# SUPREME COURT OF QUEENSLAND

| | |
|---|---|
| CITATION: | *R v Tahiraj* [2014] QCA 353 |
| PARTIES: | **R**<br>**v**<br>**TAHIRAJ, Luan**<br>(appellant/applicant) |
| FILE NO/S: | CA No 175 of 2013<br>CA No 212 of 2013<br>SC No 253 of 2013 |
| DIVISION: | Court of Appeal |
| PROCEEDING: | Appeal against Conviction & Sentence |
| ORIGINATING COURT: | Supreme Court at Brisbane |
| DELIVERED ON: | 19 December 2014 |
| DELIVERED AT: | Brisbane |
| HEARING DATE: | 2 September 2014 |
| JUDGES: | Margaret McMurdo P and Fraser JA and Alan Wilson J<br>Separate reasons for judgment of each member of the Court, each concurring as to the orders made |

ORDERS:

**1. The appeal against conviction is dismissed.**

**2. Grant the application for leave to appeal.**

**3. Allow the appeal against sentence in respect of counts 1, 2, 3 and 6.**

**4. Set aside the sentences imposed below on counts 1, 2, 3 and 6 and instead order that:**

**(i) on each of counts 1 and 2 the appellant is imprisoned for three years to commence on 20 August 2013;**

**(ii) on count 3 the appellant is imprisoned for three years to commence at the end of the sentences for counts 1 and 2; and**

**(iii) on count 6 the appellant is imprisoned for two years to commence at the end of the sentence for count 3.**

**5. The declaration that the presentence custody be time already served under the sentences imposed for counts 6, 4, 5 and 7 is vacated.**

**6. Instead it is declared that pursuant to s 159A *Penalties and Sentences Act* 1992 (Qld) the appellant**

**was held in presentence custody for 71 days between 8 April 2009 and 9 April 2009, and 12 June 2013 and 20 August 2013. This Court declares the whole of those terms are imprisonment already served under the sentences imposed for counts 1, 2, 4, 5 and 7.**

**7. In respect of all other counts a non-parole period of four years is fixed.**

**8. The Court directs that an explanation of the purpose and consequences of fixing that non-parole period be handed to the appellant in writing forthwith and a copy thereof marked "Explanation" for identification.**

**9. The sentence imposed below is otherwise confirmed.**

CATCHWORDS: CRIMINAL LAW – PROCEDURE – INFORMATION, INDICTMENT OR PRESENTMENT – JOINDER – OF COUNTS – BY STATUTE – SAME FACTS OR SERIES OF OFFENCES OF SAME OR SIMILAR CHARACTER – where the appellant was convicted after trial of two counts of using a carriage service to procure a person under 16 (counts 1 and 6); unauthorised access to a computer with intent (count 2); using a carriage service to make child pornography material available (count 3); using a carriage service to access child pornography material (count 4); using a carriage service to access child abuse material (count 5); and knowingly possessing child exploitation material (count 7) – where the appellant befriended a 13 year old girl (A) on the website "Vampire Freaks" – where A and the appellant communicated via MSN Messenger – where the appellant sent A a program over MSN Messenger which A attempted to download – where the appellant used this program to access and turn on A's webcam remotely – where the appellant told A to strip on webcam – where the appellant told A that he would destroy her computer and hack her online accounts if she did not comply – where the appellant instructed A to masturbate on webcam and write something on her breasts – where the appellant posted a video of the incident on the internet (counts 1 to 3) – where the appellant befriended a different girl (B) on the website "Vampire Freaks" – where B was 14 years old – where the appellant said things to B including "fuck me" and "do you want to meet up for sex?" (count 6) – where the Australian Federal Police (AFP) executed a search warrant on the appellant's residence – where the AFP found 181 images of child pornography, child abuse and child exploitation material on the appellant's computer and hard-drives (counts 4, 5 and 7) – where the appellant denied all seven offences – where the appellant claimed his computer was hacked and he was set up by a person or persons unknown in an act of revenge – where the appellant's trial counsel did not apply to have the seven counts severed – where counsel for the appellant on appeal contend

that the joinder of counts 1, 2 and 3 with counts 4, 5 and 7 was contrary to s 567 *Criminal Code* 1899 (Qld) and resulted in a substantial miscarriage of justice – where the appellant also contends that the joinder of counts 4, 5 and 7 with count 6 was contrary to s 567 *Criminal Code* and resulted in a substantial miscarriage of justice – where the appellant also contends that counts 1, 2 and 3 should have been severed from count 6 and a failure to do so resulted in a substantial miscarriage of justice – where the respondent contends that the appellant's decision not to apply for separate trials was a forensic and tactical one, in order to give weight to the defence case that the appellant was hacked – whether the counts were wrongly joined – whether the wrongful joinder amounted to a miscarriage of justice – whether the conviction should be set aside

CRIMINAL LAW – APPEAL AND NEW TRIAL – OBJECTIONS OR POINTS NOT RAISED IN COURT BELOW – MISDIRECTION AND NON-DIRECTION – GENERAL PRINCIPLES – where the evidence admissible to establish counts 1, 2 and 3 was not probative of guilt on counts 4, 5, 6 and 7 – where the trial judge directed the jury to consider each charge separately – where the appellant contends that the trial judge's directions did not sufficiently explain to the jury what evidence was admissible on each count – where the appellant contends that this resulted in a substantial miscarriage of justice – where there was no request for redirections at trial – whether the failure of the trial judge to give a propensity warning amounted to a miscarriage of justice – whether the conviction should be set aside

CRIMINAL LAW – APPEAL AND NEW TRIAL – OBJECTIONS OR POINTS NOT RAISED IN COURT BELOW – MISDIRECTION AND NON-DIRECTION – GENERAL PRINCIPLES – where the trial judge directed the jury to the areas of conflict between the expert witnesses – where the appellant contends that the trial judge did not direct the jury as to how to deal with those areas of conflict as set out in Bench Book Direction 55.1 – where the appellant contends that this resulted in a substantial miscarriage of justice – where there was no request for redirections at trial – whether the failure of the trial judge to give the direction amounted to a miscarriage of justice – whether the conviction should be set aside

CRIMINAL LAW – APPEAL AND NEW TRIAL – APPEAL AGAINST SENTENCE – GROUNDS FOR INTERFERENCE – SENTENCE MANIFESTLY EXCESSIVE OR INADEQUATE – where the appellant was sentenced to an effective term of 12 years imprisonment – where the trial judge considered count 6 to be the most serious offence – where the appellant was sentenced to two periods of cumulative imprisonment – whether the sentence was manifestly excessive

*Criminal Code* 1899 (Qld), s 210(1)(b), s 228D, s 567, s 597A, s 644, s 668E(1)

*Criminal Code* 1995 (Cth), s 474.19(1)(a)(i), s 474.19(1)(a)(iv), s 474.22(1)(a)(i), s 474.26(1), s 477.1(1)
*Evidence Act* 1977 (Qld), s 21A, s 93A
*Penalties and Sentences Act* 1992 (Qld), s 159A

*Barbaro v The Queen* (2014) 88 ALJR 372; [2014] HCA 2, cited
*BRS v The Queen* (1997) 191 CLR 275; [1997] HCA 47, cited
*De Jesus v The Queen* (1986) 61 ALJR 1; (1986) 68 ALR 1; [1986] HCA 65, cited
*KRM v The Queen* (2001) 206 CLR 221; [2001] HCA 11, cited
*Mill v The Queen* (1988) 166 CLR 59; [1988] HCA 70, applied
*Patel v The Queen* (2012) 247 CLR 531; [2012] HCA 29, cited
*R v Asplund* (2010) 216 A Crim R 48; [2010] NSWCCA 316, cited
*R v BBG* (2007) 174 A Crim R 86; [2007] QCA 275, cited
*R v Robinson* [2010] QCA 377, cited
*Tector v The Queen* (2008) 186 A Crim R 133; [2008] NSWCCA 151, cited
*Velevski v The Queen* (2002) 76 ALJR 402; [2002] HCA 4, cited

COUNSEL: P J Davis QC, with J R Jones, for the appellant/applicant
M J Copley QC for the respondent

SOLICITORS: Potts Lawyers for the appellant/applicant
Director of Public Prosecutions (Commonwealth) for the respondent

[1] **MARGARET McMURDO P:** The appellant, Luan Tahiraj, was convicted on 12 June 2013 after a three and a half week trial of using a carriage service to procure a person under 16 years of age contrary to s 474.26(1) *Criminal Code Act* 1995 (Cth) (counts 1 and 6); unauthorised access to a computer with intent contrary to s 477.1(1) *Criminal Code* (Cth) (count 2); using a carriage service to make child pornography material available contrary to s 474.19(1)(a)(iv) *Criminal Code* (Cth) (count 3); using a carriage service to access child pornography material contrary to s 474.19(1)(a)(i) *Criminal Code* (Cth) (count 4); using a carriage service to access child abuse material contrary to s 474.22(1)(a)(i) *Criminal Code* (Cth) (count 5); and knowingly possessing child exploitation material contrary to s 228D *Criminal Code Act* 1899 (Qld) (count 7). Each offence was alleged to have occurred between 10 November 2008 and 8 April 2009.

