IN THE COURT OF APPEAL OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA

In the matter of an appeal in terms of Section 331 of the Code of Criminal Procedure Act No. 15 of 1979 and in terms of Article 138 of the Constitution of the Democratic Socialist Republic of Sri Lanka.

Ca Case No: CA-LTA 01/2011

HC of Colombo Case No: 3652/07

Hon. Attorney-General,
Attorney General's Department
Colombo 12.

Prosecution

Vs.

Delankage Kamal Padmasiri Bandara
Wimalawera, No.516,
Daranagama,
Udupila,Delgoda.

Accused

AND NOW BETWEEN

Hon. Attorney-General,
Attorney General's Department
Colombo 12.

Appellant

Vs.

Delankage Kamal Padmasiri Bandara
Wimalawera, No.516,
Daranagama,

Udupila, Delgoda.

Accused-Respondent

Before: **D.N. Samarakoon, J.**
B. Sasi Mahendran, J.

Counsel: Rohantha Abeysooriya, ASG, PC for the Complainant- Appellant
Dr. Sunil Abeyratna with Buddika Alagiyawanna and Kudakolowa for the Accused-Respondent

Written Submissions: 28.11.2022(by the Appellant)
28.11.2022 (by the Accused- Respondent)
On

Argued On : 07.10.2022

Decided On : 15.12.2022

B. Sasi Mahendran, J.

The Accused-Respondent (hereinafter referred to as "the Accused") was indicted in the High Court of Colombo under Section 286A(1)(C) of the Penal Code as amended by Act No. 22 of 1995. The charge as set out in the indictment reads:

"j¾I 2002 ක් වූ ud¾;= මස 31 වෙනි දිනත් j¾I 2002 ක් වූ අගෝස්තු මස 11 වෙනි දිනත් අතරතුර කාලසීමාවේදී මෙම අධිකරණයේ බලසීමාව තුල පිහිටි කැලණියේදී යුෂ්මතා තම විද්‍යුත් තැපැල් ලිපිනය මගින් ළමයින්ගේ යම් අශ්ශීල PdhdrEm wka;¾cd,fha වෙබ් අඩවියකින් බෙදා හැරීමෙන් සහ තම සන්තකයේ තබා ගැනීමෙන් 1995 අංක 22 දරණ දණ්ඩ නීති සංග්‍රහය සංශෝධන පනතින් සංශෝධිත දණ්ඩ නීති සංග්‍රහයේ 286 ඈ වෙනි වගන්තිය යටතේ දඩුවම් ලැබිය යුතු ළමයින්ට අදාලව කරනු ලබන අසභ්‍ය පලකිරීමේ වරද සිදුකල බවය."

That is, during the time period between the 31st of March 2002 and the 11th of August 2002, the Accused committed the offence of being in possession of and distributing through

a website of the internet indecent photographs of children, an offence punishable under Section 286A(1)(C) of the Penal Code, as amended by Act No. 22 of 1995.

The indictment was served on the 4th of June 2007 and the trial commenced on the 2nd of October 2007. After trial, the Accused was acquitted by the learned High Court Judge by judgment dated 28th January 2011. Aggrieved by this judgment, the Honourable Attorney General filed this appeal seeking leave to appeal and to set aside the acquittal. Leave was granted on 9th December 2011.

The facts pertaining to this case, albeit briefly, are as follows;

A post/advertisement on a lewd website on 31st March 2002 seeking "young boys between 14-20 for sex and hot relationship" resulted in the commencement of an investigation by the National Child Protection Authority (hereinafter referred to as "the NCPA"). According to the evidence of one Mrs. Chandima Sanjeewani, the Internet Protection Programme Computer Operator of the NCPA at that time (PW9), she, on the instructions of the Chairman of the NCPA, replied to that post/advertisement on the website itself using the pseudonym "Shane", a fictitious 15-year-old boy. The Accused had responded to that reply and had given an email address ('kevinw@37.com') to contact him on. She had corresponded with him using the email address 'shane86lk@yahoo.com'. There was a series of emails back and forth. She explained that her task was corresponding with the Accused via email. In one such correspondence, the Accused had provided two telephone numbers ("908165" and "908164") to contact him during the day and to ask for "Kamal" when calling those numbers. The Accused had sent several pornographic images of children in those emails.

