 1. Eurojust's mission shall be to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States or requiring a prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities and by Europol.
>
> In this context, the European Parliament and the Council, by means of regulations adopted in accordance with the ordinary legislative procedure, shall determine Eurojust's structure, operation, field of action and tasks. These tasks may include:
> (a) the initiation of criminal investigations, as well as proposing the initiation of prosecutions, conducted by competent national authorities, particularly those relating to offences against the financial interests of the Union;

(b) the coordination of investigations and prosecutions referred to in point (a);
(c) the strengthening of judicial cooperation, including by resolution of conflicts of jurisdiction and by close cooperation with the European Judicial Network.

In any event, the work undertaken by the *Corpus Juris* project, the erudite study edited by Mireille Delmas-Marty and JR Spencer[8] and, in a small way, this text (together with what might be termed a companion volume),[9] may serve to illustrate the cultural and legal problems that face any project that intends to achieve a certain degree of harmony across the European Union Member States, although it may be asked why such a project should be limited to the European Union.[10]

A. DEFINING TERMS

The Admissibility of Electronic Evidence in Court project could not find a definition of electronic evidence, although references were found in national legislation that referred to electronic evidence.[11] Whilst it might be useful to clarify and define the term 'electronic evidence', a definition is not necessary for the purpose of legal proceedings because most jurisdictions admit analogue and digital evidence as a form of document, and the meaning of a document invariably extends to anything recorded in any form, which must be right.

[8] M Delmas-Marty and JR Spencer, *European Criminal Procedures*, (CUP, Cambridge, 2006).

[9] S Mason (ed), *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths, London, 2007).

[10] The reader is directed to a number of useful articles that appeared in the *ERA Forum Special Issue on European Evidence* in 2005, including PJ Cullen, 'Dealing with European Evidence: National Practice and European Union Policy' 4–8; K Macdonald, 'The Reform of Procedures for Dealing with Foreign Evidence: A Practitioner's Agenda' 9–16 and JR Spencer, 'An Academic Critique of the EU Acquis in Relation to Trans-Border Evidence-Gathering' 28–40; see also C Van Den Wyngaert, '*Corpus Juris*, European Public Prosecution and National Trials for Eurocrimes: Is There a Need for a European Pre-Trial Chamber?' (October 1999) 24 Agon 4–8, and K Hamdorf, 'The Role of the European Anti-Fraud Office in the Process of EU-Enlargement' (2001) 31 Agon 8–14. See further K Aromaa and T Viljanen (eds), *International Key Issues in Crime Prevention and Criminal Justice* (European Institute for Crime Prevention and Control, Helsinki, 2006); and M Joutsen, *The European Union and Cooperation in Criminal Matters: the Search for Balance*, HEUNI Paper No 25 (The European Institute for Crime Prevention and Control, Helsinki, 2006): both papers available online at <http://www.heuni.fi/>.

[11] *The Admissibility of Electronic Evidence in Court: Fighting Against High-Tech Crime* (Cybex, Barcelona, 2005) 27.

1. Suggested Definition of Electronic Evidence

The term 'electronic evidence' is a generative term for two types of evidence: 'analogue evidence' and 'digital evidence', and the following definition is proffered:

> Electronic evidence: data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication.[12]

To a certain extent, the introduction of evidence in analogue format was well within the world-view of judges and lawyers for the reason that the concept of a machine that creates an output is relatively easy to follow: whether it is a roll of film from a camera, or a machine for measuring the amount of alcohol in the breath. Examples of evidence obtained from analogue devices include vinyl records, audio tape, photographic film, and telephone calls made over the public switched telephone network. Analogue systems or products generate evidence in the form of data that is capable of being produced in a permanent form. For instance, a camera (depending on the type of camera: a camera that produces instant photographs does not have a negative) will create primary evidence in the form of a negative transparency or plate, and secondary evidence of the photographs taken from the film. There is a significant difference between analogue evidence and digital evidence, mainly because evidence that is the product of an analogue device is only stored on a carrier such as paper or a photographic film, or it may not even be recorded, but it can be a continuous reading, such as early versions of radar. The evidence that is recorded by an analogue device is capable of being manipulated, and a well-known example was the removal of the image of Davidovich Bronstein (Leon Trotsky) from early photographs that included images of Vladimir Ilyich Ulyanov (Lenin) in Soviet Russia. It takes great skill to alter the negative of a photographic film, but alterations can be detected. However, in comparison, digital images can be altered with ease. Examples of digital data include anything that has been created or stored on a computer, or is made available by way of the Internet, including CDs, DVDs, MP3s and digital broadcast radio. The essential point about digital evidence, which is not readily understood by many judges and lawyers, is the complexity of the topic and the nature of the characteristics of digital evidence. By failing to have even a basic knowledge of the subject, lawyers and digital evidence specialists responsible for investigating a case and deciding whether to initiate criminal

[12] Mason (n 9) para 2.03, which also includes a discussion of the elements of this definition.

action against an individual, are in danger of committing grave errors. It is for this reason that judges, lawyers and legal academics should consider it to be of vital importance that they begin to understand digital evidence.

The term 'electronic evidence' is used widely, but it is commonly used to denote digital evidence, which adds to the confusion. It is suggested that the term 'electronic evidence' is a generative term, rather than a specific term, in that it encompasses all forms of data, whether produced by an analogue device, or in digital form. The two forms of evidence should not be confused, because different evidential and procedural requirements apply to each form of evidence.

B. CASE STUDY: *STATE OF CONNECTICUT V JULIE AMERO*[13]

A serious concern with respect to digital evidence is where those involved in justice systems (whether civil or criminal) fail to fully appreciate that evidence in digital format, now virtually ubiquitous in that it appears in almost every case in one form or another, is far more complex than those taking part in the proceedings might be aware. The lack of any understanding of digital evidence by the lawyers and the judge is usually demonstrated by the way a case is conducted, and the prosecution of Julie Amero by the State of Connecticut serves to illustrate why judges and lawyers must take steps to purge their minds of any ignorance in relation to this topic. This is one of two case studies included in this chapter, both from the United States of America. The second case study, *State of Arizona v Bandy*, illustrates the nature and interpretation of the digital evidence that a prosecutor must consider before deciding to proceed against an individual. Two cases from the United States of America have been chosen simply because cases are more frequently reported, are more freely available and are easier to obtain because they are in English. That cases from the United States of

[13] Docket number CR-04-93292; Superior Court, New London Judicial District at Norwich, GA 21; 3, 4 and 5 January 2007, before The Honorable Hillary B Strackbein, Judge, with a jury of six; prosecuting: David Smith, Office of the State Attorney; defending: John F Cocheo, 111 Huntington Street, New London; transcription of the stenographic notes made by Gail C Schor, a registered professional reporter: Note that page 334 of the transcript is a repetition of page 324. Reading the text at the bottom of page 333, if the reader adds the words 'in the' to the text beginning on page 335, it would appear that page 335 is the follow-on page to page 333, and by some mistake, page 334 has been mistaken with page 324. The text on page 333 and 335 appears to flow quite logically, and there does not appear to be any missing text. A copy of the transcript was originally available on the Norwich Bulletin website at <http://www.norwichbulletin.com>, but it has since been removed. At the time of writing there were two versions available, a scanned copy of the transcript in pdf format, and a complete transcript with extraneous comments and deletions in html format at <http://julieamero.blogspot.com>. Only the page number and line numbers of the transcript are referred to in footnotes hereafter.

America have been used does not suggest that such cases are unique to the United States, and no disparagement is meant by discussing these cases in this chapter. Although the cases are from the United States of America, it will be disappointing if lawyers and judges, from whatever jurisdiction they happen to be in, adopt the view that the facts surrounding either case are not relevant to them. The facts of both cases are relevant to every jurisdiction on earth, and to adopt the view that what happens in a court other than the home jurisdiction is irrelevant, is to fail to grasp that digital evidence transcends the boundaries of individual jurisdictions, and it will be increasingly necessary for lawyers to obtain evidence from other jurisdictions, regardless of the nature of the case they are dealing with. If lawyers and judges do not begin to make themselves aware of digital evidence, it is inevitable that the justice system will be the subject of the sort of unwelcome adverse media attention given to the Julie Amero case in particular in due course.

The prosecution and subsequent conviction of Julie Amero for exposing children under the age of 16 years to images of naked and semi-naked men and women in a classroom is a striking example of a string of failures by those involved in the incident, principally the police, the prosecuting authorities and the defence. A noteworthy and disturbing feature of this case is the significant lack of understanding by most of the participants about digital data, systems and application files. For instance, the ignorance of both the prosecutor and Mr Napp (a teacher) is illustrated in the following exchange:

Q Did you ever sign into the Internet?
A I didn't sign into the Internet, I did my e-mail, which is kind of connected to the Internet.
Q I understand that. You logged onto your e-mail, you downloaded your information. When you were downloading information, your e-mails, did you ever get any pop-up ads specifically related to pornography?
A No. The e-mail program is completely separate from the Internet.[14]

The following analysis of this case aims to consider the mistakes that were made with a view to enabling the reader to understand more fully why, as a matter of professional competence, it is necessary for digital evidence specialists, lawyers and judges to recognize that it is imperative to become familiar with digital evidence, otherwise similar cases will occur in the future, to the detriment of the administration of justice. It is necessary to emphasize that data in digital format has brought about a revolution that most lawyers and judges have failed to understand. The change *has already*

[14] 35, lines 8–16.

taken place and, it seems, that a large majority of lawyers, legal academics and judges have failed to realize they are now living in a world dominated by digital evidence, *and that digital evidence is now the major form of evidence*. Although quantifiable figures are not available, it can be asserted with some confidence that the majority of lawyers, legal academics and judges do not know they do not know; a smaller number know they do not know; and an even smaller elite know about digital evidence, but they are realistic enough to know they need to know more. It is time for lawyers and judges across the globe to understand the nature of digital evidence, and lawyers in particular should look to ensuring they understand more fully the nature of digital evidence, otherwise they may find their professional indemnity insurance does not cover them.

In this case, four charges were put to Julie Amero under the General Statutes of Connecticut, Chapter 939, 53-21(a)(1) for willfully and unlawfully causing a child under the age of 16 years to be placed in such a situation that the morals of the child were likely to be impaired.[15] Whilst taking a class on 19 October 2004, certain pornographic images were displayed on the computer under the ostensible control of the teacher, some of which were seen by a number of children. In brief, the facts leading to the charges are set out below, as taken from the transcript of the trial.

1. Outline of the Facts

Mr Matthew Napp taught children in the age range 12–13 years at Kelly Middle School, Connecticut in the United States of America. On 19 October 2004, before leaving the school to attend a one-day course to learn how to score standardized testing, Mr Napp went into his classroom, he estimated at around 7.30 am, to make sure his lessons were set up for the substitute teacher. He switched the teacher's computer on and logged in under his own username and password to check the lunch menu, and to enable the substitute teacher to record the attendance of the children, because the school used such a programme to record attendance. Temporary teachers were not allocated usernames and passwords for the school's computers. Ms Amero entered the classroom at roughly the same time as children began entering the room, at between 7.45 and 8.00 am. Mr Napp and Julie Amero had a conversation when she arrived. It was Ms Amero's evidence that she asked Mr Napp to remain in the classroom to allow her to go to the ladies' cloakroom. Mr Napp did not refer to this request by Ms Amero in his evidence. He left the classroom at around 8.15 am. Ms Amero went to the ladies' cloakroom, and when she returned, her

[15] A substitute information was filed, reducing the original charges from ten to four counts, pp 3–4.

evidence was that Mr Napp was no longer in the room, and she found two children on the teacher's computer. There was a website showing hairstyles displayed on the monitor. Ms Amero told the children to leave the computer.

Ms Amero returned to the teacher's desk and the computer after giving the class their assignment. When Ms Amero returned to the teacher's desk, she found images popping up on the computer screen, which she described as images 'that were not for children to see'.[16] During the course of the day, various images in the form of pop-ups appeared on the screen of the computer, and Ms Amero gave evidence that the images did not stop: 'The pop-ups never went away. It was one after another. They were continuous. Every time I clicked the box in the corner, the red box, the red X, more were generated.'[17] Apparently, Ms Amero was in the classroom from 8.00 am to approximately 2.30 pm, when school finished, with a brief interlude when she left the classroom at around 11.30 am, and she did not leave the teacher's desk. It appears that six children[18] saw pornographic images on the teacher's screen during the course of the morning.

2. The Indictment

The charges read out to Ms Amero that she entered a plea to were written as follows:

> Connecticut General Statute Section 53-21(a) (1) and charges that on or about October 19th, 2004, in the City of Norwich, the defendant did willfully[19] and unlawfully cause a child under the age of sixteen years to be placed in such a situation that the morals of said child were likely to be impaired.

The offence as provided by the statute is as follows:

> Sec. 53-21. Injury or risk of injury to, or impairing morals of, children. (a) Any person who (1) wilfully or unlawfully causes or permits any child under the age of sixteen years to be placed in such a situation that the life or limb of such child is endangered, the health of such child is likely to be injured or the morals of such child are likely to be impaired, or does any act likely to impair the health or morals of any such child . . . shall be guilty of a class C felony for a violation of subdivision (1) or (3) of this subsection . . .