[2] Through a series of cumulative sentences the appellant was sentenced to an effective term of 12 years imprisonment.[1] On count 6, which the trial judge considered the most serious offence, he was sentenced to five years and four months imprisonment. On each of counts 1 and 2, he was sentenced to three years and four months imprisonment to be served concurrently with each other, but cumulatively upon the sentence for count 6. On count 3 he was sentenced to three years and four months imprisonment, cumulative upon the sentences on counts 1, 2 and 6. On the remaining counts he was sentenced to lesser concurrent terms of imprisonment. The judge ordered a non-parole period of six years imprisonment and declared a period of 71 days presentence custody as time already served under the sentences.

---

1 Sentencing remarks, 10 lines 30-40.

[3] The appellant has appealed against his convictions and applied for leave to appeal against his sentence, ultimately on the following grounds:

> "Ground 1: The joinder of counts 1, 2 and 3 with counts 4, 5 and 7 was not authorised and contrary to s 567 of the *Criminal Code* (Qld) and resulted in a substantial miscarriage of justice.[2]
>
> Ground 3: The joinder of counts 4, 5 and 7 with count 6 was not authorised and contrary to s 567 of the *Criminal Code* (Qld) and resulted in a substantial miscarriage of justice.
>
> Ground 4: Counts 1, 2 and 3 should have been severed from count 6. The failure to do so resulted in a substantial miscarriage of justice.
>
> Ground 5: The learned trial judge's failure to give a clear and detailed direction regarding the use to be made of the evidence in relation to each count caused a substantial miscarriage of justice.
>
> Ground 6: The learned trial judge's failure to give a clear and detailed direction regarding the expert evidence presented during the trial caused a substantial miscarriage of justice.
>
> Ground 7: The learned trial judge's directions were of no assistance to the jury and caused a substantial miscarriage of justice."

[4] The proposed ground of appeal in the application for leave to appeal against sentence was that the sentences were manifestly excessive.

[5] Before discussing these grounds of appeal it is necessary to first understand the evidence at trial.

**The prosecution case**

*Particulars*

[6] The prosecution case was particularised as follows.[3]

[7] The appellant, using the profile name 'Tick Tock', "used the carriage service TPG/Soul to procure [the 13 year old A] … to engage in or submit to sexual activity with himself." The procurement was as depicted in a video file titled kkkk.avi.[4] (count 1)

[8] The appellant used the same carriage service "to cause an authorised access of data, to or from [A's] computer … by way of malware, including a remote administration tool named Poison Ivy with the intention of committing an offence, namely, an offence against s 474.26(1) of the *Criminal Code* (Commonwealth)." (count 2)

[9] The appellant used the same carriage service "to make child pornography material available via the file sharing website Rapidshare, namely a video file titled kkkk.avi". (count 3)

---

2 The appellant abandoned ground 2 at the hearing of the appeal. T 1-6 - T 1-7.

3 Marked for identification, ex K, document no T143, as amended by marked for identification, ex O.

4 Exhibit P3.

[10] The appellant used the same carriage service "to access a quantity of child pornography material, (124 images, 1 video, 7 partial videos). 3 image files were located on [the appellant's] Verbatim USB Hard Disc drive as well as 10 unique image files (15 images in total) of child exploitation material located on the [appellant's] Toshiba Satellite Laptop". (count 4)

[11] The appellant used the same carriage service "to access a quantity of child abuse material ... namely six (6) images including:

(i) an "anime" style image depicting children with electrodes on their genitals; and

(ii) two images of a female child 8 to 12 years of age, tied up with ropes, one involving an act of bestiality with a dog;

(iii) an image collage of 12 images depicting a female child, approximately 8 to 12 years of age, tied up with ropes, performing oral sex on an adult male appearing to have semen in her mouth and involved with acts of bestiality with a dog;

(iv) a young female bound and gagged and strung up from the ceiling whilst a male ejaculates on her; and

(v) a semi-naked young Asian female bound and gagged on a bed." (count 5)

[12] The appellant using the internet account teamloosh@gmail.com and the profile name 'hai2u', used the same carriage service "to procure [the 14 year old B] … who was using the internet account random1much@hotmail.co.uk and the profile name 'PurpleRubberDucky', to engage in or submit to sexual activity, including sexual intercourse with himself. The [appellant and B], using their respective profiles and internet accounts, engaged in MSN instant messenger chats on 20 March 2009, 21 March 2009, 28 March 2009, 31 March 2009 and 1 April 2009. During these chats the [appellant] asks to see [B] naked on webcam and indicates that he want to engage in sexual activity with her". (count 6)

[13] None of the images in counts 5 and 6 were of A (with whom counts 1, 2 and 3 was concerned) or B (with whom count 6 was concerned).

[14] The sole Queensland offence, count 7, was particularised as the appellant knowingly possessing child exploitation material consisting of:

"a. 52 unique image files of child exploitation material … found on the [appellant's] Verbatim USB Hard Disc Drive and

b. 12 unique images (22 images in total) of child exploitation material … located on the [appellant's] Toshiba Satellite laptop computer."

*Admissions*

[15] The appellant made admissions[5] including that between 11 May 2007 and 9 April 2009, *TPG Internet* provided him with internet access; his date of birth, address, phone number, email addresses (teamloosh@gmail.com, sofijatajiraj@optusnet.com.au); and

---

5 Under s 644 *Criminal Code* (Qld).

that "rawful" was nominated as the account name during registration.[6] He also admitted the type of account, his IP address and that the date of registration was 11 May 2007. He used the email account "teamloosh@gmail.com" and the IP address "203.213.69.29".

[16] On 8 April 2009 Australian Federal Police (AFP) officers executed a search warrant on the appellant's residential address at North Lakes. They seized his Toshiba Satellite laptop including Hard Disk Drive, Verbatim USB Hard Disk Drive, and Seagate Hard Disk Drive.[7] The data was later examined by the AFP forensic team including Calvin Wills, Mark Whittley and Alex Tilley.

[17] On 8 April 2009 a Samsung 2.5 inch hard drive was removed from A's computer and allocated an identifying PSN number. The data contained in it was subsequently examined by the AFP forensic team including Messrs Wills, Whittley and Tilley. His IP address was used to access the child pornography material relevant to count 4 and child abuse material relevant to count 5.

[18] With reference to count 7, 52 unique image files of child exploitation material were found on his Verbatim USB Hard Disk Drive; 12 unique images (22 images in total) of child exploitation material were located on his Toshiba Satellite laptop computer; and 16 of those 22 images were retrieved from deleted files on the Toshiba hard disk drive.

*A's evidence*

[19] Although A was 13 at the time of the charged offences, she was 14 by the time her evidence by way of an interview with police under s 93A *Evidence Act* 1977 (Qld) was recorded and 16 when her pre-recorded evidence including cross-examination under s 21A *Evidence Act* was taken.