Subsequently, the NCPA assigned one Duminda Perera (PW1), a Computer Operator of the NCPA, to lend his voice to and to bring this fictitious character Shane to life by playing the role of a decoy. He had been given a file or docket of the printouts of all the correspondences, including the pornographic images. After being given the Accused's number, as aforesaid, PW1 called him, disguising his voice as that of a teenager. They spoke over the telephone on a few occasions. In the last of such calls, they agreed to meet at the Kelaniya University, where the Accused was employed as the Senior Assistant Registrar. They agreed on the date, time, place, and description of the clothes that each would wear as well. As discussed, they met on the 11th of August 2001, a Sunday, at around 3 pm. Participating in this sting operation were, among others, Chief Inspector Thomson Wijesena - the Officer in Charge of the Special Police Investigation Unit of the

NCPA (PW3), Dimuthu Prasad Galappaththi- an Investigating Officer of the NCPA (PW2), Channa Nishantha Soysa a Computer Data Entry Operator/ Recorder of the NCPA (PW5), an Investigating Officer (one Priyantha) and a few officers from the Peliyagoda Police Station. PW1 carried a small bag with a video camera that was carefully hidden in the bag in a manner that would not be visible to anyone, but capable of capturing the saga as it unfolded.

PW1, who described himself to be in an anxious state of mind as this was his first sting operation, initially whizzed past the Accused who was standing at an entrance where they were supposed to meet, dressed in the clothes he had said he would be clad in. When PW1 arrived back at the place they were supposed to meet, where the Accused was standing, the Accused said to him "කඩාගෙන ගියා නේද" (roughly translated: [you] went full speed, right). The Accused then invited him into his office and was arrested when they were making their way to his office.

At the trial, the Prosecution led the evidence of the twelve witnesses. P21 to P27, PX, and PY were the documents and productions that were marked by the Prosecution. After the Prosecution closed its case, the Accused made a dock statement and led the evidence of two witnesses. The learned High Court Judge acquitted the Accused by judgment dated 28th January 2011 (page 782 of the proceedings).

The grounds of appeal urged by the Honourable Attorney General are, reproduced verbatim, as follows:

1. "The learned High Court Judge had erroneously come to the finding that the Prosecution had failed to prove that the Accused had exclusive possession of the computer.
2. The learned High Court Judge had failed to consider the necessary inferences arising out of:
    a. the meeting of the accused and the decoy as pre-arranged over the telephone.
    b. the communication between the Accused and the decoy via emails, where the Accused refers to himself as Kamal.
    c. the communication between the Accused and the decoy via telephone, where the Accused provides a description of himself to the decoy.
    d. The conduct of the Accused upon meeting the decoy, whom the Accused claims to have never encountered before."

It must be kept in mind that a cardinal rule of a criminal trial is that the prosecution must prove the charges levelled against the Accused 'beyond reasonable doubt'. If this

standard is not met, a court of law cannot and must not convict, or affirm the conviction of, the Accused no matter how vile the crime alleged to have been committed. This standard, although originating in the adversarial system of criminal justice, is enshrined as a fundamental right in Article 13(5) of our Constitution as well. Recently, his Lordship Yasantha Kodagoda PC J. in Officer-in-Charge Special Crimes Division v. Mananage Sunil Dharmapala SC Appeal No. 155/14 decided on 28.06.2021, in an enlightening discussion of the principle observed:

"a 'reasonable doubt' means a doubt in respect of which a valid reason can be attributed. For a 'doubt' to be recognised as amounting to a 'reasonable doubt', the ground for the development of the doubt must be objective and reason based. There should be a **logical basis** for the entertaining of the doubt. That is the distinction between a 'mere doubt' and a 'reasonable doubt'." [emphasis added]

Bearing this in mind, we now venture into the task of determining whether the Prosecution has successfully met this threshold for conviction.

The contents of the photographs

Section 286A(1)(c) reads:

Any person who-

(i) takes, or assists in taking of **any indecent photograph of a child**; or
(ii) distributes or shows any such photograph or any publication containing **such photograph**;
(iii) has in his possession for distribution or showing, any **such photograph** or publication;
(iv) publishes or causes to be published, any **such photograph** or publishes or causes to be published, any advertisement capable of conveying the message that the advertiser or person named in the advertisement distributes or shows any **such photograph** or publication or intends to do so,

commits the offence of **obscene publication and exhibition relating to children** and shall on conviction be punished with imprisonment of either description for a term not less than two years and not exceeding ten years and may also be punished with fine. [emphasis added]

The fact in issue that must be proved, in addition to whether the photograph is "indecent" (which is not dealt with in this judgment as there appears to be no dispute on this aspect), in order for this Section to be applicable is whether the indecent photograph depicts a **child. A child means a person under the age of eighteen years.** (Section 286A (4)). If the pictures depicted were that of adults, this Section would be inapplicable.

As our jurisprudence has not dealt with the issue of proving or ascertaining the age of the person depicted in the indecent material it will be of use to assess the approach taken in foreign jurisdictions.