[16] 234, lines 12–13.
[17] 236, lines 13–16.
[18] The gender of the student witnesses is not apparent from the transcript of the trial, but it appears they were all male.
[19] The original spelling is used.

The use of the word 'or' between 'wilfully or unlawfully' is highly relevant, because by being charged with wilfully placing a child in a situation such that the morals of that child are likely to be impaired, the prosecution would have to prove the mental element of intent. The second part of the section does not require specific intent as an element of the crime as charged.[20] However, the wording of the charge that Ms Amero was required to plead to was written and phrased 'the defendant did willfully and unlawfully'. Arguably, if the prosecution put its case in such a way, then the prosecution held itself out to prove intent on the part of Ms Amero. If this is correct, then the learned judge ought to have adjusted her directions to the members of the jury accordingly. There is no record that the prosecution sought to amend the charges to reflect the offence as set out in the statute.

Further, it is not necessary to show that the health of the child was impaired. It is only necessary that the conduct or the acts of the defendant were such that the health of the child was likely to be impaired.[21] However, there was no evidence to indicate whether the morals of the children were likely to be impaired. In a report written by Nancy Willard,[22] it becomes apparent that the boys in the class were actively attempting to view the screen, and it is suggested that the language used by one boy clearly indicated that this was not the first time he was exposed to such images.[23] However, the discussion of this case does not extend to whether the prosecution proved its case or not.

The judge is provided with guidance when charging the members of the jury by the Criminal Jury Instructions issued by the State of Connecticut Judicial Branch Part 7.9 for § 53-21 (a) (1)–(3), revised to 31 December 2001,[24] which provides:

> To find the defendant guilty of wilfully or unlawfully causing or permitting any child under sixteen years to be placed in such a situation that the life or limb of such child is endangered, the health of such child is likely to be injured or the morals of such child are likely to be impaired, the state must prove the following elements beyond a reasonable doubt:

[20] Notes to General Statutes of Connecticut, Chapter 939, available online at <http://www.cga.ct.gov/2005/pub/Chap939.htm>.

[21] Notes to General Statutes of Connecticut, Chapter 939, available online at <http://www.cga.ct.gov/2005/pub/Chap939.htm>.

[22] Nancy Willard, MS, JD, *The Julie Amero Tragedy* (Center for Safe and Responsible Use of the Internet, February 2007), available online at <cyberbully.org/onlinedocs/AmeroTragedy.pdf>.

[23] For further information about this topic, see J Wolak, K Mitchell and D Finkelhor, *Online victimization of youth: Five years later* (National Center for Missing & Exploited Children, 2006), available online at <http://www.unh.edu/ccrc/second_youth_internet_safety-publications.html>.

[24] Available online at <http://www.jud.state.ct.us/CriminalJury/7-9.html>.

(1) that at the time of the incident, the alleged victim was under the age of sixteen years; and (2) that the defendant wilfully or unlawfully caused or permitted the victim to be placed in a situation that endangered the child's life or limb, or was likely to injure his health or impair his morals.

The conduct to be punished must involve a child under the age of sixteen years. The statute also requires wilfulness or unlawfulness in causing or permitting the child to be placed in a situation that his life or limb is endangered, or his health is likely to be injured, or his morals are likely to be impaired. This is the conduct of a person that is deliberately indifferent to, acquiesces in, or creates a situation inimical to the child's moral or physical welfare.

'Wilfully' means intentionally or deliberately. 'Unlawfully' means without legal right or justification. Causing or permitting a situation to arise within the meaning of this statute requires conduct on the part of the defendant that brings about or permits that situation to arise when the defendant had such control or right of control over the child that the defendant might have reasonably prevented it. Under this provision, the state must prove that the child's life or limb was endangered or the child's health was likely to be injured or the child's morals were likely to be impaired. 'Likely' means in all probability or probably. As used here, 'morals' means good morals, living, acting and thinking in accordance with those principles and precepts that are commonly accepted among us as right and decent.

The learned judge directed the members of the jury as follows:[25]

'Now, the defendant, Ms. Amero, was charged with four counts of Risk of Injury to a Minor, in violation of Connecticut General Statute 53-21(a)(1), which insofar as it applies in this case provides as follows: Any person who willfully or unlawfully causes or permits any child under the age of sixteen to be placed in such a situation that the morals of that child are likely to be impaired shall be punished. The intent of this statute is to protect the health, morals and well-being of children.

To find the defendant guilty of willfully or unlawfully causing or permitting any child under sixteen to be placed in a situation in which their morals are likely to be impaired, the State must have proven the following elements beyond a reasonable doubt: One, that at the time of the incident the children in question were under sixteen years old. Two, Ms. Amero willfully or unlawfully caused or permitted the victims to be placed in a situation that was likely to impair their morals. So the conduct to be punished must involve victims under sixteen years old, and

[25] 330–33.

the conduct must have placed the children in a situation in which their morals were likely to be impaired. This is the conduct that is deliberately indifferent to, acquiesces in, or creates a situation that is basically opposite to the child's moral welfare, inimical, or basically opposite to the children's moral welfare. Willful means deliberately or intentionally. Unlawfully means without legal right or justification; causing or permitting a situation to arise when the defendant, Ms. Amero, had such control or right of control over the children that the defendant could have prevented from happening.

The state must have proven that the children's morals were likely to be impaired, and likely means probable or in all probability as used here. Morals means good morals; living, acting and thinking in accordance with those principles or precepts that are commonly accepted amongst us as right and decent. As for intent, the state must have proven the defendant had the general intent to perform these acts, in other words, her behavior, if you find that she did, in fact, access these websites commonly referred to as pornographic, or that the pornographic websites were being accessed and the defendant was indifferent to, acquiesced in or created a situation that would be indifferent to or opposite to the children's moral welfare, and that the children were under sixteen years old were exposed to these websites, that would be general intent.

The state does not have to have proven that she intended the precise harm or result which may have happened. In other words, I know this is a difficult concept here. General intent is at least an intention to make a bodily movement which constitutes an act which the crime requires. The behavior had to be voluntary. Was this behavior which would be accessing websites in question in a seventh grade classroom where there was pornography present likely to impair the morals of these children.

To summarize, for the defendant to be guilty of Risk of Injury to a Minor, the state must have proven beyond a reasonable doubt, once again, that at the time of the incident the victims were under sixteen years old; that the defendant did act in a way likely to impair the morals of these children; the defendant had an intent to perform those acts.

If you find that the state has proven beyond a reasonable doubt those elements that I have described to you of Risk of Injury to a Minor, then you will find the defendant guilty. If on the other hand, you find that the state has not proven the charges beyond a reasonable doubt, then you will find the defendant Not guilty.

What a person's intention or knowledge has been is usually a matter to be determined by inference. No one is able to testify that they looked in to another's mind and saw there in a certain purpose or intention or a certain knowledge to do harm to another. The only way a jury can ordinarily determine what a person's purpose, intention or knowledge was at

> any given time, is by determining what that person's conduct was and what the circumstances were surrounding that conduct and from that infer what that intention or purpose was.'

Julie Amero was found guilty of all four counts by the jury of six on 5 January 2007. The date for sentencing was fixed at 2 March 2007,[26] although sentencing was put back on several occasions, until the new attorneys for the defendant, William F Dow III, Richard Emanuel, Timothy H Everett and Todd D Fernow, submitted a motion for a new trial on 4 June 2007, which was granted.

3. Analysis of the Investigation

(a) The physical evidence

The way in which the computer was dealt with exemplifies the dilemma an organization faces when confronted with a situation that might or might not be the subject of criminal charges in the future. Where it is obvious from the facts of the incident that criminal proceedings will be initiated, those responsible for the computer or system should ensure the physical evidence is not compromised, which means the organization ought to have a plan in place that provides a guide as to what actions should be taken in such circumstances. Where it is not obvious that the facts of the incident will lead to the opening of a criminal investigation, consideration should, nevertheless, be given to the possibility that an investigation might be instigated, which means the evidence should be treated in the same way as if it was certain that such proceedings will take place. It is in the interests of both the person that has been accused and the organization to ensure the evidence is treated properly. It is crucial to be able to demonstrate that the evidence is not tainted, because any failure to deal with the evidence correctly during the investigation may lead to the integrity of the evidence being successfully challenged by the defence. In the Julie Amero case, the sequence of events is a classic example of what not to do in such circumstances.

Mr Napp was made aware of the events that occurred in the classroom when he received an instant message at 6.00 or 7.00 pm on 19 October 2004 from one of his pupils,[27] as a result of which he went into his classroom the following day at between 7.20 am and 7.30 am to check the history on his computer.[28] In checking the history[29] (probably the temporary cache file, although this was not stated), he 'saw a bunch of different

[26] 343.
[27] 39, lines 6–10.
[28] 40, lines 2–11.
[29] 40, lines 16–23.

sites of some pictures that had questionable names'.[30] He clicked on one file to reveal it was a discussion board about lesbians, and gave evidence that the names of some of the files suggested, in his view, that they contained images of a sexual nature.[31] Mr Napp was scheduled to be out of his class on 20 October, so he sent an email to the principal, setting out what he had been told in the instant message and describing what he found on the computer. He asked the principal how he should proceed.[32] During the afternoon of 20 October, the principal visited the classroom, and Mr Napp showed him the 'log' (probably the temporary cache file).[33] The ignorance of both the prosecuting lawyer and the defence lawyer is illustrated in a question asked by the prosecution lawyer, which the defence lawyer failed to object to: 'And the log basically says what has been accessed from the Internet'[34]—the point being, the temporary cache file lists files and Internet sites, but it does not prove that the websites were actually visited. Mr Napp subsequently indicated that an IT professional (not named, but probably Mr Robert Hartz) for the district visited the school, and 'went through more extensive search of the hard drive, and we actually printed out some of the log from the screen'.[35] There was no indication of the date and time this occurred or what was printed, although Mr Hartz produced some documents that were subsequently entered as an exhibit. Mr Napp gave further evidence to the effect that on a day that was 'probably a couple of weeks afterwards' the hard drive was missing.[36] It is not clear whether it was only the hard drive that was missing, or the entire computer.

Mr Robert Hartz, the information services manager for the Norwich Public Schools System, was invited to attend the school either by the superintendent or the principal. Mr Hartz believed he attended on 20 October.[37] He took the following action:

> 'The first thing I did is I went in to the room and it was during that free period, and I talked to the teacher, Mr. Napp, a little bit, and he basically confirmed what Scott Fain and Dr. Frechette had said. There was concern that some inappropriate sites were accessed. I then went to the teacher's computer in that room, his computer, and the first thing I did was I took the IP address, because I was going to need that later, so I recorded the IP address. And then I went into the cookies file. The cookies didn't show me a whole lot. But then I went into the temporary Internet files, and that is a number of files that were dated the previous day, October 19th, with time stamps starting I believe around 8:30, 8:35,

[30] 41, lines 6–7.
[31] 41, lines 6–23.
[32] 41, lines 4–7.
[33] 42, lines 12–23.
[34] 42, lines 25–26.
[35] 43, lines 5–8.
[36] 43, lines 16–19.
[37] 64, lines 10–11.

and going through the end of the day. And so I looked at these and I saw certain sites that were accessed from this PC. As I recall, it started out with access to AOL.'[38]

Mr Hartz gave vague evidence regarding the date the computer was moved:[39]

Q Any reason the computer wasn't removed?
A To the best of my recollection, it was removed from the classroom I believe on the 20th, maybe not until the 21st and brought down to Mr. Fain's office for subsequent pickup by the police.