[20] She told police more than once that she did not want to talk about the matter and only reluctantly provided police with the following information. She understood police were taking a statement about her computer. Her email address was "princess_Shani_x@hotmail.com".[8] On 9 November 2008 she met a person online called Tick Tock on the website "www.vampirefreaks.com".[9] She told Tick Tock that she was 13 turning 14.[10] Tick Tock said he was good at hacking and he could get her more friends on MySpace.[11] She added his email address "teamloosh@gmail.com" on MSN Messenger. He sent her a program over MSN Messenger which she attempted to download.[12] Using this program, he accessed and turned on her webcam remotely.[13] He asked her to go on webcam but she declined.[14]

[21] The following day on 10 November 2008, Tick Tock talked to her after school via MSN Messenger.[15] She asked him about the program to help her get more friends on MySpace.[16] He turned on her webcam remotely.[17] She tried to block him on MSN Messenger.[18] He made a countdown appear on her computer screen and said he

---

6 Exhibit T1325, page 1.
7 Exhibit T1325, page 2.
8 Exhibit T1414, Q121, page 9.
9 Exhibit T1414, Q92, page 7.
10 Exhibit T1414, Q155, page 13.
11 Exhibit T1414, Q111, page 8.
12 Exhibit T1414, Q112, page 9.
13 Exhibit T1414, Q126, page 10.
14 Exhibit T1414, Q134, page 10.
15 Exhibit T1414, Q164, page 13.
16 Exhibit T1414, Q182, page 15.
17 Exhibit T1414, Q186, page 15.
18 Exhibit T1414, Q187, page 15.

would destroy her computer if she did not unblock him.[19] She complied. He told her to strip on webcam, threatening to destroy her computer and hack her online accounts if she did not.[20] He instructed told her to masturbate on webcam[21] and write something on her breasts.[22] She acceded, knowing the incident was being video recorded. She noticed that at about this time some of her image files were deleted from her computer.[23] She was pretty sure the person on the Vampire Freaks website had his "picture" on his profile. His "picture" in the webcam was different but "you could tell they were the same person".[24] He looked like an "Emo" with black hair and a fringe covering the face. He said he was good with computers. After the video was uploaded to the internet, a number of people on Vampire Freaks and MySpace tried to message her and add her as a friend.[25] After the incident she was crying and felt "horrible".[26] She did not want to do the things he told her to do; she complied because she was scared.[27] She did not tell anyone the details of the incident.[28]

[22] In her pre-recorded evidence on 21 April 2011, she confirmed that what she told the police was true. In cross-examination she agreed that she did not meet Tick Tock in person; their only contact was online. She saw him on webcam the night before the video recording but was unsure whether she saw him on webcam on the day of the video recording. She was, however, "quite sure" that he was the same person because "he remembered things from the night before".[29] His webcam image was close-up, about five inches square and she could see his face.[30] She identified the appellant's photo on a photo board shown to her by police as a photo of Tick Tock. She agreed she may have given him a photo the night before the video recording. He tried to get in contact with her a week or two after the video recording but she deleted her email account.

*B's evidence*

[23] B was aged 14 in March 2009 when count 6 was charged as occurring and 16 when she gave evidence by way of her police interview, admitted under s 93A *Evidence Act*, and her pre-recorded evidence including cross-examination, admitted under s 21A *Evidence Act*.

[24] She told police that she met someone on the website Vampire Freaks who "seemed nice" so she added him on MSN Messenger.[31] He told her he was 19[32] and she told him she was 14.[33] Her username was "PurpleRubberDucky".[34] Using Vampire Freaks, he said he wanted to see more of her. He said things to her including "fuck me"[35] and "do you want to meet up for sex?"[36] She declined. He called her names including

19 Exhibit T1414, Q187, page 15.
20 Exhibit T1414, Q187, page 16.
21 Exhibit T1414, Q208, page 17.
22 Exhibit T1414, Q211, page 17.
23 Exhibit T1414, Q258, page 21.
24 Exhibit T1414, Q249, page 20.
25 Exhibit T1414, Q238, page 19.
26 Exhibit T1414, Q260, page 21.
27 Exhibit T1414, Q261, page 21.
28 Exhibit T1414, Q285, page 23.
29 T 1-8, line 2.
30 T 1-9, lines 35-45; T 1-10, lines 10-15.
31 Exhibit T1415, Q42, page 5.
32 Exhibit T1415, Q129, page 12.
33 Exhibit T1415, Q55, page 6.
34 Exhibit T1415, Q52, page 6.
35 Exhibit T1415, Q33, page 4.
36 Exhibit T1415, Q72, page 8.

"dumb", "stupid bitch" and "slut".[37] She blocked him but he created another Vampire Freaks account and "did the same thing",[38] again sending her messages asking to meet up for sex.[39] He created a third account on Vampire Freaks.[40] He sent her files on MSN Messenger but she did not open them.[41] She apprehended that he had used the usernames "lolhello"[42] and "ohhi"[43] on Vampire Freaks.

[25] In her pre-recorded evidence on 21 April 2011, she confirmed that what she told police was true. In cross-examination she agreed that she did not meet or speak to this person other than on MSN Messenger and Vampire Freaks. The person had multiple profiles on Vampire Freaks. The reason she knew it was the same person using the profiles is because he said he was.[44] She "fairly quickly" identified the appellant's photo from a police photo board as the person in the photo in the Vampire Freaks account. He also had a photo on the MSN Messenger site which looked like the photo she identified.[45]

*The police and expert technical evidence*

[26] Brooke Ellis, a detective senior constable with the AFP[46] went to the appellant's house on 8 April 2009 and took possession of the Toshiba laptop, Seagate hard drive and Verbatim hard drive.[47]

[27] Gerard Murphy[48], a forensic computer examiner employed by the AFP,[49] also attended the appellant's house that day. The Toshiba laptop was in standby mode. When he opened it, a Firefox web browser was running, displaying emails for the Gmail account "teamloosh@gmail.com".[50] The program Windows Live Messenger was not logged in, but it displayed emails for the account "rofles@scriptkitty.net".[51] He examined the Toshiba laptop's hard drive and the Seagate hard drive.

[28] Alexander Tilley, a technical specialist in the cybercrime team of the AFP,[52] gave evidence which included the following. Between November 2008 and April 2009 he was assigned to monitor the website "unkn0wn.ws". He saw a message posted by someone with the username "Rofles" which stated

> "I'm Rofles, I destroy lives…I make a girl cry. I force her to strip and fuck herself. I force her to finger her asshole and lick her fingers. I then make her write a greetz to a mate of mine on her tits. Epic win?"[53]

---

37 Exhibit T1415, Q70, page 8.
38 Exhibit T1415, Q71, page 8.
39 Exhibit T1415, Q72, page 8.
40 Exhibit T1415, Q58, page 7.
41 Exhibit T1415, Q95, page 10.
42 Exhibit T1415, Q143, page 14.
43 Exhibit T1415, Q147, page 14.
44 T 1-36, line 47.
45 T 1-46, line 42.
46 T 1-40, line 47.
47 T 1-44, line 20.
48 The transcript refers to Jared Murphy but the Appeal Record Book Index prepared by the parties refers to Gerard Murphy.
49 T 1-47, line 6.
50 T 1-48, line 8.
51 T 1-48, line 24.
52 T 1-53, line 10.
53 T 1-57, line 45; T 1-58, line 35; Exhibit C0002.

[29] These messages related to the video "kkkk.avi", the subject of count 3, which was uploaded to the internet website, RapidShare.[54] Mr Tilley accessed the video[55] and ultimately indentified the girl in it as A.

[30] He apprehended that "Rofles" was an Australian[56] and contacted RapidShare[57] which confirmed that the video was uploaded on 8 January 2009 from the appellant's IP address.[58] The AFP monitored that IP address between 27 February 2009 and 9 April 2009.[59] Mr Tilley went to the appellant's house on 8 April 2009 and found the various computer equipment in the appellant's bedroom.[60] He later examined the appellant's laptop and A's computer and found that the Poison Ivy files on the appellant's laptop matched a file on A's computer.[61] He identified that the appellant's laptop had used Poison Ivy to hack into A's computer and 133 others.[62] He connected the data on these computers back to the appellant's laptop.[63] A's computer was configured so that Poison Ivy would automatically start when it was switched on, without any voluntary act from A.[64]

[31] Mr Tilley conducted a hacking experiment using the Poison Ivy files on the appellant's laptop to control another computer.[65] He downloaded files from the "victim" computer, created a countdown and remotely activated the webcam. He demonstrated that it was possible to replicate the kkkk.avi video using files from the appellant's laptop and A's computer.[66] He found no evidence of hacking of the appellant's laptop, the Toshiba hard drive, or the Seagate hard drive.[67] The reason that he did not conduct an experiment to see if a third party had hacked into the appellant's computer was because "It was impossible to do an experiment based on a computer setup and network that setup that we had no visibility of".[68]

[32] Jarrad Lisman, an electrical engineer employed by the AFP and specialising in data interception,[69] reviewed the appellant's IP address for date slices of intercepted data between 23 February 2009 and 8 April 2009.[70] In monitoring the MSN Messenger chat logs, a single line indicated that a single device was communicating.[71] If there was another device hacking into the IP address, a second line would appear and intersect with the first line.[72] As there was only one line, there was no evidence of hacking.[73]

[33] Mr Lisman explained that "Address Resolution Protocol" (ARP) poisoning was a method of corrupting a computer. It involved connecting a foreign device imitating the modem