In the United Kingdom, the case of R v. Land [1998] 1 All ER 403, dealt with a conviction for possessing indecent photographs of a child contrary to Section 1(1)(C) of the Protection of Children Act 1978. There was no direct evidence about the identity or ages of any of the persons in the videos. The Appellant argued, on appeal, that expert paediatric evidence should have been called before the jury. The Court of Appeal, dismissing the appeal, observed that Section 2(3) of the Act which provides that for the purpose of the Act "a person is taken as having been a child at any material time if it appears from the evidence as a whole that he was then under the age of 16" underscores the "difficulty of making a positive identification of an unknown person depicted in a photograph" and therefore **the age of such person is a question of fact "based on inference without any need for formal proof**". The relevant portion of the judgment is worth quoting:

"The judge directed the jury that in deciding whether it was proved that the photographs were of a child:

'You can do no more than use your own experience, your judgment and your critical faculties in deciding this issue. It is simply an issue of fact for you, the jury, to decide what you have seen with your own eyes …'

In our judgment this direction is not open to question. In any event such expert evidence tendered by either side would be inadmissible. **The purpose of expert evidence is to assist the court with information which is outside the normal experience and knowledge of the judge or jury. Perhaps the only certainty which applies to the problem in this case is that each individual reaches puberty in his or her own time. For each the process is unique and the jury is as well placed as an expert to assess any argument addressed to the question whether the prosecution has established**, as it must before there can be a conviction, **that the person depicted in the photograph is under 16 years**." [emphasis added]

However, there is doubt whether the approach taken in this case is too broad-brush. For instance, in Griffiths (Procurator Fiscal, Perth) v. Neil Macdonald Hart [2005] HCJAC 51, Lord Osborne, who delivered the opinion of the High Court of Justiciary in Scotland, having cited the last paragraph quoted above observed:

"We must respectfully disagree with that view. In our opinion, while there may be cases in which proof of the essential facts in question may be achieved without reference to an expert witness or witnesses, in other kinds of case, where the subject of the image may be approaching

the age of 16, there may be very considerable difficulty for the fact-finding tribunal in that regard. In such cases, the evidence of one or more expert witnesses may well be necessary in practice to enable the Crown to prove that the subject of an image is under 16 years of age."

However, in a recent judgment of the High Court of Justiciary, John Leadbetter v. Her Majesty's Advocate [2020] HCJAC 51 it was held that "there was no need for "expert evidence, that is to say a skilled witness, to prove that a photograph depicts a child." It found:

"There may be cases on the margins in which little weight may be put on a person's testimony that a person was a child rather than an adult; a child being a person under 18 in this context (Civic Government (Scotland) Act 1982 ss 52(2) and 52A(4)). In such cases, the evidence of a paediatrician may be advisable, if other sources, such as a birth certificate or the person's parents or other relatives, are not available. That is not to say that an adult witness, with a normal degree of experience of life, cannot express a view on whether a person, whether shown in a photograph or otherwise, is a child, especially if the person is naked. This is consistent with Griffiths v Hart 2005 SCCR 392, Lord Osborne, delivering the opinion of the court at para [15] citing R v Land [1999] QB 65, Judge LJ at 70-71.

Once it is accepted, as it was in Griffiths, that the evidence of police officers was admissible to corroborate the evidence of a paediatric endocrinologist as to the age of girls shown in photographs, that evidence must be regarded as admissible as proof that the photographs depicted children.

Whether a person appears to be a child is not a matter which requires technical or scientific evidence. Identifying a person as a child is part of everyday life. It is something within common knowledge and experience. A person is entitled to give evidence of his or her impression of whether someone is a child and, if so, within what age range. In light of all the evidence, the fact finder then has to decide whether "it appears from the evidence as a whole" that the person was under eighteen (1982 Act s 52(2)). This would, in any event, be something which a sheriff or a jury could do themselves by looking at the images, were that the evidential course taken."

Despite this dictum, it must be noted that in Leadbetter's case the pictures were relatively straightforward, meaning that it was easily identifiable that the persons depicted were children since all the children were below 14 years of age. Further, Detective James McGoldrick had been trained in categorising indecent images of children: "he did have special training in identifying whether someone was a child. Despite what was said in submissions both to the sheriff and to this court, he said both in chief and especially in cross that his Home Office training included being able to identify someone as a child."