It appears that the computer was taken into custody by Michael Belair, a sergeant with the Norwich Police Department on or about 27 October 2004. He logged the computer as evidence and placed it in the evidence room.[40] Mark Loundsbury, a crime prevention officer and the computer crimes officer in the Norwich Police Department, retrieved the computer from the evidence officer on an unknown date some two years later.[41] He gave evidence in response to a re-cross-examination by the defence attorney that the computer was last used on 26 October 2004.[42] One report suggests it was a Gateway computer running Windows 98 that was seized,[43] although it transpired that the computer was manufactured by Dell, and the system was running an original version of Windows 98 (4 October 1998), which was an upgrade from Windows 95, together with Internet Explorer 6.0.2800.1106IC.[44]

(b) Elements of failure

The police officer was neither invited by the prosecuting attorney to provide an accurate indication of precisely what was seized, nor did he offer the information: it is not clear whether it was the computer including the monitor and the keyboard, whether it was just the computer, or whether it was

[38] 64, lines 20–27; 65, lines 1–4.
[39] 92, lines 15–19.
[40] 96, lines 14–20.
[41] 118, lines 4–6.
[42] 135, lines 3–8.
[43] A Patrizio, 'Computer-Clueless In Connecticut' *Internetnews.com* (28 March 2007), <http://www.internetnews.com/reporters_notebook/article.php/3668451>.
[44] AA Eckelberry, G Dardick, PhD, JA Folkerts, A Shipp, E Sites, J Stewart and R Stuart, 'Technical Review of the Trial Testimony State of Connecticut vs Julie Amero' (21 March 2007) 3 and 15; this document is a working draft and was drafted as an attorney work product and marked 'Confidential, not for distribution'. A copy of this document was passed to the author with permission for the author to use the findings of the analysis for the purpose of illustrating the issues concerning the hard drive in this case. It is anticipated that a final-version report will be made available generally, once the lawyers for Ms Amero are satisfied that the document can be put into the public domain.

just the hard drive. However, considering the evidence given by Mark Loundsbury, it is probable that only the computer was seized, because he had to replace the floppy drive. There was no evidence to indicate whether the computer was placed in an evidence bag, and there was no evidence to indicate the serial number of the computer or the relevant component parts of the computer, or the manufacturer of the computer. There does not appear to have been any evidence to demonstrate the police, when investigating the case, followed the guidelines set out in Chapter 2, 'Evidence Assessment', in *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* issued by the US Department of Justice.[45]

The prosecution failed to establish the chain of evidence or make it clear precisely what the police seized. The defence failed to challenge the chain of evidence, which ought to have been considered, because of the volatility of the digital data and the possibility that the data on the hard drive might have been corrupted.[46] The defence also failed to alert the members of the jury to the inconsistency in the date that Mr Napp and Mr Hartz claimed the computer was moved, and also failed to follow up the admission by the police officer that the last date the computer was used was 26 October 2004.[47] This was a very important point, because this meant that because the computer was used after 19 October, relevant data in the browser cache and history files may have been overwritten. This aspect of the evidence was not followed up by the defence or not followed up sufficiently when cross-examining the prosecution witnesses.

(c) The hard drive

(i) Copying the hard drive

When beginning the investigation of a computer or computer-like device, the first action should be to take a sector-by-sector or bit-stream duplicate copy of the original storage medium, in this instance the hard drive of the computer. The importance of this act cannot be overestimated:

> There are two fundamental principles in relation to copying digital evidence that a digital evidence specialist should be aware of:
> a. The process of making the image should not alter the original evidence. This means the appropriate steps should be taken to ensure that the process used to take the image should not write any data to the original medium.

[45] J Ashcroft (Attorney General), DJ Daniels (Assistant Attorney General) and SV Hart (Director, National Institute of Justice), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, US Department of Justice, Office of Justice Programs, National Institute of Justice, Special (APR. 04 NCJ 199408),

[46] Mason (n 9) Chapter 2 and 8.122 footnote 2.

[47] 135, lines 3–8.

b. The process of copying data should produce an exact copy of the original. Such a reproduction should allow the specialist to investigate the files in the way they that existed on the original medium.[48]

The tool used for this purpose by the digital evidence specialist should be appropriate for the task. In particular, for the evidence to have any probative value, it is necessary to ensure the tool protects the data by the use of a checksum operation called a hash function, which should be applied to each file or disk that is copied. Neither Mark Lounsbury nor Mr Horner were asked by either lawyer during the trial for details of the tool used to copy the contents of the hard disk.

In fact, a disk replication product by the name of Ghost by Symantec was used to take an image of the disk.[49] Although it might be possible to use this product, as indicated in the lecture notes by Thomas R O'Connor,[50] nevertheless the publication *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, issued by the US Department of Justice, makes it clear that digital evidence must be acquired very carefully, which means the tool used to obtain a copy of the content of a hard disk must be appropriate for the purpose:

> **How is digital evidence processed?**
> **Acquisition.** Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a ***copy*** of the ***original evidence***. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence.[51] (Emphasis in the original)

This is discussed in detail by Eoghan Casey, and the particular product used in this instance is not included in the list of tools provided in his text;[52] furthermore, it does not appear to have been tested by the National

[48] Mason (n 9) 3.13.

[49] Eckelberry (n 44) 2–3.

[50] TR O'Connor, Criminal Justice and Homeland Security Program Manager, Austin Peay State University Center at Ft Campbell, 'Digital Evidence Collection & Handling (A three-part lecture including Privacy & Cyberlaw and Investigation of Cybercrime)': '4. Make sure your copy of the hard drive is a bit stream backup, using programs such as Encase, SafeBack, or Code Blue (for remote diagnostics). Norton Ghost also has some switches and options that can be used for this purpose, and the UNIX dd (data dumper) utility is sometimes used.' Updated as at 26 February 2006, available online at <http://faculty.ncwc.edu/toconnor/426/426lect06.htm>.

[51] US Department of Justice, Office of Justice Programs, National Institute of Justice, Special (APR. 04 NCJ 199408) 1; such practices are also reflected in the 'Good Practice Guide for Computer-Based Electronic Evidence' (ACPO, 2007).

[52] E Casey, *Digital Evidence and Computer Crime* (2nd edn, Elsevier Academic Press, London, 2004) generally Chapter 10.

Institute of Standards and Technology.[53] It is essential that the product that is used is capable of making a sector-by-sector or bit-stream duplicate copy of the hard drive in a way that preserves its integrity. It is also recommended that the hard disk is copied using more than one tool.[54] Such tools can be the subject of cross-examination as to the underlying scientific methodology used by the tool, and consideration ought to be given by lawyers to this aspect of the evidence-gathering process, especially as there is some discussion in the digital forensic community as to whether or not some of the tools take an exact copy of the disk.[55]

Not only is the actual tool used to obtain a copy of the hard disk an important factor for a digital evidence specialist to consider, but it might also be necessary, before taking a sector-by-sector or bit-stream duplicate image of the hard disk, to retrieve information about the configuration of the computer through a controlled boot of the system, as outlined in Chapter 3 of *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* issued by the US Department of Justice. No evidence was offered as to whether the investigating police officer undertook the actions as recommended in this chapter, and the defence failed to cross-examine the police officer in relation to any aspect of this part of the investigation.

(ii) Examination of the hard drive

It is a tenant of any investigation of digital evidence that the investigator does not examine the original hard drive unless it is absolutely necessary. It is normal and recommended to examine a copy of the hard drive, not the original, as provided by the first principle to Chapter 4 of *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* issued by the US Department of Justice: '**Procedure:** Conduct the examination on data that have been acquired using accepted forensic procedures. Whenever possible, the examination should not be conducted on original evidence' (Emphasis in the original).

It should be possible for the findings of the investigator to be replicated by a third party, whether it is another police specialist or an independent examiner. It is for this reason that the original investigator should provide a full report of the actions they took, and only work on a copy of the original hard drive. It appears from the transcript that Mr Lounsbury created a

[53] National Institute of Standards and Technology, Information Technology Laboratory, Computer Forensics Tool Testing Program, available online at <http://www.cftt.nist.gov/disk_imaging.htm>; see also *Disk Imaging Tool Specification*, Version 3.1.6 (12 October 2001) and *Digital Data Acquisition Tool Specification* , Draft 1 for Public Review of Version 4.0 (4 October 2004).

[54] Casey (n 52) paragraph 10.3.

[55] *Digital Data Acquisition Tool Test Assertions and Test Plan*, Draft 1 for public comment of Version 1.0 (10 November 2005) (National Institute of Standards and Technology); Mason (n 9) 3.28–3.32.

copy of the hard drive for the defence, and then proceeded to examine the original hard drive, rather than a sector-by-sector or bit-stream duplicate copy, as is normal with digital evidence specialists:

Q Okay. And prior to this last examination you did, what access did you have with this computer?
A I had to provide the defense with originally the—the order was to provide them with the evidence which would have been the computer or hard drive itself. And in order to do that, I had to create a copy of the hard drive, which has all the information which is located inside the original computer. So the hard drive was removed from the computer. It was placed in a sterile environment, which is another computer with its own operating system, no other software installed. I obtained a new hard drive from the defense representative and made a copy of that drive so that they could have the evidence in that fashion.
Q Other than that access, to your knowledge has that hard drive on the computer in question been accessed?
A No, sir.
Q Prior to you accessing it to gather information for this case?
A No, sir.
Q At some point, you had this computer powered up, correct?
A Yes.
Q And you were in the process of conducting a forensic examination of the hard drive, is that correct?
A Yes, sir.[56]

It is most unusual to examine a live hard drive, because once the hard drive has been examined, the tool itself will alter the data on the hard drive, thus compromising the data permanently. There seems to be no reason why the police officer neglected to make a copy of the hard drive for his own examination, although a later comment by the officer in examination-in-chief may indicate he might have worked from a copy, given that an MD5 signature is referred to, although it is not certain that he used a copy:

A There is an MD5 signature.
Q What's that?
A That tells you that the image has not been tampered with. It's a unique hexadecimal number which identifies the picture has not been changed in any way.

[56] 118, lines 14–27; 119, lines 1–14.

Q And that is information provided on all of the images that were downloaded directly from this computer in question?
A Yes.[57]

(iii) Malicious software

Mr Hartz gave evidence that there was anti-virus software on the computer called InoculateIT by Computer Associates.[58] In a somewhat clumsy question, he was asked in cross-examination whether the anti-virus software was up to date, and in reply he offered a somewhat incomplete and confusing answer that merited further examination:

A Anti-virus updates, Inoculate IT was updated I want to say weekly. It would have been updated no later than October 12th, the week before that and probably sometimes towards the middle of the week. Trend Microscan Mail, that was updated nightly.

In fact, Computer Associates ceased to provide support for this product from 17 March 2004: 'CA has dropped support for InoculateIT/Inoculan v 4.x for Windows (including signature updates and localized versions) effective March 17, 2004'.[59] The report by Alex A Eckelberry and others indicated that the update log on the computer registered that the anti-virus signatures were last updated on 31 August 2004 at 11:46:57, and the actual signatures dated from 30 June 2004.[60] Thus it can only be concluded that there was no up-to-date anti-virus software in operation on this computer at the material date, and the statement by Mr Hertz was not correct.

He was also asked whether Mr Napp's computer was infected by viruses:

Q To your knowledge, was the PC in question, Mr. Napp's PC, to your knowledge at the time infected with any viruses?
A Not to my knowledge.[61]

He confirmed this when cross-examined:

Q Was there any adware, spyware or virus found on the computer?
A I did not find any of that, although I did not look for adware or spyware.[62]

[57] 131, lines 4–12.
[58] 81, lines 7–22.
[59] <http://www.ca.com/us/securityadvisor/newsinfo/collateral.aspx?cid=52311>.
[60] Eckelberry et al (n 44) 5–6.
[61] 81, lines 26–27; 82, lines 1–2; see also 86, lines 13–16.
[62] 86, lines 25–27; 87, line 1. Adware (also known as advertising-supported software) is a software package that, once it is installed on a computer, will automatically play, display, or download advertising material to a computer.

Mr Hertz was also asked in cross-examination:

> Q Does spyware and adware generate pornography?
> A Not to the best of my knowledge.[63]

Although the question was not well constructed, nevertheless the defence lawyer was asking whether spyware or adware programmes were capable of generating pop-ups that contained pornographic material. The fact is, they are capable of placing pornographic images on a computer without the permission of the owner or user.[64]

One of the considerations that ought to have been foremost in the mind of the investigating officer when examining the content of the hard disk included checking for the existence of malicious software, as indicated on page 1 to the Introduction to *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* issued by the US Department of Justice:

> **How is digital evidence processed?**
> **Assessment.** Computer forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take. (Emphasis in the original)

Mark Lounsbury was explicitly asked if he had tested the hard drive for viruses and spyware in cross-examination:

> Q Did you examine the hard drive for spyware, adware, viruses or parasites?
> A No, I didn't.[65]

That the police officer conducting the investigation failed to examine the hard drive for malicious software is an astounding admission that is tantamount to a degree of carelessness that appears to be the hallmark of this particular case. The fact is, it is very well known that malicious software can cause files to be downloaded to a computer without the authority or the consent of the owner or user of the computer.[66] It is for this reason that those conducting the investigation have a duty to the accused to determine,

[63] 86, lines 17–18.

[64] D McCullagh, 'Spying on the spyware makers' *CNET News.com* (4 May 2005), <http://www.news.com/Spying-on-the-spyware-makers/2008-1012_3-5694455.html>; B Edelman, 'Spyware Showing Unrequested Sexually-Explicit Images' (22 June 2006), <http://www.benedelman.org/news/062206-1.html>.

[65] 133, lines 13–15.

[66] M Carney and M Rogers, 'The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction' (Spring 2004) 2 International Journal of Digital Evidence, available online at <http://www.ijde.org>.

in the first instance, whether there is malicious software on the computer that could be responsible for the behaviour complained of. This ought to be considered in particular where an explanation is offered to the effect that the user or owner was not aware of the offending materials or lost control of the websites appearing on the screen, as in this case.