---

54 T 1-62, line 45.
55 T 1-64, line 45.
56 T 1-61, line 17.
57 T 2-3, line 43.
58 T 2-4, line 23.
59 T 2-5, line 45.
60 T 2-6, line 13.
61 T 2-22, line 19.
62 T 2-23, line 36.
63 T 2-23, line 44.
64 T 2-34, line 15.
65 T 2-30, line 42.
66 T 2-30, line 46; T 2-31, line 19; T 2-32, line 31; T 2-31, line 44; T 2-31, line 5; T 2-32, line 43.
67 T 2-38, line 43.
68 T 2-69, line 3.
69 T 3-18, line 17 and 27.
70 T 3-22, line 10.
71 T 3-25, line 43.
72 T 3-26, line 3.
73 T 3-26, line 22.

router to the computer. Given the close proximity of the appellant's laptop to his router (approximately one metre), ARP poisoning "would never work."[74] In order to successfully execute an ARP poisoning attack, the hacking device would need to be closer to the computer than the actual router, in this case within one metre. Any hacking attempt on the appellant's wireless network would be visible unless the hacking device directed the traffic through another connection such as 3G.[75] A hacking attempt using a wired-device would require the hacking device to be physically attached to the router, with an additional wire leading to a device.[76] The wires connecting the hacking device to the router would be visible.[77] The degree of sophistication required to hack into the computer without any visible trace would involve a team of people such as a law enforcement or intelligence agency working over a two month period.[78] Mr Lisman considered that in 2008 an eight-character password would have taken 25 years to crack.[79]

[34] Constable Paul Georgiades, an AFP police officer and the principal investigating officer[80] gave evidence including the following. He also attended the appellant's house on 8 April 2009. He examined the kkkk.avi video and identified that it commenced recording between 3.24 pm and 3.26 pm Queensland time on 10 November 2008 and finished recording between 4.02 pm and 4.04 pm Queensland time.[81] At 5.06 pm that day, an email was sent from "rofles@scriptkitty.net" to "gs69azza@hotmail.com" containing the subject line "hey aaron i got a gift for you"[82] and containing the MSN Messenger chat log between Tick Tock and A when the video was being recorded.[83]

[35] Calvin Wills, a senior digital forensic investigator and examiner employed by the AFP,[84] analysed the appellant's Toshiba laptop.[85] It had the username "Rofles"[86] and contained a Poison Ivy folder created on 15 January 2008[87] which was last modified on 8 March 2009.[88] A Poison Ivy sub-folder created on 9 November 2008 contained photos of a girl in various degrees of undress.[89] Images found on the appellant's Verbatim hard drive resembled those of A in the kkkk.avi video.[90]

[36] MSN Messenger chat logs on the appellant's Toshiba laptop and Seagate hard drive were connected to two accounts: "rofles@scriptkitty.net" and "teamloosh@gmail.com".[91] The appellant's MSN Messenger contact list included the email addresses: "princess_shani_x@hotmail.com"[92] (belonging to A) and

---

74 T 3-37, line 45.
75 T 3-42, line 22 and 37.
76 T 3-38, line 38.
77 T 3-38, line 45.
78 T 3-43, line 12.
79 T 3-34, line 37.
80 T 3-79, line 43.
81 T 3-81, line 36; T 3-82, line 6.
82 Exhibit T0054; T 3-84, line 22.
83 T 3-85, line 17.
84 T 4-8, line 14-20.
85 T 4-9, line 46.
86 T 4-10, line 7.
87 T 4-16, line 24.
88 T 4-16, line 27.
89 T 4-24, line 8. These photos were listed as being created on 10 November 2006 but Mr Tilley apprehended that the date had been altered by a software tool. It is common ground that this 2006 date is incorrect; T 4-39, line 35; T 4-40, line 3; T 4-39, line 42.
90 T 4-52, line 9.
91 T 4-28, line 44.
92 T 4-30, line 10.

"random1much@hotmail.co.uk" (belonging to B).[93] Mr Wills also examined A's hard drive and discovered that one of her MSN Messenger contacts was "teamloosh@gmail.com".[94] He found child exploitation material on the appellant's Verbatim hard drive[95] and Toshiba laptop (count 7).[96] He also found traces of the kkkk.avi video on the laptop.[97] RapidShare, the program through which the kkkk.avi video was uploaded to the internet, had been installed on the appellant's Seagate hard drive.[98] There was no evidence (such as logs of access with external parties, failed password attempts or additional software)[99] to indicate that any third party had exercised control over the appellant's laptop.[100]

[37] Craig Wright, an information security network forensics specialist, [101] qualified in security, malware, digital forensics, secure coding, attack techniques and penetration testing gave evidence about the possibility of the appellant's computer being hacked. A "pineapple device" would be required to intercept the signal between the appellant's Toshiba laptop and the wireless router. A pineapple device is a small computer that imitates the local wireless network, intercepts data and forwards internet traffic away from the router to the device.[102] It requires a large antenna and draws a lot of battery power.[103] Given the appellant's brick house and the layout of his bedroom, a 15 decibel gain antenna may work, but such an antenna would only have a battery life of half an hour.[104] The pineapple device would need to be within 30 metres of the antenna and the Toshiba laptop.[105] Had such a device been used, there would be visible evidence of hacking on the intercepted traffic of the wireless router.[106] Security warnings and error signals would appear when the appellant accessed websites.[107] The hacking tools would also be detected by the appellant's "Norton Ghost" anti-virus software.[108] The use of a pineapple device alone would be insufficient to plant directory files, directory subfolders or photographic images on the appellant's laptop or hard drive.[109] A RAT would also be required[110] and it would be "extremely difficult"[111] to use this undetected.

[38] In cross-examination Mr Wright agreed that his report was based on the assumption that there was one wireless network[112] and no other devices were present in the network trace.[113] He also agreed that it was possible to divert the intercepted traffic through the computer using a 3G network but added that this would require a modified pineapple with two antennae.[114]

---

93 T 4-33, line 35.
94 T 4-49, line 39.
95 T 4-35, line 33.
96 T 4-35, line 37.
97 T 4-65, line 28.
98 T 4-66, line 27.
99 T 4-67, line 30.
100 T 4-68, line 1; T 4-67, line 10.
101 T 5-59, line 31.
102 T 5-61, line 40.
103 T 5-61, line 46.
104 T 5-64, line 15.
105 T 5-64, line 34.
106 T 5-62, line 28.
107 T 5-66, line 35.
108 T 5-70, line 10.
109 T 5-67, line 21; t 5-67, line 37.
110 T 5-67, line 43.
111 T 5-68, line 19.
112 T 5-75, line 40.
113 T 5-76, line 22.
114 T 5-89, line 28.

[39] Edward Cornejo, a technical specialist employed by the AFP,[115] examined the data intercepted by the AFP and developed an algorithm. This program identified that data communication between two computers did not contain any missing fragments not captured by the AFP intercept system.[116]

[40] Jeffery Martin, a technical officer employed by the AFP whose work involved the delivery and integrity of telecommunications interceptive products,[117] gave evidence including the following. He examined the intercepted data captured by the AFP between 18 and 30 March 2009 to ensure that the entire product intercepted by the carriage service provider was delivered correctly to the AFP.[118] As all the files were present,[119] this indicated that during that period no files were missed.[120]

[41] Aaron Parrey gave evidence that he is the owner of the email address "gs69azza@hotmail.com"[121] and one of his contacts is the appellant's email address "rofles@scriptkitty.net".[122] He received an email from "rofles@scriptkitty.net"[123] with the subject line "hey aaron i got a gift for you".[124] There was nothing attached to the email but when he spoke to "Rofles" on either MSN or IRC[125] "Rofles" sent him a video. He clicked on the link, downloaded the video and watched part of it.[126] The screenshots from the kkkk.avi video matched the video sent to him by "Rofles".[127]

**The defence case**

*The appellant's evidence*

[42] The appellant's evidence included the following. He denied knowingly committing any of the charged offences[128] and said he did not hack A's computer[129] or upload the kkkk.avi video to the internet via RapidShare.[130] He denied any contact with B.[131] He was not the person who used the carriage service to access child pornography material or child abuse material.[132] He had no knowledge of the child pornography, child abuse, or child exploitation material that was found on his Toshiba laptop, his Verbatim hard drive and his Seagate hard drive.[133]

[43] He often turned off his firewall because he believed it was "useless"[134] and he very rarely updated his Windows operating system.[135] He used the password "r0lf3z"[136] during