In the United States, jurisprudence is of mixed opinion. The position can be summarised in the following passage quoted from the judgment of the United States Court of Appeals for the Fifth Circuit in United States v. Katz 178 F.3d 368 (1999):

"The threshold question — whether the age of a model in a child pornography prosecution can be determined by a lay jury without the assistance of expert testimony — must be determined on a case by case basis. As the government correctly points out, it is sometimes possible for the fact finder to decide the issue of age in a child pornography case without hearing any expert testimony. *See United States v. O'Malley,* 854 F.2d 1085 (8th Cir.1988) …. However, in other cases, the parties have been allowed to present conflicting expert testimony. *See United States v. Anderton,* 136 F.3d 747, 750 (11th Cir.1998) … In yet other cases, one party presents expert testimony, while the other does not. *See United States v. Broyles,* 37 F.3d 1314, 1316 (8th Cir.1994)(Government presented the expert testimony of a paediatric endocrinologist and Broyles presented no evidence.) A case by case analysis will encounter some images in which the models are prepubescent children who are so obviously less than 18 years old that expert testimony is not necessary or helpful to the fact finder. On the other hand, some cases will be based on images of models of sufficient maturity that there is no need for expert testimony. However, in this case, in which the government must prove that a model, who is post-puberty but appears quite young, is less than eighteen years old, expert testimony may well be necessary to "assist the trier of fact to understand the evidence or to determine a fact in issue." Fed.R.Evid. 702."

Citing this passage with approval, the Superior Court of Pennsylvania in Commonwealth v. Robertson- Dewar 829 A.2d 1207 (2003) observed the flexibility inherent in the law was due to the following concern:

"Given the anonymity of the internet, the identity of children depicted and their whereabouts are frequently unknown. Thus, conventional means of proving age such as birth certificates or testimony of a relative are usually unavailable. To require law enforcement officials to track down and identify the children depicted in order to successfully prosecute a child pornography case would rip the teeth out of the child pornography statute and destroy its efficacy as a preventive measure in the sexual exploitation of children. Therefore, the legislature has vested the trier of fact with the function of determining the age of the child depicted and further allows for this element to be sufficiently established through competent expert testimony in close cases."

There is academic scepticism about the correctness of the approach taken in Land as well. Alisdair A. Gillespie in an article titled 'Child pornography' (an article in 'Information & Communications Technology Law', October 2017) notes that it appears

"strange that expert evidence is not required". This is considering the severity of the punishment an accused must face if convicted. Further:

"There does appear some evidence that lay persons are as good at identifying the age of children as experts, although that was one study and did not involve the use of real children as subjects. However, research suggests identifying age is complicated."

He reconciles that the rejection of expert evidence might be "the law's way of ensuring that the image is looked at through a lay-person's eyes and not the gaze of those who are looking for evidence of childhood."

Jonathan Clough in 'Lawful Acts, Unlawful Images: The Problematic Definition of 'Child' Pornography' ((2012) 38(3) Monash University Law Review 212 at 231) commenting on Land notes:

"This decision was made at a time when the relevant age in England and Wales was under 16. Whatever merit there may have been at that time, it may be doubted whether one could state, with the confidence necessary in the context of a penal provision, that a 'glance will quickly show' whether the person depicted is under 18. Ascertaining the age of a person from a visual image is notoriously unreliable. Apart from the variability in rates of sexual maturation due to biological, personal and environmental factors, viewing an image in two dimensions does not allow for a full inspection of features."

The literature available on estimating or ascertaining the age of a child or whether in fact a person depicted is a child amply demonstrates that it is not a straightforward question. The methodology used to make such an estimation, when the person depicted is not known, needs to be addressed if cases of this type are to be successfully prosecuted. Therefore, we will not attempt to generalise the method that has to be adopted in cases of this nature, and instead leave it to be decided on the facts and circumstances of each case. However, we must note that with the advent of technology newer issues such as whether the images have been morphed or are depicting 'real children', which as per the literature, can be done so seamlessly, that it may appear that the task of ascertaining or estimating the age of the child depicted becomes more arduous. Whether our legislation can capture within its fold the new advancements in technology will have to be seen as well. Therefore, in reaching that right balance between the prosecution of such crimes and ensuring a fair trial for the Accused, this Court must be cautious not to set the standard too high or too low.

Yet, what is evident in the cases discussed above and, in the literature, available is the fact that the majority favours a cautious approach when ascertaining or estimating the age of the person depicted in the photographs. In grey areas, for instance where the image is of a pubescent child or where there is an allegation that the image is not of a real child, expert evidence, such as that of gynaecologists, paediatricians have proved beneficial. It would be prudent to exercise caution and subject the photographs to forensic analysis or the opinion of medical professionals even when the images are straightforward. This is important not only because of the severe penalties the Accused would face, if convicted, but, also because in our law it is possession of child pornography that is illegal. There is no general prohibition on the possession of adult pornography for personal gratification, subject to certain exceptions such as non-consensual adult pornography. That distinction then becomes important.