When conducting the examination of the copy of the hard drive supplied to him, Mr Horner reported discovering an alarming state of affairs, although no detailed information about the nature of the spyware or adware is available in the public domain as the result of Mr Horner's report for the defence:

> During the copy process we received several 'Security Alerts!' from our antivirus program. We analyzed the activity log and noted that there were spyware/adware programs installed on the hard drive. We ran two other adware/spyware detection programs and more spyware/adware tracking cookie/programs were discovered. Out of the 42, 27 were accessed or modified days if not a month before October 19, 2004. We also noted that there was no firewall and there was an outdated antivirus program on the PC. The PC was being tracked before October 19, 2004 by adware and spyware.[67]

In addition, he mentioned spyware and adware during cross-examination:

> A In this case, because of the spyware and the adware that was being uploaded because of the interest of the user, there was an opportunity to go to many different sites being presented in the background in the Internet cache files. And by the way, there are many different files to look at. You can't just look at one set of files, you have got to look at the whole picture.[68]

He was later asked for his conclusions by the prosecutor in respect to his analysis of the hard drive:

> Q What is your conclusion? You didn't ever state it, I don't think. What is your conclusion?

[67] 'The Strange Case of Ms Julie Amero: Commentary by Mr. Herb Horner', online at <http://www.networkperformancedaily.com/2007/01/th e_strange_case_of_ms_julie_a_1.html >.

[68] 210, lines 8–14. It should be noted that during an exchange in the absence of the members of the jury, Mr Horner mentioned that he found spyware on the computer (195, line 26) and evidence given by Mr Horner 'This site did not directly connect to pornography, however, this site enacted spyware and adware programs to be uploaded in to the computer. Then after this site was looked at by the children, you will notice the small icons' was removed from the record at the direction of the learned judge (202, line 12).

A The conclusion is because of the lack of an updated firewall, because of the lack of anti-spyware, because of the lack of anti-adware programs, this computer was subject to advanced—to the opportunity for that person to go to pornographic sites totally out of control because there was no protection. And if I were allowed to show my findings, there were forty adware spyware programs tracking the person's interests.[69]

Alex A Eckelberry and his team found that an adware programme 'newdotnet' was installed on the computer on 12 October 2004, after a screen saver was downloaded, called 'Haunted House screensaver'.[70]

(iv) Content filtering

Mr Hartz gave evidence that the Norwich school system used a content filtering firewall on a server, which meant that when a person directed a computer to visit the Internet, the request and connection went through the server. The firewall was a combination of hardware and software, and the software was called Raptor.[71] However, he admitted it was not up to date.[72]

(d) Elements of failure

The prosecution failed to establish the name of the tool that was used to take an image of the hard drive, which in turn undermined the authenticity and integrity of the evidence. The prosecution were not even challenged or required to lay the foundations for the authenticity or integrity of the evidence, which was a serious procedural flaw in these proceedings. The defence failed to understand the importance of establishing which tool was used for taking the image of the hard drive, and ought to have required the prosecution to lay the correct foundations for the authenticity of the evidence before the police office was permitted to relate his findings.

The prosecutor was completely taken aback when the defence expert witness began his evidence, because he sought to introduce the report he had prepared. Apparently, Mr Cocheo, the defence lawyer, had failed to provide a copy of the report to the prosecution in advance. As a result, Mr Smith for the prosecution objected to hearing the details contained in the report. Apparently, Mr Cocheo did not himself have advanced sight of the report prepared by Mr Horner, and the learned judge determined that the report would not be admitted into evidence. Mr Horner was not permitted

[69] 228, lines 25–27; 229, lines 1–5.
[70] Eckelberry et al (n 44) 4, 15 and 17.
[71] 61, line 27; 62, lines 1–2.
[72] 79, lines 8–25; 83, lines 3–17; 90, lines 18–27; 91, lines 1–5.

to refer to the findings contained in the report.[73] The failure to provide the report to the prosecutor in advance might be considered somewhat remiss, although the response of the prosecuting attorney to the claim that the computer contained malicious software was astounding, given that a one of the first things a digital evidence specialist will normally do when examining a computer is to establish whether there was any malicious software on the hard drive:

> MR. SMITH: That should have been turned over to the state. I don't think he should be able to reference the information on this sheet.
> THE COURT: I am not sure I am clear what you mean.
> MR. SMITH: Specifically, he brings out spyware, all the information, all the spyware should have been turned over to the state and it wasn't, so we could have done an investigation to either prove or disprove the information he is talking about. That is what this discovery process is about.
> THE COURT: Right.
> MR. SMITH: I am clearly at a disadvantage now. I don't see how I can, unless obviously there is time provided, go back to look at the various sites, to examine the documents that he is putting in evidence or that he is using to base his opinion on. My assumption was he was going to base it on the information he had in the past, and this was discussed in chambers, if I am right, with Mr. Cocheo.
> THE COURT: Right.[74]

The claim by the defence that there was malicious software on the computer ought to have been anticipated by the prosecution, and the police officer conducting the investigation ought to have established whether there was any malicious software on the hard disk as a matter of course. In addition, the prosecuting attorney ought, also as a matter of course, to have canvassed this possibility with the police expert. It should not have been a surprise that there was a probability that there was malicious software on the hard drive, yet the prosecuting attorney was clearly badly prepared for such an eventuality, which is a startling state of affairs given the extent of the global publicity that attaches to attacks caused by malicious software and the resources made available to the state prosecutor's office.

4. Qualifications of the Experts

To establish the qualifications of Mark Lounsbury, the prosecution lawyer asked the following questions of the police officer:

[73] 193, lines 19–27.

[74] 197, lines 5–26.

Q It kind of leads to the question, you are engaged in investigating computer crimes specifically?
A Yes, sir.
Q And part of your job duties, does it entail investigating computer crimes of a pornographic nature?
A I investigate crimes of a pornographic nature, yes, sir.
Q Computer crimes specifically of a pornographic nature?
A Yes.
Q How long have you been a police officer?
A Almost eighteen years now.
Q How long have you been involved in the investigation of computer crimes?
A Approximately seven years.
Q And do you have any training and experience specifically in investigating computer crimes?
A Yes, I do.[75]

The defence lawyer did not seek to challenge the foundation for the police officer's qualifications, although one report has suggested the he 'completed two two-week FBI training seminars on computer security and other continuing education programs. He is also a certified user of the computer monitoring software ComputerCOP Pro'.[76] If the media report about the qualifications of the police officer is correct, this is of great concern, especially when an investigator is examining a hard drive in circumstances where a person may be accused of criminal activity that can lead to a substantial term of imprisonment.

Mr Wilson H Horner's employment history is set out on pages 187–89 of the transcript, and he later set out the actions he took after being approached by the defence:

Q Mr. Horner, can you tell us what actions you took concerning this case.
A Basically I—what I had to do is determine as much as I can about this forensic analysis of this particular computer. The first thing we did, my group and my company, we went out and found as much information as we possibly could, either through seminars or through the Internet and libraries on how to conduct this examination. And the reason I did that, even though I had a lot of experience doing that type of thing, I just wanted to make sure that I did not leave anything out.

[75] 116, lines 15–27; 117, lines 1–5.
[76] L Beyerstein, 'Questionable conviction of Connecticut teacher in pop-up porn case' AlterNet (19 January 2007), <http://www.alternet.org/story/46925/>.

> And I wanted to make it as thorough as I possibly could. So what I am showing here are all the references that I used to assist us with this investigation. And I don't know if it is necessary to read them all, but I can. And I also listed up there the authors and either the websites or where they were located.

It is for the reader to determine, based on the evidence given to the court in this case in relation to their qualifications, whether either expert witness would have been considered sufficiently qualified in any other jurisdiction.

5. Analysis of the Presentation of the Evidence in Court

(a) Forensic analysis by the police

The police digital evidence specialist, Mark Lounsbury, used a programme called ComputerCop Professional[77] to conduct his analysis of the content of the hard disk. It is not certain whether this particular tool is widely used by digital evidence specialists, and it is highly debatable whether the investigating officer should only use a single tool to examine a hard drive, given that each digital evidence processing tool has its weaknesses and limitations.[78] Bearing in mind the prosecution sought to prove that Ms Amero deliberately obtained access to the various pornographic websites listed in the Temporary Internet Files, it was important to establish proof that this was the case. It should be stressed that the company responsible for this programme admitted that the tool was not capable of determining why files are on the computer, or whether it was caused by malicious software, or by direct and wilful use.[79]

In striking contrast to the analysis offered by the police officer in evidence, Mr Horner offered a more detailed outline of the use of the computer, although this information was not brought before the members of the jury because the defence failed to provide the prosecution with the expert report in advance:

> On October 19, 2004, around 8:00 A.M., Mr. Napp, the class'[s] regular teacher logged on to the PC because Julie Amero being a substitute teacher did not have her own id and password. It makes sense that Mr. Napp told Julie not to logoff or shut the computer off, for if she did she

[77] It was version v.3.16.3: The Strange Case of Ms Julie Amero: Commentary by Detective Mark Lounsbury, online at <http://www.networkperformancedaily.com/2007/01/the_strange_ case_of_ms_julie_a_3.html>.

[78] Casey (n 52) para 10.3

[79] B Boyko, 'The Strange Case of Ms. Julie Amero: More Information in the interlude' (Tuesday 23 January 2007), <http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_2.html>.

> and the students would not have access to the computer. The initial user continued use of the PC and accessed Tickle.com, cookie.monster.com, addynamics.com, and adrevolver.com all between 8:06:14 - 8:08:03 AM. During the next few moments Julie retrieved her email through AOL.
>
> http://www.hair-styles.org was accessed at 8:14:24 A.M., based upon the hair style images uploaded to the PC we were led to believe that there were students using the computer to search out hair styles. The user went to http://www.crayola.com at 8:35:27 A.M. The user continued accessing the original hair site and was directed to http://new-hair-styles.com. This site had pornographic links, pop-ups were then initiated by http://pagead2.googlesyndication.com. There were additional pop-ups by realmedia.com, cnentrport.net, and by 9:20:00 A.M., several java, aspx's and html scripts were uploaded. A click on the curlyhairstyles.htm icon on the http://www.new-hair-styles.com site led to the execution of the curlyhairstyle script along with others that contained pornographic links and pop-ups. Once the aforementioned started, it would be very difficult even for an experienced user to extricate themselves from this situation of porn pop-ups and loops.[80]

Although the clock on the computer was inaccurate by approximately 10 or 12 minutes according to Mr Hartz, the timing might be crucial to the evidence in the case.[81] Mr Hertz indicated that somebody viewed a website with links to a pornography site after 8.35 am, which tends to corroborate the comments made by Mr Horner. Mark Lounsbury did not give any evidence as to when the images began or when they ended, but it is reasonably certain that they appeared around 8.35 am and continued until 11.13 am.[82] It seems to be inconceivable that the police expert was not aware of this information, and either the prosecutor was not aware of this information, or if he was, he failed to ask the police officer to confirm the time scale during which the images appeared. This is particularly important, given the comments made by Mr Lounsbury after the trial:

> The police take into account all the available facts and circumstances, for example: who was the individual, what was the individual doing, when were they doing it, where were they doing it, and how long was the individual engaged in the observed activity? (A minute, twenty minutes, two hours?)[83]

[80] 'The Strange Case of Ms Julie Amero: Commentary by Mr. Herb Horner', online at <http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_1.html>.

[81] 67, lines 6–7: Mr Hartz could not recall whether it was fast or slow.

[82] Eckelberry et al (n 44) 16.

[83] The Strange Case of Ms Julie Amero: Commentary by Detective Mark Lounsbury, online at <http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_3. html>.

If the clock on the computer was fast by 12 minutes, 8.35 am would actually have been 8.23 am. If it was slow by 12 minutes, 8.35 am would have actually been 8.47 am. If the latter time was correct, it might constitute conclusive proof that Ms Amero viewed a website that had a link to the pornographic website. If the former time was correct, it is possible that the two school children were responsible for viewing the websites whilst Ms Amero was out of the classroom. This point is so significant, that it appears to be almost unbelievable that the defence attorney failed to take particular care to cross-examine Mr Hartz and Mr Lounsbury on this matter.

(b) Temporary Internet Files

Mr Hartz referred to the Temporary Internet Files and the firewall log without qualification, in that he gave evidence to the effect that because websites were listed in the files or log, the computer was therefore directed to visit such sites. Although he indicated that he took action to corroborate the files discovered in the Temporary Internet Files by comparing the files listed in the log of the firewall server, nevertheless the most important point was that the logs that Mr Hartz viewed contained a list of those sites that placed information on the computer, whether the user actually visited the website in question or not.[84] The inference was that where the Temporary Internet Files listed a website, it meant that Julie Amero intentionally clicked on the website to visit it. The evidence given by Mr Hartz did not prove that Ms Amero visited pornographic websites deliberately, but this might have been a point that the members of the jury failed to grasp, because of its subtlety—it was certainly a point that was not referred to by her defence lawyer. To illustrate the point, consider the following evidence from the transcript:

Q The hairstyle site is approximately 9:00 a.m., correct, if you can see it?
A Yes. That column on the right is the date and time stamp that that file was modified.
Q Various hairstyle sites, and I believe you also say that this computer accessed hairstyling and Orbitz site, that is the site of the travel you stated?
A Yes. There is an entry for Orbitz.
Q Around 9:15 or so, correct?
A That is what it appears to be, yes.
Q And then at some point you indicated, and I will show this, more Orbitz sites, correct?

[84] 68–79.