---

115 T 3-76, line 45.
116 T 3-77, line 46; T 3-78, line 1.
117 T 6-12, line 23.
118 T 6-12, line 33.
119 T 6-16, line 15.
120 T 6-16, line 31.
121 T 5-43, line 35.
122 T 5-44, line 44.
123 T 5-46, line 20.
124 Exhibit T0054.
125 Internet Relay Chat.
126 T 5-47, line 3.
127 T 5-47, line 17.
128 T 12-55, line 36.
129 T 12-55, line 36.
130 T 10-50, line 34.
131 T 11-18, line 38.
132 T 10-51, line 36.
133 T 10-51, line 43; T 11-9, line 5.
134 T 10-46, line 44.
135 T 10-47, line 16.
136 T 10-47, line 47; T 11-24, line 8.

the relevant period between 2008 and 2009.[137] He also created the email addresses "teamloosh@gmail.com" and "rofles@scriptkitty.net".[138] He denied setting up a Vampire Freaks account under the name "hai2u" with the password "r0lf3z" even though it was linked to his IP address.[139] He also denied setting up a Vampire Freaks account under the name "OHHI" with the password "r0lf3z" even though he agreed it was linked to his IP address and a photo of him accompanied the profile.[140]

[44] A person known as "Digerati", the appellant claimed, may have committed all seven counts. Digerati hacked his computer and planted the evidence out of revenge[141] because the appellant had previously leaked documents in which he claimed that Digerati had groomed children online and tried to have sex with them.[142]

[45] The appellant denied posting a screenshot under the name "Rofles" which said:

> "…its extremely easy to get a girl to do shit, just coax them along - be friendly – be nice – if that fails…OMG…then you hack them and force the fucking bitch to do it. if they d/c or say no or anything just wait and wait and boom 'why is my computer turning off and wheres my documents'".[143]

The appellant knew Aaron Parrey but denied sending him any emails.[144]

[46] The appellant used both a free version of RapidShare and, from 2006 onwards, another version through his brother's account.[145] He downloaded the program Poison Ivy and saved it in the folder "PI2.3.2" on his Toshiba laptop.[146] He used the folder "H4X04" which was on his laptop, but he knew nothing of its sub-folder, "Sharni_PC".[147] He reformatted his computer on 7 April 2009 because he believed he found remnants of a "rootkit".[148]

[47] In cross-examination, he agreed that he recalled part, but not all of the MSN Messenger communications found on his Seagate hard drive. He did not recall the conversation made via the email address "teamloosh@gmail.com" which stated: "[I] just ruined some girls life, hacked her computer n msn, and gave everyone nude pics of her haha".[149] He did not recall his girlfriend contacting him via MSN Messenger a few days later in these terms: "Luan, what do you mean the other night when you said to me that you hacked into a girl's MSN and gave everyone nude pictures of her?"[150]

[48] He could not remember whether he gave a folder containing images of child pornography, including four images of A,[151] the name, "My Cockuments".[152] He denied any knowledge of a message sent from "teamloosh@gmail.com":

---

137 T 11-24, line 8.
138 T 10-49, line 26.
139 Exhibit T0187; T 11-25, line 24.
140 Exhibit T0162; T 11-30, line 46; T 11-34, line 18.
141 T 11-9, line 15; T 12-47, line 25.
142 T 11-7, line 31.
143 Exhibit T0004; T 11-9, line 35.
144 T 11-10, line 12.
145 T 11-11, line 17.
146 Exhibit T2222; T 11-11, line 40; T 11-12, line 34.
147 Exhibit 1242; T 11-13, line 24.
148 T 11-16, line 23; T 11-16, line 38.
149 Exhibit T0017; T 11-54, line 43.
150 T12-14, line 36.
151 T 12-25, line 46.
152 Exhibit T1328.

> "U get a program called Poison Ivy, with that program you make a server, that server is classed as a virus (trojan virus) you then send it to people, they open it, and your client (Poison Ivy) goes LOLOLOL, LET'S GO NUTS."[153]

[49] He suggested that a computer technician who attended his house during 2008 or 2009 may have been responsible for hacking his laptop[154] and that his girlfriend's account may also have been hacked.[155]

*The evidence of Dr Bradley Schatz*

[50] The appellant called Dr Bradley Schatz, a digital forensic computer scientist,[156] whose evidence included the following. Dr Schatz, in his report of 11 August 2012,[157] stated that he located trace evidence of the kkkk.avi video on the appellant's Toshiba hard drive.[158] It was possible for a computer's IP address to be cloned using either ARP poisoning (which requires the attacker to be in physical proximity to the wireless network), or a routing attack (which requires the attacker to have control over the network infrastructure).[159] The prosecution evidence was consistent with the Windows Operating System on the appellant's laptop being reinstalled on or around 7 April 2009.[160] Dr Schatz noted that "such an operation generally results in significant overwriting of evidence."[161] It was reasonable to conclude that there were vulnerabilities in the appellant's laptop which may have enabled it to be hacked.[162] His opinion was based on the general vulnerability of computers,[163] and not a specific analysis of the appellant's laptop. In a supplementary report, he stated that he "found no abnormalities … which might indicate the involvement, or potential involvement, of a third party accessing the IP address."[164]

[51] In his oral evidence in chief Dr Schatz confirmed his findings that trace evidence of hacking may have been lost as a result of the appellant reinstalling or reformatting his Toshiba laptop in April 2009.[165] He explained that a "BIOS-level rootkit" is a piece of malware which hides inside the operating system[166] and would not be affected by a reinstall.[167] It was possible the appellant's IP address had been cloned and the appellant had been the target of an "ARP poisoning attack".[168] For this to occur, the attacker would need to be connected to the same wireless or wired network as the victim computer,[169] have access to the network password,[170] a power supply,[171] a RAT[172] and proximity

---

153 Exhibit T0021; T 12-40, line 7.
154 T 11-81, line 39.
155 T 12-19, line 20.
156 T 12-63, line 3.
157 Exhibit D0001, Report of Dr Bradley Schatz dated 11 August 2012.
158 Above, 21.
159 Above, 8.
160 Above, 10.
161 Above.
162 Above.
163 Above.
164 Exhibit D0002, Supplementary Report of Dr Bradley Schatz dated 28 August 2012, 8.
165 T 12-65, line 13.
166 T 12-65, line 20.
167 T 12-65, line 43.
168 T 12-69, line 22.
169 T 12-70, line 1.
170 T 12-70, line 19.
171 T 12-71, line 4.
172 T 12-86, line 46.

to the network.[173] He agreed with Mr Tilley's assessment that the range would be within twenty metres.[174] The scenario of a RAT such as Poison Ivy being used to remotely hack into and operate the appellant's laptop[175] was not a viable method of attack because evidence of hacking would be observed through the intercepted data of the AFP.[176]

[52] He also considered whether an attacker using a 3G network connection together with the appellant's wireless network could hack into the appellant's laptop.[177] A pineapple device or similar with a 3G dongle would be sufficient to obtain a signal,[178] but the device would need to be linked to a power source, contain an inbuilt antenna and be within 20 metres of the appellant's computer.[179] The limitations on hacking include the features of the house (brick rather than timber)[180] and the size of the antenna.[181] A wireless connection would be too weak to hack in from more than one house away.[182] He conducted an experiment involving communication between a victim computer, a controlling computer and a third party controlling computer.[183] He was able to achieve a signal between the attack computer and the access point through three floors and one metre of concrete.[184]

[53] He next considered the scenario of an ARP poisoning attack where the attacking computer uses a 3G connection to imitate the appellant's access point and redirects all the network communications without detection.[185] If this were to happen, there would be no internet traffic at all on the intercepted line[186] and he would not expect the AFP to discover the intercepted data.[187] This scenario presupposed the existence of 3G network coverage in 2008 in North Lakes where the appellant resided[188] and the pineapple device used being compatible with a 3G dongle device.[189] As with the other scenarios considered, the attacker would need to be within close proximity to the appellant's laptop[190] and have a power supply.[191] This scenario involving an ARP poisoning attack through a 3G connection was the only hacking method consistent with the intercepted data evidence analysed by the AFP.[192] He did not consider that, if the appellant's laptop was in sleep or hibernation mode, it could be accessed by a third party hacker.[193] Only if the laptop had been configured to not go into standby mode when the lid was closed could it continue to communicate.[194]

[54] He disagreed with Mr Lisman's evidence that it would take 25 years to break a network password. He undertook another experiment involving a wireless attack in order to