We must then see whether this level of minimal caution has been exercised by the relevant prosecuting authorities in the present case. It appears that this factor has been neglected in the judgment of the learned High Court Judge. There were statements of witnesses made that the images they saw were of underage male children. It appears inconclusive whether they depicted children: For instance, PW1 when referring to the pictures in the emails says on the one hand that it depicted "බාලවයස්කාර පිරිමි දරුවන්" (page 47 of the Brief – proceedings dated 2nd October 2007) and, on the other hand, "බාලවයස්කාර **දරුවන්ගේ පෙනීම තිබෙන අයගේ** නිරුවත් සහ අශ්ශීල ඡායාරූපයක්" (page 72 of the Brief – proceedings dated 9th January 2008). Referring to one particular image PW1 remarks "මෙහි ඉහලින් තිබෙන ඡායාරූපයෙන් ළමයින් සහ තරුණ වයසේ පසුවන පිරිමි දෙදෙනෙක් බව මට පේනවා" (page 115 of the Brief – proceedings dated 21st February 2008).

However, in the absence of any proof that the photographs were in fact of persons below 18 years of age such as a Forensic Report or any expert opinion this fundamental condition has not been made out. The Prosecution has also failed to establish the competence or level of experience of the relevant witnesses in their ability to ascertain or estimate the age of the children depicted in such photographs.

It must be reiterated that although we do not intend to stifle child pornography prosecutions, as the relevant Section makes it applicable only to material involving "children" specifically, the Prosecution must satisfy that the photograph did in fact depict

"children". Additionally, given the consequences involved if found guilty of this offence it is prudent to err on the side of caution. Equally important is that it must be "obscene".

The authenticity of the emails – were they authored by the Accused?

The next pressing issue is whether the Prosecution successfully proved that the emails were authored by the Accused himself. The emails emanated from the address 'kevinw@37.com'. This was denied by the Accused, who claimed in his dock statement that he operated/owned only one email address, which was an official email address 'wimal@klm.ac.lk', and that he neither created nor operated the 'kevinw@37.com' email address.

The evidence of the witnesses demonstrates how easy it would be to create an email address. This is a commonly known fact as well. For instance, this is clearly borne out in the evidence of PW9 on page 335 of the Brief (proceedings dated 6th October 2008):

"ප්‍ර : ඒ වගේම සාක්ෂිකාරිය තමන්ට අදටත් කියන්න බැහැ තමන් මේ ඉදිරිපත් කරපු E -Mail පණිවිඩ භෞතික

වශයෙන් කවිද එව්වේ කියලා?

උ : එහෙමයි.

ප්‍ර : එක තමයි තත්ත්වය?

උ : එහෙමයි.

ප්‍ර : තමන් නමින් චන්දිමා නමින් 1,2,3 වශයෙන් ලිපිනයන් යොදාගෙන E-mail පණිවිඩ ලබා ගන්න ලිපිනයක්

හදාගන්න ඕන කෙනෙකුට පුළුවන්?

උ : එහෙමයි.

ප්‍ර : මේකෙන් කියන්නේ නැහැ ඔහු විසින් එවන ලද E-mail පණිවිඩයක අයිතිකරු ඔහු කියලා?

උ : නැහැ."

The Prosecution has not made use of the provisions found in Section 201 of the Criminal Procedure Code. There was no rebuttal. There is nothing to connect the Accused as the sender of the vulgar emails, apart from mere inferences that the Honourable Attorney General has laid out in the afore-quoted second ground of appeal. Firstly, we do not see the relevance of such inferences to the charge (which deals with sending child pornography through email, and possession of child pornography in the Accused's computer). Secondly, the inferences are weak. It is indisputable that they met, but this

Court finds that the meeting alone is insufficient to prove that the Accused sent the emails. We are also mindful that the evidence of interested witnesses such as PW1 (the decoy) must be analysed cautiously.

There is a failure to establish that the Accused is the author of the initial post on the lewd website, and the subsequent email correspondences.

Authentication of emails, and determining their source is not a straightforward task. As Samuel A. Thumma and Darrel S. Jackson commented in 'The History of Electronic Mail in litigation' 16 Santa Clara High Tech. L.J.1 (2000):

"Not surprisingly, attorneys have discovered that e-mail messages can be particularly relevant and instructive evidence in litigation, and can be a gold mine, or a nightmare, depending upon the party an attorney represents."

We are compelled to look to foreign jurisdictions to glean some guidance on the issue of authenticating the identity of the person sending the email, as our law is yet to address it.