A Correct.
Q At some point, you indicated that it changed over to some sites that were questionable in nature to you, correct?
A And I think on this page is where you see some of that.
Q Approximately 9:24 I see here there is an access to www.FemaleSexual.com. Again, this comes from this computer, correct?
A Yes.
Q From Mr. Napp's computer?
A Correct.
Q These are various pages listed on the web pages.
A It's an indication that that site has been hit and actually when a picture is pulled down, you get another entry in here. But at 9:24, that site was accessed.[85]

Sole reliance on these particular files is very dangerous, and there should have been a greater analysis of other files, including the index.dat file. The index.dat file is a file used by the Internet Explorer web browser. It comprises a number of files including a Temporary Internet index file, cookies file and history file. The reason for retaining such databases is to enable the easy retrieval of the information and enables a faster response to queries.[86] This is a point that Mr Horner tried to make to the prosecutor during his cross-examination:

A In this case, because of the spyware and the adware that was being uploaded because of the interest of the user, there was an opportunity to go to many different sites being presented in the background in the Internet cache files. And by the way, there are many different files to look at. You can't just look at one set of files, you have got to look at the whole picture.[87]

Mr Horner was cross-examined for some time by the prosecutor about how a file would appear in the Temporary Internet Files (also referred to as the temporary cache file). Mr Horner mentioned the index.dat file several times to explain that where a website appeared in the temporary cache file as the result of being redirected from another website, the relevant details would be found in the index.dat file. However, the prosecutor completely failed to grasp what Mr Horner was saying in reference to the index.dat file or the additional files that ought to be considered when investigating the computer.[88] It appeared as if the prosecutor ignored the comments made by

[85] 71, lines 14–27; 72, lines 1–14.
[86] Casey (n 52) para 10.8.1.
[87] 210, lines 8–14.
[88] 219, lines 4–24; 220, lines 16–25; 221, lines 23–26; 222, lines 3–25; 223, lines 3–12.

Mr Horner as he tried to explain that there were far more files to consider on the computer than just the Temporary Internet Files. Consider the tenor of the exchanges during cross-examination:

Q When a pop-up ad appears, is that information saved in the temporary Internet logs like you have right there?
A Pop-ups, yes, but not a redirect.
Q Okay. Redirects would not be?
A No. That is why they are so elusive.
Q I understand that. So whenever a pop-up would come through, it would show up here, correct, on the login? I am showing you again State's Exhibit 4.
A Not all pop-ups, but some of them would show up.
Q Why would one show up and not another?
A It's a good question. I never really figured that out.[89]

It seemed as if the prosecutor was fixated by the presence of web addresses and images in the Temporary Internet Files, although the final response by Mr Horner tends to undermine any expertise he might have had in respect of the analysis of digital evidence. One further exchange slightly later serves to reinforce the apparent inability of the prosecutor to understand what the witness was referring to:[x]

Q So in order for it to show up on the temporary Internet files, that person would have to actively go to that site, correct? They were not redirected to that site, correct?
A Wrong.
Q Okay.
A You don't understand.
Q I hear you saying that.
A Give me more questions.
Q I am trying to get it with you. I will do it this way. If a person is redirected to a pornographic—any web site, that would not show up in the temporary cache files, correct, based on your testimony?
A Based upon my experience, based upon my testimony, and based upon those manuals over there, a redirect does not show up. It's on the index.dat hashing files.
Q The cache file?
A Hashing.[90]

[89] 219, lines 15–27.

[90] 222, lines 21–27; 223, lines 1–12.

(c) Colour of links in Temporary Internet Files and proof of obtaining access to websites

The police officer, Mark Lounsbury, was recalled to give further evidence on the third day of the trial. He gave evidence in particular in relation to the change of colour of a link:

> Q Are there any specific characteristics that may occur to a web page when you click on specific link?
> A Yes. When you click on a link, again, links are Javascripted, you click on a link, it changes color and then you will get sent to that new address, that new page or site.[91]

The prosecuting attorney continued this line of questioning:

> Q Detective, when you actively clicked on a link from the web page, what are one of the detail signs that it was an active click of a link on a web page?
> A Again, it would be a different color, it will change colors.
> Q That is based on—
> A They do that so that you know where you are now. If you have a number of links, they are all the same color, you click a link, it sends you somewhere else. You still have your list of links. You see one that is highlighted, that's where you are now.
> Q I'm going to post this on the poster here. Again, this is one of the pages you took from the hard drive originally, correct?
> A Yes.
> Q I understand you had a limited amount of time; we just contacted you this morning about this, correct?
> A Yes.
> Q I'm going to come down here and read a couple of website pages. Could you tell me what those are?
> A Bring Her To Climax, Give A Girl An Orgasm, Orgasm Machine, Pussy Orgasms, Female Sex Enhancers, Ask Our Doctors.
> Q Are those indicative of other website pages that originally existed on the computer?
> A Those are all links.
> Q I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?
> A The color, it's red.

[91] 288, lines 25–27; 289, lines 1–3.

Q And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?
A That indicates that that link was actively clicked on and you were then sent to that page.
Q Okay. So a person would actually have to click on the Female Sex Enhancers link to go to another page, correct?
A. Yes.

Not only did the police officer incorrectly indicate that the colour of the link would be altered by clicking on to the link, but he also erroneously asserted that the link had been actively clicked on in order to reach the website. When examined by the defence attorney, the police officer continued to assert that the colour of a link changed when it was visited:

Q Detective Lounsbury, you indicated that, I guess, the coloration in the photograph shown to you by Mr. Smith indicates that links were clicked on, is that correct?
A Yes, sir.
Q When you say indicated, you are not saying a hundred percent?
A I've never seen anything other than that.
Q But you're not saying a hundred percent?
A In my mind it is.
Q Are you saying you're positive?
A Based on my knowledge of how it works, yes.
Q What about the science of it also?
A Which is based on my knowledge of the science.

The police officer also asserted that he was able to specifically indicate when a website was actively clicked by a user:

Q Based on your examination of the computer, you were able to determine that this specific picture was attached to the web page that was purposefully viewed on that day?
A Yes.
Q And again, at approximately 9:54:32 a.m., correct?
A Yes, sir.
Q Last question, how do you know that?
A The information is in the source code.
Q Right now you are showing what is considered a source code.
A Yes.
Q What does that tell you in general?
A This is the web page.
Q Yes.

A And the web page is the information as to links, Javascripting—actually words that are written and images. And in here it has the name of the image, the type of image, and gives the date and time associated with the image. The web page creation date/time is the same as the image. The image name is Jasmine1.jpg. The image associated to that on that page is Jasmine1.jpg.

This is an astounding claim, being able to differentiate whether a website was deliberately viewed by looking at the source code. It would be interesting to know which source code he referred to: whether it was the source code of the websites that were visited, or whether the police officer actually went over the Internet to visit the servers that held the HTML for the websites and forensically examine their source code. This cannot be answered from the transcript of the trial.

Furthermore, the prosecuting attorney spent some time on this aspect of the evidence in his closing speech to the members of the jury:[92]

I think it's very clear that that just didn't happen, pop-ups randomly popping up over and over and over during the course of the day.

I will get back to this in a second. What I point out is that the defense's own expert indicated that if redirects were to come through, it would not leave an address on the computer.[93] I believe he stated it up there. You have to type it in, and that is when the address comes in. You don't get a mark in the temporary Internet folder unless you actively go to that site. I believe I made that clear with him.[94]

I would ask that you look at State's Exhibit 4, the Internet sites visited on the log, and you will see specific sites about masterbation.com, or orgasm.mystery.com, store.sex-superstore.com. I believe there is also later in the day vaginalcumshots.com. Based on the testimony of the defense's witness,[95] that information could only get there if she actively accessed those sites.[96]

I'm also going to bring in Mr. Fain who testified, and there is in the temporary Internet files evidence which is State's Exhibit 1, the temporary Internet files directly related to what the defense attorney stated. You would have to actively click to get at these sites.[97] Femalesexual.

[92] 315–16.

[93] This comment is not accurate. Mr Horner made it clear that such information would be available in the index.dat file.

[94] This comment is not accurate, because Mr Horner made it clear that several logs had to be reviewed, including the index.dat file.

[95] There does not appear to be any aspect of Mr Horner's evidence to substantiate this claim made by the prosecuting attorney in his closing speech.

[96] This statement is inaccurate and does not reflect Mr Horner's evidence.

[97] This is a further inaccurate statement that is not substantiated by the evidence.

com, cheating-lesbians.com. I would ask you to go through that, correlate that with the time, correlate that with what their witness said about you have to actively physically click on it to get to the site.[98]

Finally, as you recall I brought Detective Lounsbury back in. Exhibit 6 hopefully is trying to explain the difference in color as to the Javascript elements which he clicked on. Some of us using our common sense understand this; when you click on a web page it transfers you over. And that changes to show that you actually accessed that page.[99] Take this in to account for intent; that the defendant purposely accessed those websites.

I think the evidence is overwhelming that she did purposely access those websites and she should be found guilty of all of those counts by the information the state put forward.

Factually, the evidence given to the members of the jury relating to the change in colour was incorrect for a number of reasons. First, however, it is admitted that whenever a website is visited, whether it is clicked on by a user or not, the colour does tend to change, although there are exceptions.[100] However, the colour of the links had been changed in the registry of the computer from the default red to a greenish-grey colour, and not to red, as indicated by Mark Lounsbury in his evidence. The default colour of the links were defined in the registry as '96,100,32', a greenish-grey colour. The relevant entry was named '\Software\Microsoft\InternetExplorer\Settings\Anchor Color Visited', which in turn was found in the USER.DAT registry in the Windows directory.[101]

By comparing the evidence of Mark Lounsbury to the contents of the hard drive, Alex A Eckelberry and his colleagues were able to determine that Mr Lounsbury probably referred to a website 'orgasm-mystery.com'. By examining the HTML source on the relevant page, it was possible to demonstrate that the text 'Female sex enhancers' that appeared in the Temporary Internet Files, which was coloured red, was actually coloured red by the designer of the webpage, and not because it was visited:

```
<img src="images/folder_25a.gif" width="18"
height="12" align="absbottom"><a target="_blank"
```

[98] This is a further inaccurate statement that is not substantiated by the evidence.

[99] Although not explicitly proven by the evidence, this statement is not accurate.

[100] Jakob Nielsen, Change the Color of Visited Links, Alertbox, 3 May 2004, online at <http://www.useit.com/alertbox/20040503.html>; 'Usability violation: link colors that don't change when visited', online at <http://justaddwater.dk/2007/07/24/usability-violation-link-colors-that-dont-change-when-visited/>; see also 'Visited links don't change colour on this forum. Why?', a comment added on Monday 21 May 2007 at 8:17 am in relation to the change of colour, online at <http://www.accessifyforum.com/viewtopic.php?t=8154>.

[101] Eckelberry et al (n 44) 11–12.

```
href="viagra-cream-for-woman.htm"><font
color="#FF0000">Female sex enhancers!</font></a>
```

The text `<font color="#FF0000">` indicates the colour of the link, as given by the web designer.[102] Further, Mr Lounsbury also gave evidence that the link was visited at 9.54.32 am on 19 October 2004.[103] Mr A Eckelberry and his colleagues failed to find any evidence that such a visit had occurred. Apparently, the link on the page referred to by Mr Lounsbury refers to a page entitled 'viagra-cream-for-woman.htm', and this page does not appear in any of the Internet File caches or the Internet History DAT files. There was no recorded attempt to obtain access to or retrieve this page.[104] If this is correct, his evidence was both incorrect and misleading.

(d) Endless loop of unsuitable images

The defence questioned Mr Hertz about pornography, and whether it can be produced in a seemingly endless loop:

> Q Thank you. Is it possible to be in an endless loop of pornography?
> A I've never seen that, so I would have to say probably not.[105]

The correct answer would have been to indicate that he did not know, rather than assert that such endless loops were improbable. The fact is, that 'mouse trapping' is an entrapment technique that prevents or delays a user leaving a website, and occurs regularly on pornographic websites.[106] Mark Lounsbury was also asked about this by the prosecution attorney when he returned to give evidence on the third day of the trial:

[102] 219, lines 15–25; Eckelberry et al (n 44) 12–13; Mr A Eckelberry and his colleagues also indicate clearly where they found this page, and how it came to be on the computer. Had Mr Lounsbury conducted a thorough investigation, he would have discovered the same information as described by Mr A Eckelberry and his colleagues.

[103] 292, lines 5–10.

[104] Eckelberry et al (n 44) 13–14.

[105] 88, lines 3–6.

[106] For a definition, see 'Protecting Australian Families Online', Australian Government NetAlert, <http://www.netalert.gov.au/programs/cybersafe_schools/Support/cybernetrix/support_content/glossary.html#P>; see also the discussion of 'mousetrapping' in the claim to transfer a domain name in the case of *Qwest Communications International Inc v Domain Admin a/k/a DomDom*, Claim Number: FA0406000286024, National Arbitration Forum, decision by the Honorable Charles K McCotter, Jr (Ret), Panelist, 26 July 2004, <http://www.arb-forum.com/domains/decisions/286024.htm> and the case of *Federal Trade Commission, v John Zuccarini, individually and doing business as Cupcake Party, et al*, (United States District Court for the Eastern District of Pennsylvania), Civil Action No 2:01-CV-04854-BMS, FTC File No: X010063, available online at <http://www.ftc.gov/os/caselist/zuccarini/index.shtm>.