---

173 T 12-71, line 3.
174 T 12-70, line 36.
175 T 12-87, line 24.
176 T 12-87, line 30.
177 T 12-88, line 17.
178 T 12-88, line 39.
179 T 12-89, line 24.
180 T 12-90, line 1.
181 T 12-89, line 47.
182 T 12-90, line 14.
183 T 12-78, line 35.
184 T 12-90, line 37.
185 T 12-91, line 11.
186 T 12-91, line 20.
187 T 12-92, line 13.
188 T 12-96, line 36.
189 T 12-88, line 17; T 12-96, line 40.
190 T 12-98, line 20.
191 T 12-97, line 9.
192 T 12-94, line 35.
193 T 12-99, line 37.
194 T 13-4, line 14.

crack a password.[195] He fed the information captured by the wireless attack into a cracking tool[196] and found that if the password was a word in the dictionary, it would only take a few seconds to crack.[197] He disagreed with Mr Lisman's evidence that an attacking computer would need to be next to the victim computer.[198] He also disagreed with both Mr Lisman's and Mr Wright's evidence that the attacking device would need to be closer to the laptop than the router;[199] it could be further away.[200] He agreed that if the appellant was using his laptop while it was being hacked by a third party, the appellant would be able to see that someone else was controlling his laptop.[201]

[55] In cross-examination he agreed that his experiments were conducted over a five to 30 minute period. He also agreed that the likelihood of the hacking attack being successful was significantly reduced due to network drop outs, the standard of technology in 2008,[202] and the fact that it was conducted over a five month period.[203] There was no actual evidence that the appellant's laptop had been hacked.[204] He agreed with Mr Tilley that the Poison Ivy program found on the appellant's computer was the same Poison Ivy program found on A's computer.[205] It would be very difficult for a hacker to plant a trace file of the kkkk.avi video on the appellant's computer without being detected.[206] He also agreed with Mr Tilley that the analysis of the MSN Messenger communication with "random1much@hotmail.co.uk" (B's email address) showed no evidence to indicate any involvement of a third party hacking the appellant's IP address.[207]

**The appeal against conviction**

***Joinder of all counts***

[56] It is logical to deal first with the issue raised in grounds 1, 3 and 4 as to the wrongful joinder of counts. Ultimately the appellant did not contend that counts 1, 2 and 3 concerning A were unlawfully joined with count 6 concerning B. Rather he contended that counts 1, 2, 3 and 6 were wrongly joined with counts 4, 5 and 7 and that count 6 should also have been severed in the interests of justice.

[57] Joinder of charges is permitted in trials in Queensland in limited circumstances under s 567 *Criminal Code* 1899 (Qld) which relevantly provides:

> "**Joinder of charges**
>
> **567**(1) Except as otherwise expressly provided, an indictment must charge 1 offence only and not 2 or more offences.
>
> (2) Charges for more than 1 indictable offence may be joined in the same indictment against the same person if those charges are founded on the same facts or are, or form part of, a series of offences of the same or similar character or a series of offences committed in the prosecution of a single purpose.
>
> …"

---

195 T 12-104, line 24.
196 T 12-104, line 31.
197 T 12-104, line 34.
198 T 13-9, line 39; T 13-9, line 43.
199 T 13-38, line 38.
200 T 13-9, line 43.
201 T 13-16, line 15; T 13-25, line 4.
202 T 13-18, line 22.
203 T 13-18, line 24.
204 T 13-21, line 12.
205 T 13-33, line 12.
206 T 13-36, line 45.
207 T 13-39, line 19.

[58] A person charged with multiple offences may apply for separate trials under s 597A(1) *Criminal Code* which provides:

> "**Separate trials where 2 or more charges against the same person**
>
> **597A**(1) Where before a trial or at any time during a trial the court is of opinion that the accused person may be prejudiced or embarrassed in the person's defence by reason of the person's being charged with more than 1 offence in the same indictment or that for any other reason it is desirable to direct that the person should be tried separately for any 1 or more than 1 offence charged in an indictment the court may order a separate trial of any count or counts in the indictment."

[59] It is common ground that counts 4 and 5 were not properly joined under s 567 with counts 1 to 3 and count 6. In my view, that part of count 7 which did not relate to the four images of A was also not joinable under s 567(2). The appellant contended that the evidence on the wrongly joined counts 4, 5 and 7 was highly prejudicial and was prone to encourage the jury to improperly use propensity reasoning. The appellant also contended that the joinder of count 6 concerning B with counts 1 to 5 and count 7 resulted in a miscarriage of justice. Neither the evidence relating to A, nor the evidence relating to the child pornography, child abuse and child exploitation material (counts 4, 5 and 7) nor the evidence relating to B, the appellant contended, were cross-admissible or joinable.

[60] The difficulty for the appellant in making those contentions for the first time on appeal is that trial counsel, who had been acting for the appellant since the committal proceedings, did not apply for separate trials. He appeared to have made a forensic decision to have all counts tried together and in doing so waived this procedural irregularity. Ordinarily, litigants cannot forensically conduct a trial one way and, when the tactic adopted results in conviction, appeal on the basis that they should have conducted the trial another way. As the plurality of the High Court noted in *Patel v The Queen*[208]: "Although the law recognises the possibility that justice may demand exceptions, it is a cardinal principle of litigation, including criminal litigation, that parties are bound by the conduct of their counsel."[209]

[61] Trial and appellate courts do everything possible to limit the almost inevitable jury prejudice flowing from hearing disturbing cases like this involving the sexual exploitation of children and young people. That is because, as Gibbs CJ noted almost 30 years ago in *De Jesus v The Queen*, such cases "are peculiarly likely to arouse prejudice against which a direction to the jury is unlikely to guard".[210] Had the appellant applied for separate trials on counts 1, 2 and 3; counts 4, 5 and that part of count 7 not concerning A; and count 6, he is likely to have succeeded. But Gibbs CJ also recognised that whilst

> "it is not necessarily fatal to an appeal that counsel for the accused at the trial failed to raise the necessary objection … if it were thought that counsel had deliberately refrained at the trial from submitting that the joinder was impermissible, in order to gain some tactical advantage, the case would be different …"[211]

---

208 (2012) 247 CLR 531.

209 Above, 562.

210 (1986) 68 ALR 1, 4-5.

211 Above, 5.

[62] The appellant's omission to object to the joinder of the counts in this case seems to have been a carefully considered, rational, tactical decision. The defence case was that someone had hacked into and taken control of the appellant's computer without his knowledge and used it to commit counts 1 to 7. This, the appellant claimed, may have been done in an act of revenge by former associates with whom he played computer games, and hacked into computers belonging to others, and whom he later antagonised. This hypothesis was arguably more likely if the hacking of the appellant's computer was extensive, on a grand scale, on multiple occasions and of a kind calculated to get him into serious trouble. On the defence case the appellant was as horrified as anyone about the offences because he was an innocent dupe, set up by someone else. The appellant appears to have pursued a well thought out forensic advantage in not applying for separate trials.

[63] As the appellant did not apply for separate trials, there has been no error of law under s 668E(1) *Criminal Code*. Nevertheless, this Court will set aside the guilty verdicts under s 668E(1) if the wrongful joinder has amounted to a miscarriage of justice.[212] Defence counsel made carefully considered admissions with the result that the jury did not view the improperly joined material in counts 4, 5 and 7. The jury merely saw a table indicating the computer file type and the times and dates when the material was accessed from the appellant's IP address.[213] Unquestionably, the most concerning material before the jury was the kkkk.avi video relevant to the charges involving A. The jury would have seen this material had the counts involving A (counts 1 to 3 and part of count 7) proceeded separately. I am satisfied that in all the circumstances pertaining here, the appellant's forensic decision not to apply for separate trials has not produced any unfairness amounting to a miscarriage of justice under s 668E(1). Grounds of appeal 1, 3 and 4 are not made out.

**The course of the trial and the judge's directions**

[64] In considering the remaining contentions, it is essential to discuss how the trial was conducted and relevant aspects of the judge's directions to the jury.

[65] From the beginning of the trial when defence counsel, somewhat unusually, made an opening address, it was clear to the jury that the sole issue was whether the prosecution could establish beyond reasonable doubt that the appellant had committed the offences, rather than someone else who had hacked into his computer and set him up.[214] The appellant made admissions, cross-examined the prosecution expert witnesses and gave and called expert evidence in a way which was consistent with all the offences being committed. His evidence was that he was not the offender; and Dr Schatz gave evidence in the defence case raising the possibility of someone else hacking into the appellant's computer and using it to commit the offences.