In the United States, in the case of State of Idaho v. Michael Eugene Koch 157 Idaho 89, 334 P.3d 280 (2014) the Supreme Court of the State of Idaho discussed several methods in which email evidence may be authenticated. It observed:

"Other jurisdictions have recognized that electronic evidence may be authenticated in a number of different ways consistent with Federal Rule 901 and corresponding state statutes. Courts have not required proponents offering printouts of emails, internet chat room dialogues, and cellular phone text messages to authenticate them with direct evidence, such as an admission by the author or the testimony of a witness who saw the purported author typing the message. See, e.g., United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012). Rather, courts have held that circumstantial evidence establishing that the evidence was what the proponent claimed it to be was sufficient. See, e.g., State v. Thompson, 777 N.W.2d 617, 624 (N.D. 2010) (providing a comprehensive review of other jurisdictions' authenticity requirements for electronic communications). Circumstantial proof might include the email address, cell phone number, or screen name connected with the message; the content of the messages, facts included within the text, or style of writing; and metadata such as the document's size, last modification date, or the computer IP address. See Fluker, 698 F.3d at 999; United States v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000); United States v. Safavian, 435 F. Supp. 2d 36, 40–41 (D.D.C. 2006).

In support of his argument that eyewitness testimony is necessary to authenticate a text message when the defendant does not admit to sending it, Koch points to the Nevada Supreme Court decision, Rodriguez v. State, 273 P.3d 845, 849 (Nev. 2012) ……. The court required actual

proof of the defendant sending the text message because there was direct evidence that the text messages were sent while the phone was in the possession of multiple people other than the phone's actual owner. Rodriguez does not stand for the proposition that eyewitness testimony of who sent a text is required for its authentication, but rather that where evidence establishes that a phone is in multiple people's possession at the time incriminating messages are sent, a higher level of proof that the defendant sent the incriminating messages is required."

In India, the High Court of Calcutta in Abdul Rahaman Kunji v. The State of West Bengal (2014) held:

"It is true that merely sending e-mail from a particular e-mail address would not lead to a presumption that the particular e-mail was sent by the originator, i.e., the person from whose e-mail address a mail emanates. Hacking is not an unknown phenomenon in the world of electronic records. Therefore, the salutary provision in law is that the presumption relating to the genuineness of an electronic message is rebuttable and the Court cannot presume that the message has been sent by a particular person."

A word of caution of the learned Judges of the Calcutta High Court worth reiterating is:

"Today, closed circuit television cameras are being installed in most areas where computers are accessible or where it is possible to use one's own devices which access Wi-Fi connections, or mobile networks, e.g., personal computers, mobile phones, tablet computers etc. The evidence obtained from such video recordings could be used to corroborate the identity of the originator of the electronic communications who sends such communications especially from a closed area. This would make it easier for the investigating officers in future to unearth the truth in crimes involving electronic messaging and communications with more certainty. It is necessary for the investigation agencies to keep pace with the technological advances in the world of electronics and to prove their case in accordance with the Evidence Act by making the best use of such technologies."

Laird Kirkpatrick in an article titled '§ 9:9 Authenticating Email, Social Media, Web Pages, Text Messages, Instant Messaging, Electronic Signatures' (December 18, 2014) 5 Federal Evidence 9:9 (4th ed. Thomson/Reuters 2013); GWU Law School Public Law Research Paper No. 2014-60; GWU Legal Studies Research Paper No. 2014-60 notes:

"**Certainly testimony by a person who saw the purported author write and send such material would suffice**. If the computer, or for that matter the cell phone or "android" from which such material was sent is owned by a particular person, was **seized from that person's possession, or there are other compelling circumstances linking the computer to that person, such facts may**

be enough to authenticate the material as having come from that person. If it is a shared computer, or one to which others had access, additional evidence linking the purported author to the email seems essential. For example, proof that the person in question was the one using the computer when the message was sent should suffice to connect the message to that person. Particularly in criminal cases where establishing authorship, and where a jury may have to be persuaded beyond a reasonable doubt that the defendant was the author in order to convict him, prosecutors sometimes call technical witnesses who do a trace. For emails, an expert may rely on the coded Internet Protocol Address appearing in the email header and trace it back to the service provider who relayed the message and sometimes back to a particular computer."

We recognise that this offence took place in 2002 and that sophisticated techniques for proving authorship of emails may not have been as advanced as in today's day and age. We are reminded of the words of Lord Denning in Roe v. Minister of Health [1954] 2 QB 66 "We must not look at the 1947 accident with 1954 spectacles."

Nevertheless, the distinguishing factor in the instant case is the inability to unmask that it was the Accused who posted the advertisement and authored those distasteful correspondences. This only becomes more difficult to prove when considering the next part of the judgment.