Q Was there any indication that there were uncontrollable pop-ups?
A There was no evidence.[107]

However, Mr A Eckelberry and his colleagues found evidence of what they describe as pop-ups that occurred in a rapid fashion, described as soon as one pop-up was closed, so more would appear. From an analysis log created by Joe Stewart, the following was observed:

Cache entry created: 2004-10-19 09:19:26
File mtime: 2004-10-19 09:19:28
Last access by IE: 2—4-10-19 09:19:26
File path: whur4da3\a@Position3[1]
http://network.realmedia.com/RealMedia/ads/adstream_jx.ads/harinews/1x1pop/ron/wmn/ss/a@Position3

Apparently, this page was loaded 21 times in one second, according to an analysis performed by Glenn Dardick when using the computer forensics tool X-Ways Trace. The team also found another page, <www.about masturbation.com>, that was loaded 16 times in one second.[108]

A final comment might usefully be mentioned at this point. Various references were made to JavaScript during the course of the trial. However, it was never clear, nor is it clear now, what the relevance of JavaScript is to the links relating to websites. This is also commented upon by Mr A Eckelberry and his colleagues in their report.

(e) The length of time the pop-ups appeared

Julie Amero had a poor recollection of the events of the day, although it is not surprising, given that she gave evidence over two years after the incident and the experience of the pop-ups probably affected her perception of the time scale, given the trauma she must have been subject to when seeing the images appearing on the teacher's screen in a classroom full of children that she was responsible for. During cross-examination, Ms Amero accepted the suggestion of the prosecutor that the pop-ups occurred all day:

Q Were these alleged pop-ups, as you called them, happening, I should say all day?
A Yes.
Q From when you first were in the classroom alone without Mr. Napp?
A Yes.

[107] 294, lines 4–6.

[108] Eckelberry et al (n 44) 14–15.

Q Until the end of the day, correct?
A Yes.[109]

Mr Hartz also erroneously referred to activity continuing the entire day, from around 8.30 am or thereabouts.[110] However, the reports by Mr A Eckelberry and his colleagues indicate that the logs demonstrate that the last pop-ups of a pornographic nature appeared at 11.13 am. Thereafter, no further pop-ups appeared on the screen.

The failure of the prosecution to make it clear how long the pop-ups appeared on the screen acted to infer that Ms Amero's evidence was correct, that the pop-ups appeared throughout the day. This was particularly damaging to her case, because it might have been assumed by the members of the jury that Ms Amero left the computer at the end of the day with pornographic images actually on the screen, which was not correct. Indeed, the prosecuting attorney indicated in his closing speech that Ms Amero was viewing pornography all day: 'It's the state's contention that she purposefully went to these websites, was sitting there all day, that is the evidence, viewing the Internet.'[111]

The prejudicial effect of failing to correct the impression that the pop-ups appeared on the screen all day cannot be over-emphasized. The defence ought to have been advised of this by their expert witness, and ought to have cross-examined the police officer in relation to this matter.

6. Possible Tampering with the Evidence

Mr A Eckelberry and his colleagues found evidence that the hard drive was altered after 19 October 2004. Apparently, the entry for the 'Haunted House screensaver' which was downloaded on 12 October 2004 from screensaver.com was still in the registry, but the entire directory was missing from the hard drive, where it was installed into C:Program Files\ScreenSaver.com\Haunted House. It was not clear if any uninstall process would remove the entire ScreenSaver.com directory, or the directory tree was deleted because it was recognized that is might be some form of malicious software.[112] In addition, they also found that on 20 October 2004 at 15:19:18, website address <http://store.sex-superstore.com/favicon.ico> was stored in the cache. A favicon (favorites icon) is also known as a website icon, a page icon or an urlicon. This is an icon that is associated with a particular website or webpage. Where a browser supports favicons, the browser may display them in the URL bar, next to the name of the website in the bookmarks list. Internet Explorer 6 would, generally, only

[109] 245, lines 19–26; see also 236, lines 13–16.
[110] 64, lines 20–27; 65, lines 1–4.
[111] 317, lines 3–6.
[112] Eckelberry et al (n 44) 17.

ask a website for a favicon when it is deliberately added by the user to the Favourites folder. The entry for sex-superstore.com was no longer in the Favourites folder on the copy of the hard disk, which means it was removed on 20 October 2004.[113]

Given these findings, the defence expert ought to have alerted the defence lawyer to these issues. That is, if Mr Horner was himself aware of these important points. Mr Napp gave evidence to the effect that he never permitted students to use the computer reserved for his use,[114] and given that he appeared to be the only other person to have used the computer, he ought to have been subject to examination and cross-examination respecting these findings, serious as they undoubtedly are. This is reinforced by the findings of Mr Eckelberry and his colleagues, in that they discovered a number of websites that were regularly visited before 19 October 2004 that were not related to education, such as ESPN.com, CBS Sportsline, ffch.football.sportsline.com/standings, football.fantasysports.yahoo.com, eharmony.com (a dating website) and Peoples.com (an online banking website).[115]

7. Unfairness of a Prejudicial Nature

A number of aspects of the trial are striking, because of apparent unfairness that might have had a prejudicial effect on the minds of the members of the jury. First, the prosecution failed to provide a clear indication of the sequence of events, the times that the seven children that gave evidence were actually in the classroom, at what time they saw the images, the size of the images they saw, and precisely which images they saw (although this latter point might not be of relevance, and it will have been difficult for a child to recall the precise nature of the images they saw two years before giving evidence). The prosecution took great pains to illustrate a number of images to the members of the jury through a computer and projected on to a screen in the court, but failed to indicate whether any of the images shown to the members of the jury had been seen by any of the child witnesses, and also failed to indicate which image was related to each of the four charges, although it might have been impossible to link a particular image to what a child saw some two years after the event. It is also uncertain whether any of the images seen by the members of the jury corresponded to the images seen by the children, which is, arguably, a more important point.

Secondly, of equal seriousness is the fact that it appears the images that were shown to the members of the jury were viewed many sizes greater than the image that originally appeared on the computer screen. Mr Horner did

[113] Eckelberry et al (n 44) 17.
[114] 35, lines 1–3; 47, lines 18–23; 48, lines 24–27; 49, lines 1–2.
[115] Eckelberry et al (n 44) 18.

not give evidence on this point, but referred to the size of the images later:

> All of the jpg's that we looked at in the internet cache folders were of the 5, 6 and 15 kB size, very small images indeed. Normally, when a person goes to a pornographic website they are interested in the larger pictures of greater resolution and those jpgs would be at least 35 kB and larger. We found no evidence of where this kind of surfing was exercised on October 19, 2004.[116]

This is a significant issue that the defence failed to deal with when cross-examining the police officer. This means that where a pop-up was only a matter of two inches square, for instance, the image would be magnified many times on the screen shown to the members of the jury. Further, there was no evidence to indicate where the images that were shown to the members of the jury were actually placed on a page. It is conceivable for a page to be very long, with a large number of pop-ups arranged throughout the page, and only a small fraction of the images would be seen on the screen, unless the viewer scrolled down the screen to bring other images into view.

The defence attorney took issue with the prosecution in relation to the intention to reproduce the images on a screen, and objected in a somewhat dilatory fashion to the proposed size of the images that the prosecution intended to show the members of the jury:

> THE COURT: Good morning. Any preliminary issues before we bring out the jury?
> MR. COCHEO: I have an objection, Your Honor, to the size of the photos that the prosecution intends to show the jury. My claim is that it will be highly prejudicial to the jury to see these large photos of these sexually explicit allegations on the screen.
> MR. SMITH: Clearly, it will be prejudicial, that is the whole point of showing the pictures, although it is not excessively prejudicial. I think it's informative to the jury. I don't think they are highly large size. They are clearly not excessively large. It is easier for the jury to see, and I think the state is allowed to present its evidence as it sees fit to communicate to the jury.
> THE COURT: I will overrule your objection, Mr. Cocheo. It's an element of the crimes charged and the state has a right to its proof. I believe it's going to be through the overhead projector.

[116] 'The Strange Case of Ms Julie Amero: Commentary by Mr. Herb Horner', online at <http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_1.html>.

MR. SMITH: It will come through the computer, through the projector up across the courtroom away from the jurors, and it's large enough so they will be able to see it. But well below—. I do not believe it will be excessively large.
THE COURT: I will overrule your objection right now, but if it appears to be an excessively large picture, you can again, we will take it up at that time.
When the prosecution was ready to illustrate some of the images to the members of the jury, the defence attorney raised his objection once more:[118]
MR. SMITH: At this point, I ask for permission to publish, not necessarily all, but some of the images in the information to the jury.
THE COURT: Any objection?
MR. COCHEO: Well, my objection stands, Your Honor.
THE COURT: Your Original objection?
MR. COCHEO: Yes.
THE COURT: That was overruled. Yes. You may publish. You don't need to leave them up.
MR. SMITH: I will not, Your Honor.[117]

There can be no doubt that the images were prejudicial, but if they had been published to the members of the jury in the same size as had appeared on the computer screen, it would have been perfectly proper for the prosecution to ask for and be granted the right to exhibit the images to the members of the jury. However, there was no evidence as to the size of the images that were seen by the children, but there was a great deal of evidence to make it clear that the images appeared to be pop-ups, rather than images that filled the screen. From an organizational point of view, this trial ought to have taken place in a court with appropriate facilities, so that the judge, members of the jury and the lawyers had screens in front of them, thus enabling the correct size of the files to be replicated for the purpose of the proceedings. Whether such a request was ever made by the defence or the prosecution is not known, but this is a prime example of the need for courts to have suitable facilities made available, otherwise evidence will continue to be distorted in the same way in the future as it was in this case. The defence had a perfectly legitimate reason for opposing the prosecution with respect to the size of the images to be shown to the jury. This matter was not well argued or, arguably, at all, and the learned judge, it is suggested, ought to have considered the application in more detail than she did.

The third point relates to the way the learned judge responded to the defence's failure to produce its expert report in advance. It appears that the

[117] 114, lines 1–26; 115, lines 1–4.

[118] 124, lines 8–18.

prosecution requested disclosure of the documents, but they were not made available:

> MR. SMITH: Judge, here is the problem I had at the bench and I will state it for the record. Quite a while ago I asked for discovery on any documents that he had created or was going to use in the course of this trial, specifically for this. That has been displayed. Unfortunately, the jury has already seen it. They are definitions of various programs that he allegedly or supposedly used to check it out. There is various information that was allegedly or supposedly on the hard drive copy that he got, that I would have liked to check it out obviously before trial. For example, one of them is, I believe, is a security alert document, spyware program, noted market score and the like. I don't see how I can effectively cross-examine based on these documents that I should have gotten before trial so I could check it out.
> THE COURT: Why weren't these provided?
> MR. COCHEO: I did not have these documents, Your Honor.
> THE COURT: You didn't have them, but now here they are. So I am not allowing it. What will have to happen, your witness can testify about what he did and what happened regarding Mr. Napp's computer on that day and what the results of his investigation were. All right?
> MR. COCHEO: Thank you, Your Honor.

Clearly the failure of the defence to provide a copy of the expert report it intended to rely upon in advance was a serious error, and ought to have been at the centre of the defence attorney's mind when preparing for the trial. No matter how embarrassing, the defence attorney ought to have made an application for the trial date to be moved if the expert witness failed to provide the report on time, or he ought to have alerted the learned judge to the issue immediately, and certainly before the defence case began, if not before the trial began. However, the prosecution attorney was aware that the defence had an expert witness, as pointed out at the beginning of the trial:[119]

> MR. SMITH: At this time, the state would invoke the rule of sequestration. The state has spoken to defense counsel. The rule of sequestration is to have witnesses not speak about the case, however, the defense does have an expert witness. The state does not have an objection to the expert witness being present when the state presents evidence by its two witnesses, specifically concerning the computers, which would be Mr. Hartz and Detective Lounsbury.
> THE COURT: Is that by agreement?
> MR. COCHEO: Yes, Your Honor.[120]

[119] 4, lines 11–22. [120] 193, lines 1–27; 194, line 1.

It seems to be somewhat inattentive of the prosecution to have failed to formally request at this early stage of the trial whether the defence expert would be relying on a report of his findings. Further, it also seems somewhat odd that the prosecution failed to ask the defence for a copy well before the trial, given that the defence were requested to provide a copy of the report in advance. The prosecution could easily have requested a preliminary hearing before the learned trial judge to ascertain when the report was going to be disclosed by the defence.

The learned judge was adamant that the defence case would proceed in the absence of the evidence outlined in Mr Horner's report:

> THE COURT: That was all supposed to be provided to the state before, all of it.
> MR. HORNER: They can have it.
> THE COURT: You don't understand. This is a trial. This is over. There is no time now. We are going forward right now. The demonstration—you can go to a website, if that is what you want, if it is a website that the computer went to that day.[121]

Although the learned trial judge was put into an unenviable position at such a point during the trial, but given that the charges were laid against a woman who had no previous convictions, and each charge had a penalty of a maximum of 10 years' imprisonment (even if imprisonment was an unlikely sentencing option in these circumstances), it is respectfully suggested that the learned judge ought to have considered this matter for slightly longer, and considered suspending the trial for a day to enable the prosecution to review Mr Horner's report. In the interests of justice, it might have been appropriate to canvass how quickly the prosecution could read through and respond to the report prepared by Mr Horner before making a final decision on the matter.