[66] At the close of the evidence, the judge and counsel discussed the matters of law to be dealt with in the judge's jury directions. The prosecutor invited the judge to give a detailed propensity warning with which defence counsel largely agreed.[215] Whether inadvertently or deliberately, the judge ultimately did not give that direction and was not asked to redirect.

---

212 *R v BBG* [2007] QCA 275, [27].

213 Exhibit T1328; Exhibit T1325; Exhibit T1408; Exhibit T1407.

214 T 1-14 to 16.

215 T 13-48 to 53.

[67] The judge gave the following relevant jury directions

> "… Under our system of criminal law, the onus is on the prosecution – the Crown – to prove every element of the offence charged – of the seven offences charged. There is no burden on the accused to prove anything, let alone to prove his innocence. He is presumed innocent unless and until the Crown proves otherwise. You can convict only if the prosecution has established that he is guilty. *And you do this, of course, on a charge by charge basis*. There is a certain standard that the prosecution has to reach. To discharge that onus, the prosecution must prove beyond reasonable doubt that the accused is guilty. It's for you to decide whether you have such a doubt as you consider reasonable.
>
> You have to decide whether you are satisfied that the prosecution has proved all the elements of the offence – *any particular offence* – beyond reasonable doubt. If you are left with a reasonable doubt about guilt, it is your duty to acquit *on that charge*. If you are not left with any such doubt, it is your duty to convict." (my emphasis)

[68] Later his Honour in uncontroversially explaining how the jury could draw inferences, stated that it was

> "necessary not only that guilt be a reasonable inference, but also that it be the only rational inference open in the circumstances. Otherwise you couldn't be satisfied beyond reasonable doubt. If there is a reasonable hypothesis consistent with innocence, it's your duty to acquit. A reasonable hypothesis is more than a bare possibility. It cannot be based on mere speculation or conjecture that has no basis in the evidence. A reasonable hypothesis is one which has regard to the whole of the evidence, and not just to each individual item of circumstantial evidence considered separately.
>
> You should not reject one circumstance merely because considered alone, no inference of guilt can be drawn from it. The process is like looking at a rope: one strand may not be enough to take the weight of the load, put all the strands together and the rope is fine. It's for you to say whether the inference of guilt on *any particular charge* exists actually and clearly and so overcomes the others as to leave no reasonable doubt of guilt in your mind."[216]

[69] The judge reminded the jury that the fact that the appellant had given evidence did not reverse the onus of proof: "The Crown must still prove the case against him and do so beyond reasonable doubt."[217] His Honour gave appropriate and uncontroversial directions as to the dangers and shortcomings of the identification evidence given by A and B. His Honour then referred the jury to the agreed list of uncharged discreditable conduct led in the prosecution case, pointing out that the appellant denied responsibility for most of this; he said it was someone else, not him. But, his Honour explained,

> "even if you came to the conclusion that that wasn't true and that it was he who was responsible for these discreditable actions or conduct, they do not point toward guilt; you can't use them to draw an inference of guilt."[218]

---

216 Summing-up, 4 lines 29-44.

217 Summing-up, 6 lines 6-7.

218 Summing-up, 7, lines 5-9.

[70] His Honour explained that

> "[T]he prosecution put all of that evidence before you to demonstrate that the [appellant] had the technical skills to access [A's] computer on 9 and 10 November 2008. You must not use that evidence as evidence to conclude that the [appellant] was someone who had a tendency to commit the type of behaviour involved in the commission of counts 1 or 2 or, for that matter, count 6. It would be wrong for you to reason that the [appellant] ran the Poison Ivy program on many other occasions, therefore, it's more likely that he committed any of these charges or because he said things on other occasions, therefore, it's more likely that he committed any of these offences. That's not sensible rational reasoning.
>
> Now, that's all conduct which he denied. He says it wasn't him anyway who did any of that. There's also evidence of some conduct, which he admits, which you might think is discreditable. He admitted that he hacked games and that he cheated at games. Again, that evidence was led to show that there were people on the internet with a motive to harm him. It would be wrong to reason that he's more likely to be guilty by reason of that conduct."[219]

[71] His Honour told the jury that they could "consider the charges in any order"[220] and explained to the jury that the appellant was

> "charged with the seven offences set out in the indictment. You must consider each charge separately. If you find you have a reasonable doubt about an essential element of one charge, you must find the [appellant] not guilty of that charge. You then go on and consider the other charges, each in turn, and each gets considered separately. However, there is a common theme in the [appellant's] response to the charges. To each he says that he was not involved.
>
> His primary submission in relation to counts 1 to 6 is that you could not be satisfied beyond reasonable doubt that he did the acts constituting the offences, that is, use of, or in one case, conduct by means of, a carriage service. In relation to count 7, his primary submission is that you could not be satisfied beyond reasonable doubt that he had knowledge that the offending material was on his computer. Those aspects of his case were dealt with by his counsel collectively, together, and rightly so because the totality of the evidence is what you have to have regard to in assessing whether you're satisfied beyond reasonable doubt that he was the perpetrator of these events.
>
> … Now, the prosecution alleges the use of a carriage service at the following times: count 1, 10th of November, 2008; count 2, 9th of November, 2008; count 3, on or about the 8th of January, 2009; count 4, between 22nd of February and 8th of April, 2009; count 5, on or about the 26th of February, 2009; count 6, between 19 March and 29 March, 2009. Those are the six counts that involve the use of a carriage service. The seventh count, the possession of material, relates to the day of the police raid in April.

---

219 Summing-up, 7 lines 39-45 to 8, lines 1-6.

220 Summing-up, 8 lines 9-10.

> The [appellant] does not dispute that his computer and the carriage service connected to his IP address were used at those times in the manner alleged by the Crown. He submits that you could not be satisfied beyond reasonable doubt that at any of the relevant times his computer was not under the control of a malicious third party. The prosecution submits to the contrary."[221]

[72] His Honour then summarised the prosecution case, explaining that it emphasised the evidence of Mr Tilley that there were no signs of a third party having intervened in the use of the appellant's computer and the extreme difficulty for someone to do this. The prosecution said that the appellant had the computer, the skills and the necessary software to commit the offences and his IP address was used to do so.

[73] The defence case, his Honour explained, was that the appellant's computer had been hacked and used unlawfully by others who forged and fabricated his name in emails. The offences occurred around the time of the illness and death of the appellant's father when he was not using his computer as much. The defence expert evidence established that it was possible to compromise his computer and his IP address. The defence argued that the prosecution had not proved his guilt beyond reasonable doubt. This was especially so as the appellant had enemies on the internet who had a motive and the skill to compromise his position. He sometimes switched off his firewall and his anti-virus. The actual chat log with A and the kkkk.avi video were not found on his backup drive by the prosecution, although traces of it were found by the appellant's expert, Dr Schatz. As to the identification, the defence pointed out that the unlawful hacker could easily have sent a photograph and used his profile as this material was freely available on the web.

[74] The judge explained that, in summary, the "big issue in this trial" was who did the accessing; who did the use of the carriage service and who put the child exploitation material on the computer.

[75] His Honour handed the jury the relevant sections of the *Criminal Code* (Cth) and *Criminal Code* (Qld) relating to each count and explained the elements of each count in a manner about which there is no complaint. His Honour explained the elements of each offence but again emphasised that the big question in the trial was whether the jury was satisfied beyond reasonable doubt that the appellant committed each offence. When explaining the elements of count 4, his Honour noted:

> "The relevant material is admitted to have consisted of 124 images, one video and seven partial videos. The admission that that was child pornography material has relieved you from the unpleasant duty of having to scrutinise this muck and – and make a decision about whether it was indeed child pornography material; it's admitted that it was by the [appellant]. And he accepts, also, that a carriage service was used to access that material. The only issue is whether it was he who did the accessing and, again, we've been through that evidence now at – at some length.
>
> Unless you are satisfied beyond reasonable doubt that it was he that did the accessing, your verdict should be not guilty. …"

[76] In relation to count 5, the judge again explained to the jury that the appellant had

---

221 Summing-up, D2-2 lines 39-46.

> "admitted that his IP address was used to access child abuse material. He accepts that a carriage service was used to access material and that the material was child abuse material. It consisted of some 17 images. The admission makes it unnecessary for you to examine the material, which is even more upsetting. The only issue is whether it was he who did the accessing and, again, you've been referred to the evidence on that. Again, unless you're satisfied beyond reasonable doubt that it was he who did so, your verdict should be not guilty."