I would wish to draw a parallel to the defence of an alibi. The Accused's emphatic rejection that he did not create, own or operate the particular email address, through which he corresponded with "Shane", is similar to the defence of an alibi, in which the Accused would deny ever being at the scene of the crime. The burden of proof would be on the Prosecution to prove that he did in fact author those emails.

Possession of indecent photographs of Children

It must be noted that the computer which contained the illicit pictures was the one found in the cubicle of the Accused's office. The question that then arises is whether the Accused had exclusive access or possession of the computer in his cubicle or whether his colleagues, four others as per the evidence, had access to it as well. This question could have been more conveniently dealt with had it been his personal computer.

According to the evidence elicited by PW1 before he and the Accused entered the Accused's office, the officers that participated in the sting operation with him inspected the computer, not in the presence of the Accused. Meaning that they were able to access

the computer without any difficulty such as having to enter a password. The fact that the computer did not have password protection is borne out in the evidence of other witnesses as well. For instance, PW2 (Dimuthu Prasad Galappaththi of the NCPA) who was at the scene when the computer was inspected answered as follows (Page 211 of the Brief – proceedings dated 1st July 2008):

"ප්‍ර : කවුද පරිගණකය ක්‍රියාත්මක කළේ ?

උ : චන්න මහත්මයා. මම එතන හිටියා පමණයි.

ප්‍ර : ඒ මහත්මයා පරිගණකය ක්‍රියාත්මක කළේ මොනවා හරි දත්ත පරිගණකයට යොදලාද?

උ : නැහැ. නිකන්ම ඔන් කළා . ඊට පසු මුල් පිටුව වැටුනා.

ප්‍ර : පරිගණක වැඩසටහනකට යන්න අවශ්‍ය ප්‍රධානම පිටුවට ප්‍රශ්නයක් නැතිව ඔහු අවතීර්ණ වුනා?

උ : එහෙමයි.

ප්‍ර : දැන්, අවතීර්ණ වී තමයි තමන් කියන හැටියට පරිගණකයේ තියෙනවා කිව්වා ඡායාරූප බැලුවේ?

උ : එහෙමයි.

ප්‍ර : දැන්, ඊට පසු තමන් පරිගණකයේ ප්‍රධාන යන්ත්‍රය මුද්‍රා තැබුවා කියලා?

උ : එහෙමයි."

This is corroborated by the evidence of PW5 (Channa Nishantha Soysa of the NCPA):

"ප්‍ර : තමාලා එම ස්ථානයට ගොස් මොනවද කළේ ?

උ : මෙම විත්තිකරුගේ පරිගණකය පරීක්ෂා කළා.

ප්‍ර : තමා පරිගණකය පරීක්ෂා කිරීමට සහභාගී වුනාද?

උ : ඔව්.

ප්‍ර : තමා කොහොමද පරිගණකය ක්‍රියාත්මක කළේ ?

උ : ස්ටාට් බවින් එක ප්‍රේෂ් කරලා වර්ඩ් එකක් තෝරාගෙන පරිගණකය ක්‍රියාත්මක කළා. ඉන්පසුව ජානාන්තර

සබඳතා ලබා ගැනීම සඳහා පෝමැටි තුනක් තිබෙනවා. එම පෝමැටි තුන ජේඩීජී, බී එම්පී, ජීඅයිඑ කියා

කියන්නේ."

(Page 261 of the Brief – proceedings dated 3rd September 2008)

"ප්‍ර : ඔය කාර්යාලයට තමා ගිහින් කළා කිව්වේ පරිගණකයට අයිති රහස් අංකයක් යෙදුවේ නෑ , කෙලින්ම

පරිගණකය ක්‍රියාත්මක කළා කියා?

උ : ඔව්."

(Page 270 of the Brief – proceedings dated 3rd September 2008)

Therefore, the pornographic content found on the computer, a computer that was openly accessible by anyone including the Accused, and one which was not password protected creates doubt about whether it was he in fact who had downloaded and stored the indecent photographs.

In the notable case of Don Sunny v. Attorney General (Amarapala Murder Case) [1998] 2 SLR 1 it was famously held:

"The prosecution must prove that no one else other than the accused had the opportunity of committing the offence."