8. Where the Blame Should Lie

This is a disturbing case for a number of reasons. Arguably, the school ought to have been challenged for failing to protect a teacher from having to cope with such a traumatic experience. However, the provisions of section 230 'Protection for private blocking and screening of offensive material' of the Computer Decency Act (47 USC Sec 230) appears to provide a safe haven for schools in the circumstances that Ms Amero found herself in, although it is conceivable that action might have been taken against the school under the terms of 'E-rate', which is the common name

[121] 195, lines 9–16.

for the Universal Service Fund for Schools and Libraries, established by section 254 of the Federal Telecommunications Act of 1996, in combination with the provisions of the Children's Internet Protection Act. The Children's Internet Protection Act provides as follows:

> SEC. 3601. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.
> (a) INTERNET SAFETY.—
> (1) IN GENERAL.—No funds made available under this title to a local educational agency for an elementary or secondary school that does not receive services at discount rates under section 254(h)(5) of the Communications Act of 1934, as added by section 1721 of Children's Internet Protection Act, may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such school unless the school, school board, local educational agency, or other authority with responsibility for administration of such school both—
> (A)(i) has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—
> (I) obscene;
> (II) child pornography; or
> (III) harmful to minors; and
> (ii) is enforcing the operation of such technology protection measure during any use of such computers by minors; and
> (B)(i) has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—
> (I) obscene; or
> (II) child pornography; and
> (ii) is enforcing the operation of such technology protection measure during any use of such computers.

Section 3601 further provides, in sub-section 2, that the school or relevant authority is required to provide assurances that it has put in place those requirements set out in sub-sections (a) and (b):

> (2) TIMING AND APPLICABILITY OF IMPLEMENTATION.—
> (A) IN GENERAL.—The local educational agency with responsibility for a school covered by paragraph (1) shall certify the compliance of such school with the requirements of paragraph (1) as part of the appli-

> cation process for the next program funding year under this Act following the effective date of this section, and for each subsequent program funding year thereafter.
> (B) PROCESS.—
> (i) SCHOOLS WITH INTERNET SAFETY POLICIES AND TECHNOLOGY PROTECTION MEASURES IN PLACE.—A local educational agency with responsibility for a school covered by paragraph (1) that has in place an Internet safety policy meeting the requirements of paragraph (1) shall certify its compliance with paragraph (1) during each annual program application cycle under this Act.

In a 2006 report by Judith Lohman, prepared at the request of the Connecticut General Assembly, it was stated that

> The Connecticut Education Network (CEN) provides schools, libraries, and higher education institutions with high-speed Internet access, among other things. According to Rob Vietzke, CEN's co-program manager and network architect, connections were available in all K-12 school districts at the start of the 2005–06 school year.[122]

Although this report referred to a period of time after 2004, it will be of interest to know whether the Connecticut Education Network included Kelly Middle School at the material time, and if it did, what action, if any, was taken against the school for failing to protect the children and members of staff as required under the terms of the Children's Internet Protection Act.

This case starkly illustrates the risks involved with the use of the Internet in schools. Although the subject of this case only covered one aspect of the use of the Internet, nevertheless it can only be the subject of speculation as to how well protected the files of students are in schools across the world, not just in the United States of America. It appears that teaching unions have remained mute in respect of the digital revolution that politicians have imposed upon schools, and teachers have been made to use technology without understanding the risks, with little or poor training, and the governing bodies of schools have failed to provide adequate protection, not only to the teachers, as this case illustrates, but also to the children. It appears that Ms Amero used the Internet in the past to a degree that caused Mr Fain to discuss this with her before the incident occurred,[123] and it is also pertinent to note that Ms Amero's actions in attempting to shield the children from viewing the images on the screen can hardly be described as

[122] J Lohman (Chief Analyst), 'Connecticut Education Network and E-Rate' (9 January 2006) 2006-R-0036, available online at <http://www.cga.ct.gov/2006/rpt/2006-R-0036.htm>.
[123] 21, lines 120–27; 22, lines 1–9.

adequate in the circumstances, although it may be perfectly correct to accept that her knowledge of computers was so poor that she did not know that she could switch off the monitor without switching off the computer. In this respect, there can be no doubt that the blame can be laid at the door of her employers for failing to provide her with any adequate training, as well as failing to protect her and the children in the class she was responsible for.

C. CASE STUDY: *STATE OF ARIZONA V BANDY*[124]

In November 2004, the Internet service provider Yahoo!, sent a report to the National Center for Missing and Exploited Children's CyberTipline detailing that on 7 November 2004, abusive images of children were uploaded to a location on one of their servers that contained a Yahoo! group 'beth_lard9'. The person that caused the images to be posted logged into the group using the screen name 'mrbob1980hoopdu'. Detectives assigned to the Internet Crimes Against Children Task Force of the Phoenix Police Department carried out the subsequent investigation.[125] Yahoo! are required to report abusive images of children under section 13032(b)(1), Title 42, Chapter 132, Subchapter 4, US Code, dealing with the reporting of child pornography by electronic communication service providers, the relevant part of which reads:

> (1) Duty to report.—Whoever, while engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce, obtains knowledge of facts or circumstances from which a violation of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of title 18, involving child pornography (as defined in section 2256 of that title), or a violation of section 1466A of that title, is apparent, shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General.

An application was subsequently made for a subpoena directed to Yahoo!, requesting the subscriber information for the person using the screen name

[124] Case number CR2005-014635-001 DT. Matthew Bandy was born on 23 March 1988.

[125] The facts are partly taken from AP Thomas, *Memorandum: Factual and Forensic Report State of Arizona v Matthew Bandy CR2005-014635-001 DT*, (Office of the Maricopa County Attorney, 2 February 2007), available online at <http://www.maricopacountyattorney.org/Press/PDF/bandy_case_20070107.pdf>.

'mrbob1980hoopdu'. Yahoo! subsequently provided the subscriber information, together with the most recent log-in times recorded for this user. The user provides the subscriber information when the account is created, although the accuracy of the information is not verified. In this instance, the user made the following entries in the various fields:

Full name: 'Ms. Joe Bean'
City: 'Phoenix'
State: 'AZ'

The account 'mrbob1980hoopdu' was created on 5 November 2004, using the IP address 68.98.62.49 owned by Cox Communications, Inc. The user of the account 'mrbob1980hoopdu' used the same IP address to log in from 5 November to 8 November 2004. A subpoena was served on Cox Communications, Inc to determine the name and address of customer that was assigned the IP address during the material time, and Cox confirmed that the account was registered to a Greg Bandy of 1425 E Desert Broom Way in Phoenix, and the veracity of this information was checked by other conventional methods. On 16 December 2004, a warrant was served at the Bandy residence. During the course of the search, one of the detectives heard Matthew Bandy tell his mother that he had obtained access to Yahoo! groups. During the course of the search, Matthew Bandy agreed to speak with the detectives. He admitted that he had created the screen name 'joebean1988hoopdu' to obtain access to Yahoo!, and he denied any knowledge of the screen name 'mrbob1980hoopdu'. He stated that he viewed adult pornography, but did not download any of the images he viewed. Mr and Mrs Bandy denied using the computer for improper purposes, and a result of which they were not considered suspects.

Detective Larry Core of the Maricopa County Attorney's Office, a computer forensics investigator certified by the International Association of Computer Investigative Specialists (IACIS), conducted a forensic preview of the computer that Matthew Bandy admitted using. A text search of the computer indicated that the screen name 'mrbob1980hoopdu' was listed approximately 80 times, and the Yahoo! group 'beth_lard9' was listed approximately 500 times. Thumbnail images of abusive images of children were also found. The computer equipment, including compact discs burnt at home, were seized under the provisions of the warrant to enable a full forensic analysis to be carried out.

1. Results of the Forensic Examinations

In all, three forensic investigations were carried out by the police, and one forensic examination by Tami I Loehrs of Law2000, Inc for the defence.

(a) First forensic investigation by the police

The first forensic analysis of the computer equipment was carried out in June 2005. Using the latest version of the forensic software programme EnCase at the time, the following evidence of relevance was revealed (taken from the Memorandum of Andrew P Thomas, pp 3–4):[126]

> Located in 'D\documents and Settings\Owner\My Documents\My eBooks' was a folder called ('). Located under (') was a subfolder called 'kid'. Located under 'kid' was a subfolder called 'Lolita' that contained images of child pornography. Located under 'Lolita' was a subfolder called 'good ones' that contained 72 images of child pornography. The images received by Detective Curley in his complaint matched almost all of the images on the CD.
> Searching for the word 'mrbob1980hoopdu' received 299 hits.
> Searching for the word 'beth_lard9' received 949 hits.
> Located in the 'Temporary Internet Files' were deleted images of adult and sexual cartoons pornography.
> Text fragments were bookmarked that did show the pornography sites were visited.
> Located in the 'Recycler Folder' were images of young children and sexual cartoons.
> Located in the 'Recycler Folder' were link files to pornography.
> Deleted from the 'Recycler Folders' were various pornography files.
> Located on the hard drive was the profile of 'mrbob1980hoopdu'.
> Located on the hard drive was the e-mail address of 'mrbob992000'.
> Located on the hard drive in unallocated clusters was the following.
>
> [Basic User Info (EReg)]
> firstname=matt
> middle initial=G
> lastname=Bandy
> company=none
> address=1425 Youdontneedtoknow lane
> address2=
> city=Phoenix
> Country=UNITED STATES|USA
> state=Arizona|AZ
> zip code=15489
> phone=000-867-5309
> phone extension=

[126] For a more detailed list of the findings, see Andrew P Thomas *Memorandum: Factual and Forensic Report State of Arizona v. Matthew Bandy CR2005-014635-001 DT.*

dialout prefix=
use dialout prefix=
email=mrbob1980hoopdu@yahoo.com
email2=
Gender=MALE
Address Type=HOME
Phone Type=HOME
Use=PERSONAL

The relevance of this last finding cannot be over-estimated, because it includes the screen name 'mrbob1980hoopdu@yahoo.com', which Matthew Bandy denied using.

A forensic examination of the CDs was also carried out. One of the CDs contained the same abusive images of children that were located on the hard drive of the computer. It had 51 folders that contained over 2,800 images of abusive images of children, adult pornography and animated child pornography. This CD was created by Roxio DVD and CD burning software, and Roxio was on the hard drive in the computer when the CD was burned. Apparently the Bandy's claimed that this CD was a back-up of the entire computer system, and when it was reloaded onto the computer, these images were inadvertently put back as part of the installation. This was impossible, because the CD had a storage capacity of 650 megabytes, whilst the computer contained more than 100 gigabytes of files. There was a folder named 'kid/lolita/goodones' on the CD that contained abusive images of children. Several of the images were saved to the CD on 11 November 2004, the date the uploads were reported to Phoenix Police Department. The police concluded that the forensic evidence pointed to Matthew Bandy. The defence offered different theories of why this conduct should not be attributed to him, including the theory of a malicious virus. This caused the police to conduct a second examination conducted on 28 September 2006 for the purpose of testing the defendant's theories.

(b) Second forensic examination by the police

The second examination of the hard drive revealed the following:

The operating system was first installed on 9 April 2003 at 4:06 pm, and was reinstalled on 4 December 2004 at 05:41:52 pm.
The folders and files that contained the abusive images of children were created on 4 December 2004 at between 05:48:15pm and 05:48:24 pm.
Approximately 72 files were installed on the hard drive on 8 December 2004 at 03:57 pm in 'My Documents Folder'.
The images that were the subject of the charges were located on both the hard drive and the CD. The MD5 hash matched all of the images.

The police reached the conclusion that it was not impossible for a malicious virus, Trojan, worm, or a hacker to do the following:

> Create the screen name of 'mrbob1980hoopdu@yahoo.com' with the user information of Matt G. Bandy.
> Download child pornography on 11 November 2004.
> Burn the abusive images of children to a CD.
> Reinstall the operating system on 4 December 2004.
> Insert the CD into the CD drive and create folders in 'D:\Documents and Settings\Owner \My Documents\My eBook\'\kid\Lolita\good ones' and then transfer images from the CD back to the hard drive.

In addition, the police claimed that it was not possible for a malicious virus, Trojan, worm, or a hacker to create the 72 files on 8 December 2004 at the same time on the hard drive in 'My Documents Folder'. On these files, 32 images of animated abusive images of children were created between 5.48.29 pm and 5.48.32 pm on 12 December 2004 in a folder named 'Animated', and 120 images were created on 4 December 2004 between 5.47.42 pm and 5.47.49 pm in a folder named 'Tight'.