When we peruse the judgment, the learned High Court Judge has correctly identified these related issues. The following excerpts duly illustrate the same:

"එම කාර්යාලයට දැන් යතුරක් තිබෙන බවත්, ඒ කාලයේ යතුරක් තිබුනාද කියා ඔහු පවසා නැත. මෙම අධ්‍යන පීටයේ ඉරිදා දිනවල පාටමාලා 30ක් පමණ පවත්වන ලද අතර, 2002.08.11 වන දින පාටමාලා 25 ක් පැවැතු බවත් මෙම සාක්ෂිකරු කියා සිටින ලදී. මෙම සාක්ෂිකරුගේ සහ විත්තිකරුගේ කාර්යාලයන් එකම කාර්යාලය දෙකට වෙන්කර තිබු බවත්, මෙම කාර්යාලයේ වෙනත් ලිපිකාර සේවකයින් සිටි බවත්, ඔවුන් ඉරිදා දිනද වැඩ කරන බවත් කියා සිටින ලදී.

ප්‍ර : මේ කාර්යාලයේ වෙනත් නිලධාරීන් සිටියාද?

උ : ක්ලරිකල් ස්ටාෆ් එක අපිට ඉදිරිපසින් සිටියා.

ප්‍ර : ඒ ය ඉරිදා වැඩ කරනවද?

උ : ඉරිදා වැඩ කරනවා ඕ.ටී කරනවා.

මේ අනුව මෙම සාක්ෂිකරුගේ සාක්ෂියෙන් විත්තිකරු සිටි කාර්යාලයේ නවත් ලිපිකරුවන්ද සේවය කල බවත්, මොවුන් අතීතකාල සේවයේ ඉරිදා දිනවල යෙදෙන බවත් පෙනී යයි."

(Page 11-12 of the judgment- Page 793 of the Brief)

"සාමාන්‍ය යෙන් සෑම පරිගණකයකම වගේ පාස්වර්ඩ් එකක් තිබෙන බවත්, මෙම පරිගණකයකට පාස්වර්ඩ් එකක් තිබුනාද කියා නොදන්නා බවත් මෙම සාක්ෂිකරු පිළිගන්නා ලදී. මෙම චුදිත සිටි අංශයේ සිටි සියලුම නිලධාරීන්ට පරිගණක නොතිබුණු බවත්, එහි 4 දෙනෙකු සිටි අතර, පරිගණක 3 ක් පමණ තිබු බවත් මෙම සාක්ෂිකරු හරස් ප්‍රශ්නවලදී පිළිගන්නා ලදී."

(Page 13 of the judgment – Page 795 of the Brief)

"මේ සාක්ෂිය අනුව මෙම නිලධාරීන් චුදිත නොමැතිව එම පරිගණකය ක්‍රියාත්මක කර ඇති අතර, පරිගණකයට පාස්වර්ඩ් එකක් තිබුනා නම් ඔවුන්ට චුදිත නොමැතිව එය ක්‍රියාත්මක කිරීමට නොහැකි වනු ඇත."

(Page 16 of the judgment – Page 798 of the Brief)

Therefore, we find no reason to interfere with the judgment of the learned High Court Judge.

Before we conclude there is one observation that must be made. To do so, the words of his Lordship Colin-Thome J. in Benwell v. Republic of Sri Lanka [1978-79] 2 SLR 194 is a good starting point:

"Computer evidence is in a category of its own. It is neither original evidence nor derivative evidence and in admitting such a document a Court must be satisfied that the document has not been tampered with. Under the law of Sri Lanka computer evidence is not admissible under any section of the Evidence Ordinance and certainly not under section 34. One has, therefore, to look to the law of England which can be brought in under section 100 of the Evidence Ordinance.

In England under the Civil Evidence Act, 1968, computer evidence has been made admissible only in civil cases and that too under the most stringent conditions as set out in section 5 of the Act..... In any event such evidence is not admissible in English Law in criminal cases. Such evidence is clearly inadmissible under any provisions of the Evidence Ordinance of Sri Lanka."

To address this lacuna, the Legislature introduced the Evidence (Special Provisions) Act No. 14 of 1995, after a period of about fifteen years, to permit computer evidence in civil and criminal cases. It appears in the Journal Entries of the High Court record (15th August 2007) that the Prosecution has given notice, as required under Section 7 of the Act, at the request of the Accused, at the High Court. However, we observe that at various stages when productions were introduced such as printouts of the email correspondences and the relevant tape recordings of the telephone conversations, those were admitted "subject to proof". If the provisions of the Section 7 notice had been complied with we are unsure why such evidence was admitted subject to proof.

We would advise, therefore, if the Honourable Attorney General seeks to rely on computer evidence, it would be efficacious and strengthen the purpose for introducing the Evidence (Special Provisions) Act for Section 7 notice to be issued and for the inspection of the computer evidence to take place prior to serving the indictment, at the Magistrate's Court.

The appeal is dismissed without costs.

JUDGE OF THE COURT OF APPEAL

D. N. SAMARAKOON, J.

I AGREE

JUDGE OF THE COURT OF APPEAL