(c) Forensic examination for the defence

Tami I Loehrs of Law2000, Inc conducted an examination of a copy of the hard disk for the defence, although she did not examine the copy of the CD that was also passed to her by the police.[127] This report is the subject of criticisms by the police, which are set out in the Memorandum by Andrew P Thomas, pages 7–11. In her report, Ms Loehrs noted that she located over 200 infected files, and stated on page 4 of her report that 'one or more of the infections identified on the system renamed a significant number of computer files making it impossible to detect or track all of the activity'. Ms Loehrs could not positively identify all of the intrusions found on the system, although she listed the following on page 5 of her report: Backdoor.W32.Rbot,[128] Backdoor.Rbot.gen,[129] TrojanProxy.Win32.

[127] A copy of this report is available by way of a hyperlink online at <http://www.justice4matt.com/>.

[128] The description provided by Ms Loehrs for this process is taken from <http://www.processlibrary.com/directory/files/bb>; the website suggests that this process is probably adware or spyware.

[129] The description provided by Ms Loehrs for this process is taken from <http://www.f-secure.com/v-descs/rbot.shtml>; this is described by the web site as a remote access tool for a hacker, also known as a backdoor, and it is possible for such a tool to enable a hacker to control a computer remotely.

Bobax.c,[130] Win32.Winshow.G,[131] divx.exe[132] and instsrv.exe.[133] In addition, Ms Loehrs identified

> a significant number of suspicious executable files that began running on or about 11/6/2004 and continued through 12/3/2004. All files had similar naming conventions (ie: A0004696.exe, A0009921.exe, A0007346.exe, etc.) I was unable to determine the purpose of these files, however, they appear to be related to one or more of the backdoor Trojans identified on the system.

Ms Loehrs provided the following conclusion, which bears quoting in full:

> Based on my examination and analysis of the digital evidence in this case (ie: HDD01) I found the system extensively infected with malicious software. While I did note current anti-virus software installed, I can only conclude that it was not functioning properly or had been disabled due to the significant number of viruses, Trojans and worms infecting the system.[134] Of considerable concern are the backdoor Trojans found on the system. With no firewall protection in place, the system was extremely vulnerable to compromise by outside sources such as hackers. Conversely, with no IDS system in place,[135] it would be virtually impossible to determine if, when or by whom the system was compromised. In this regard, it would be impossible to state with certainty which activities were conducted by users within the household and which activities were a result of one of the many malicious software applications and/or outside sources such as hackers.

[130] The description provided by Ms Loehrs for this process is taken from <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BOBAX.C>; this is described as a worm that is known to exploit a Windows vulnerability that allows an attacker to gain full control of an affected system.

[131] The description provided by Ms Loehrs for this process is taken from <http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=39170>; this is described as a Trojan that redirects a user's Internet Explorer start page and search URLs with the intent to increase the number of visits to webpages owned by the author of the Trojan.

[132] The description provided by Ms Loehrs for this process is taken from <http://www.auditmypc.com/process/dr-divx.asp>; the website is indicated that it is not certain whether dr.divx.exe is spyware or a Trojan.

[133] The description provided by Ms Loehrs for this process is taken from <http://www.auditmypc.com/process/instsrv.asp>; the website considered this is possible a worm.

[134] On this point, the police stated, on page 11 of the Memorandum by Andrew P Thomas, that: 'In fact, the Norton Antivirus on Bandy's hard drive was running and the "Auto-Protect" was on, "Email Scanning" was off, "Script Blocking" was on, "Automatic LiveUpdate" was on, and the system was scanned on December 10, 2004. The virus definitions were updated on December 15, 2004. See Exhibit 13.' This illustrates the point that anti-virus software does not work.

[135] An IDS system is an intrusion detection system.

> Further, all activity on this computer was conducted under the default user account 'Owner'. Computer activity is often associated with a user based on the personal account with which they log on to the computer. With no personal user accounts identified, it is impossible to state with any certainty which user was responsible for which activity.[136]

(d) Third forensic examination by the police

The police conducted a third examination of the hard drive after the television station ABC discussed the case of Matthew Bandy during an episode of 20/20, in which Ms Loehrs claimed, according to the Memorandum by Andrew P Thomas, that a hacker had corrupted the hard drive by using a backdoor Trojan to save abusive images of children on the computer. In response to the comments by Ms Loehrs, the Memorandum made the following observations:

> Where Ms. Loehrs identified six Trojans, the investigation found only two on the hard drive, neither of which were capable of permitting a third person to control the computer remotely.
>
> The virus 'instsrv.exe' was described as the 'bargain buddy' adware program, which is not capable of controlling a computer remotely.
>
> The virus divx.exe, which, it was stated in the Memorandum, was created to target users downloading abusive images of children and illegal software, had the error message 'failed to download url;' and this was also not able to control the computer.
>
> The other Trojan and adware files listed by Ms Loehrs in her report were not found on the computer.
>
> Ms. Loehrs reported that the viruses were present between 6 November 2004 and 3 December 3004, however, the relevant files were viewed before the viruses were found on the hard drive.

2. The Expert Reports

It is instructive to be given an insight into the content of a report by a digital evidence specialist, and to be able to read the criticisms by the other party to the proceedings. This is particularly relevant, because the police examined the hard disk three times, and found increasing amount of information on each occasion. Although the quality of the examination is important, nevertheless it is the interpretation of the evidence found as a result of

[136] It should be noted that the level of technical knowledge of lay people is such that the vast majority of computers in households are used by all members of the household and their guests, and few have the knowledge or understanding to create separate accounts for each user.

the examination that is critical. The Memorandum by Andrew P Thomas clearly takes issue over a number of points made by Ms Loehrs, many of which appear to be entirely legitimate, and require further explanation. The report by Ms Loehrs appears to be somewhat basic in nature, and fails to offer the sort of in-depth analysis as described by Eoghan Casey.[137] It is to be be expected that an investigator should indicate precisely where the malicious software was found, such as in the Windows or the Windows\System folder, and to identify the precise name of the relevant malicious software. Also, it is necessary for the digital evidence specialist to report on what they found, and in this case Ms Loehrs ought to have considered providing some evidence to demonstrate how a hacker took control of the hard drive. There was a difference of opinion between Ms Loehrs and the police digital evidence specialist about whether is it known that a hacker can or had ever taken over the computer of a third party with the intention of storing pornography on the host computer. The police posted a question to this effect on the IACIS list server, and the responses received are included in the Memorandum by Andrew P Thomas. Whilst it appears that the responses to this question led to the consensus that the authors of the emails had no knowledge of such an occurrence, it is known that third parties will take over computers belonging to others, and the infected computer is known as a zombie. The defence is known as the 'Trojan horse' defence, and it has been known to persuade the members of a jury that pornographic images might have been added to a computer without the authority or knowledge of the owner or user of the computer.[138] Evidently the anti-virus software did not act to prevent malicious software from being added to this computer, and clearly there were significant differences between the conclusions of the two digital evidence specialists. What is disturbing about the response by the police digital evidence specialist is that a conclusion was reached about what malicious software is capable of doing (or not capable of doing, whichever the case may be) without accepting that the explanation might be correct, or taking the time and trouble to research the literature to reach a reasoned conclusion on the matter. In this respect, the conclusions of the two specialists were divergent, but neither offered a reasoned response to reinforce their position, or to rebut the conclusions of the other.

Given the fine balance as a result of the examination of the hard drive and the conclusions reached by both specialists, the lawyers found themselves in a precarious position. The prosecuting authorities are required to

[137] Casey (n 52), although dealing with the process of the investigation, nevertheless, the comments in Chapters 4 and 5 are very useful for all digital evidence specialists.

[138] *R v Schofield* (Reading Crown Court, April 2003), *R v Green* (Exeter Crown Court, October 2003) and *R v Caffrey* (Southwark Crown Court, October 2003); see also E George, 'Casenote' (June 2004) 1 Digital Investigation 89.

treat the downloading of abusive images of children with utmost seriousness. This is what society expects. As a result, it is important for the prosecutor to be satisfied that they have sufficient evidence to persuade the members of a jury that the accused is guilty of the offence charged beyond reasonable doubt. Conversely, the lawyer for the defence must weigh up the technical evidence and conclusions against other factors, such as those noted by Jonathan Bernstein:[139]

> Here's some of what the Bandys were advised by defense counsel Novak, as he summarized in an email to me:
>
> > Every jury trial has risks. Perhaps the most significant is the jury pool in the County. We find more older people, uneducated and undereducated, more unemployed and government workers in the jury box. Minorities are underrepresented. The understanding of computers by jurors is generally less than that of better educated professional or even, office workers.
> >
> > The penalties for conviction are draconian. Matt faced 90 years in prison if convicted.[140] The judge would have no discretion. Our Supreme Court recently found a 200 year sentence was not cruel and unusual. The governor cannot pardon and commutation provisions are limited.
> >
> > The jury would see the images and, like photos of any other crime scene, it is hard to get some jurors to focus on reasonable doubt once those images have been displayed.
> >
> > The polygraph tests are not admissible.[141] Matt admitted to viewing adult pornography on the computer. Inferences might be drawn from such activity by the jury.

As part of this process lawyers on both sides not only rely on the accuracy of the examination of the digital evidence, but they also have to carefully take into account the explanations and conclusions reached by the digital evidence specialists.

[139] J Bernstein, 'The Matt Bandy Story A Nightmare Before Christmas', available online at <http://www.justice4matt.com/>.

[140] See AP Thomas, *Memorandum: Factual and Forensic Report State of Arizona v Matthew Bandy CR2005-014635-001 DT*, 6, for the history of the charges and the offences Matthew Bandy entered a plea of guilty to.

[141] Mr and Mrs Bandy and Matthew Bandy took a polygraph test (see <http://www.justice4matt.com/>). Such tests, as noted, are not admissible in courts in the United States of America. The polygraph has no scientific basis, for which see GW Maschke and GJ Scalabrini, *The Lie Behind the Lie Detector* (4th edn) available in electronic format at <http://antipolygraph.org/pubs.shtml> and A Cumming, *Polygraph Used by the Department of Energy: Issues for Congress,* (CRS Report for Congress, RL31988, 14 February 2007), available online at <www.fas.org/sgp/crs/intel/RL31988.pdf>.

D. CONCLUDING REMARKS

The introduction of evidence in analogue format did not create many problems for lawyers and judges, but evidence in digital format has caused a great many concerns for a range of reasons. First, the technology changes rapidly and law schools can no longer assume they can teach law students about digital evidence at some time in the future: a law student, once they become qualified to practice, will be required to advise on digital evidence almost immediately, yet the vast majority of law students across the world are woefully ill prepared for the revolution that has already taken place.

Secondly, judges have the unenviable task of conducting a case, hearing and adjudicating on technical legal arguments introduced by lawyers, (sometimes with good reason, sometimes for a spurious reason), controlling the court and making sure justice is served whilst applying both substantive and procedural laws. The modern judge may also be required to read through a large number of papers before reaching court, and it may also be necessary for them to hear a greater number of cases than hitherto. The use of technology may have improved the ability of a judge to cope with the increased workload (a workload that has increased for most other people in work as well), but the ability to keep up to date with changes to the law, case law and new topics such as the complexities relating to digital evidence have exposed the weaknesses in judicial education. Judges must begin to insist on regular continuing education, otherwise they may face the same problems as the Honorable Hillary B Strackbein in the case of Julie Amero. It is not in the interests of judges, the parties or the legal system for judges to be out of touch with digital evidence, and the issues that legitimately surround the analysis and challenges that can be brought to bear in respect of digital evidence.[142]

Thirdly, lawyers also need to take steps to educate themselves about digital evidence. The actions of the two lawyers in the case of Julie Amero clearly illustrate that neither fully understood the nature of the evidence. From a policy point of view, it is astounding that the decision was taken to take action against the teacher, and not the school; but where action is contemplated, the lawyers involved ought to make themselves aware of the complexities that accompany evidence in digital format. Lawyers in private practice may well find that their professional indemnity insurers might take a dim view of their failure to educate themselves in relation to digital evidence, and it is not beyond the realms of possibility for an insurer to refuse to provide cover unless lawyers can prove they have taken adequate

[142] A view shared by N Ritter, 'Digital Evidence: How Law Enforcement Can Level the Playing Field With Criminal' (July 2006) 254 National Institute of Justice Journal, available online at <http://www.ojp.usdoj.gov/nij/journals/254/digital–evidence.html>.

steps to become familiar with digital evidence. Digital evidence affects all walks of life, and thus every aspect of law, not just criminal law. The recorded cases relating to digital evidence cover virtually every aspect of law in virtually every jurisdiction on the globe, and it is no excuse to argue that a particular area of law is not affected by digital evidence.

Finally, the qualifications of digital evidence specialists should be rigorously challenged in court where it is not clear if the person purporting to be an 'expert' really is a digital evidence specialist. That people can claim to have such an expertise will be for countries to determine either by setting our formal legal requirements, as indicated by the majority of the jurisdictions included in this text, or for courts to ensure that the person claiming to be a digital evidence specialist has the requisite ability and expertise to offer evidence and opinions on digital evidence. It is also for the lawyers to ensure they ask the right questions of digital evidence specialists, and to ensure they brief digital evidence specialists accurately and properly, otherwise they will never get anything near an adequate answer.