[77] As to count 7, the judge explained it was not in dispute that child exploitation images were found on the appellant's Verbatim and Toshiba hard disk drives as the appellant admitted this. The issue was whether he knew they were there. The judge referred again to the competing contentions and explained it was a matter for the jury whether they were satisfied beyond reasonable doubt that the appellant did know; if they were so satisfied they would return a verdict of guilty, but, if not, their verdict would be not guilty.

[78] His Honour added: "… You can, of course, give verdicts on those charges on which you are unanimous, even if you aren't unanimous on all of them. … Consider each charge separately."[222]

[79] Significantly, defence counsel at trial did not apply for any redirections on matters relevant to the grounds of appeal.

**The absence of a clear and detailed jury direction as to the use to be made of evidence in relation to each count.**

[80] The appellant contended the judge's directions did not sufficiently explain to the jury what evidence was admissible on each count and that this resulted in a substantial miscarriage of justice (ground 5). This was problematic as, for example, evidence admissible to establish counts 1, 2 and 3 was not probative of guilt on counts 4, 5, 6 and 7. While the judge directed the jury to consider each charge separately, the appellant emphasised that his Honour did not direct them against considering all evidence led at trial in respect of each count. The appellant submitted that the directions fell well short of those contained in the Supreme and District Courts Bench Book and left open the possibility that the jury could engage in propensity reasoning.

[81] True it is that the usual practice in cases involving multiple counts is for the judge to direct the jury, in accordance with the Supreme and District Court Bench Book,[223] that the jury must consider each charge separately, evaluate the evidence relating to that particular charge and decide whether they are satisfied beyond reasonable doubt that the prosecution has proved its essential elements.

[82] The trial, from beginning to end, was conducted by the defence on the basis that the prosecution could not disprove beyond reasonable doubt that someone had maliciously hacked into the appellant's computer and used it to commit the offences, thus setting up the appellant. The judge, with the full concurrence of trial counsel, properly highlighted for the jury the real issue on each count: whether the prosecution had established beyond reasonable doubt that the appellant was responsible for the unlawful conduct rather than a malicious unknown hacker. When the judge's directions to the jury are considered as a whole, they sufficiently identified the relevant evidence and law applicable in each case so that the jury understood the real issues in the trial.

---

222 Summing-up, 2-13 lines 37-41.

223 No 34.

[83] It is also true that there was not propensity warning. But such a warning is not always required merely because an accused person is charged with a number of counts containing the same or similar offences against the same victim: *KRM v The Queen.*[224] Whilst these charges did not all concern the same victim, I consider that a propensity warning was unnecessary because of the way the defence case was conducted. To have given a warning of that kind may have diverted the jury from the real issue in this case. It would not have been helpful to the defence.[225] There is no reason to think that the jury here may have convicted the appellant through propensity reasoning given the focussed way in which the trial was conducted. In truth, if the jury were in doubt about the appellant's guilt on one charge because someone may have hacked into his computer and committed the offences, they would have had a doubt on all charges.

[84] As the judge was not asked to give the directions of the kind now sought on appeal, there has been no error of law under s 668E(1) *Criminal Code* (Qld). In light of the way the trial was conducted and the directions which were given, I am unpersuaded there has been any miscarriage of justice under s 668E(1) arising from these aspects of the judge's directions. It follows that this ground of appeal is not made out.

**The judge's directions to the jury as to the expert evidence**

[85] The appellant emphasised that at no stage did the judge direct the jury as to how to deal with the expert evidence which was an important feature of the trial. The significant question was whether the prosecution was able to negative the hypothesis raised by the defence expert witness, Dr Schatz. In a number of areas the experts called by the prosecution disagreed with Dr Schatz. The judge gave no direction to the jury as to how to deal with these areas of conflict despite the complex nature of the expert evidence.

[86] Mr Lisman, Mr Wright and Dr Schatz, the appellant contended, agreed that any wireless attack using the appellant's wireless network rather than a 3G connection would be visible on the intercepted traffic of the appellant's router.[226] Mr Wright considered the required pineapple device would need a large, external antenna and a large power source.[227] Dr Schatz considered the inbuilt antenna would be sufficient to capture the signal of the wireless network. Mr Wright considered a pineapple device would need to be within 30 metres of the appellant's Toshiba laptop[228] whereas Dr Schatz believed it could be 100 metres away if an external antenna was used. Otherwise Dr Schatz agreed with Mr Tilley that the pineapple device would need to be within 20 metres of the appellant's router to connect to the wireless network.[229] Mr Wright believed a device using a 3G connection would require two antennae.[230] Mr Lisman and Mr Wright considered that any pineapple device intercepting communications between the appellant's Toshiba laptop and router would need to be closer to the laptop than the router, whereas Dr Schatz considered it could be further away.[231] Mr Lisman believed that an eight letter password would take 25 years to crack[232] whereas Dr Schatz gave evidence that an eight letter password from the dictionary could be cracked in

---

224 (2001) 206 CLR 221, McHugh J [35], Hayne J [131].
225 *KRM*, McHugh J [37].
226 T 3-42 line 37; T 5-62 line 28; T 12-87, line 30.
227 T 5-61 line 45; T 5-62 line 17.
228 T 5-64 line 34.
229 T 12-70 line 36; T 12-90 line 14.
230 T 5-89 line 28.
231 T 3-38 line 1.
232 T 3-34 line 37.

seconds.[233] The appellant contended that the judge's directions did not sufficiently deal with the issues in conflict between the expert witnesses. The judge should have tailored a direction so that the jurors knew and understood where the relevant evidence was in conflict.

[87] Gummow and Callinan JJ explained in *Velevksi v The Queen*[234] that conflicting expert evidence calls for careful evaluation as it deals with generally unfamiliar and technical matters and will always require careful and usually more elaborate directions from the trial judge to the jury. It is true the judge did not give the directions on expert evidence contained in the Supreme and District Court Bench Book.[235] But as this Court explained in *R v Robinson*,[236] the Bench Book is not a statute prescribing mandatory directions.[237] The judge told the jury that they were the sole judges of fact and made clear that the critical issue in the case was whether the prosecution had negatived beyond reasonable doubt on each count the hypothesis raised by Dr Schatz that someone may have maliciously hacked into the appellant's computer and committed the seven counts.

[88] The appellant in his contentions has rightly identified the areas of conflict between the expert witnesses in this case. But in the end the differences between them were not great. Dr Schatz's evidence established the hypothetical possibility of someone hacking into the appellant's computer and committing the offences without his involvement or knowledge. The prosecution case was that, on the whole of the evidence, the possibility of this occurring was not a reasonable one and could be excluded beyond reasonable doubt.

[89] His Honour referred in his summing-up to the following matters: Mr Tilley gave evidence that there were no signs of a third party having interfered with the appellant's computer. For this to occur, the appellant would have had to click onto a link or a file to activate a RAT which was not something a person with his computer skills would do. The pineapple antenna would have been extremely difficult to set up in the appellant's house. It would have had to be close to his router and to have a power supply. It was not feasible for it to have been in the appellant's bedroom without him discovering it. On the prosecution evidence, had it been outside the house it would have needed an external antenna to connect through brick walls. The prosecution time slice analysis evidence showed usage overlap so that there could have been no interference by another person. The prosecution case was that whilst it was theoretically possible for a computer to be hacked in the way raised by Dr Schatz, it was not reasonably possible for this particular computer in this particular environment to have been hacked.[238] The trial judge told the jury

> "it's a matter for you as to how far you think the evidence went, whether the evidence established that it was possible to compromise his computer or simply that this was a general proposition, possible to compromise computers in this situation."[239]

[90] Later in his summing-up the judge directed the jury to reject any view which he appeared to have expressed on the evidence; it was their experience and judgment

---

233 T 12-104 line 20; T 12-104, line 32.
234 [2002] HCA 4, [181].
235 No 55.1.
236 [2010] QCA 377.
237 Above, [51].
238 Summing-up, D2-2 to 3.
239 Summing-up, D2-4 lines 11-13.

which had to be applied and they must form their own views.[240] His Honour fairly and accurately placed the defence case before the jury. It must be remembered that Dr Schatz found no evidence that the appellant's computer had been hacked and, whilst admitting hacking was possible, he did not think this could be done while the appellant's laptop was in sleep or hibernation mode. His explanation of how it may have been possible for a hacker to takeover the appellant's computer without his knowledge was not one that seemed in the least likely. Directions of the kind now sought may not have helped the defence and would tended to have confused the jury as to the real issue in the trial.

[91] Again, it was significant that a redirection in the terms now sought by the appellant was not requested by defence counsel at trial. The judge's directions adequately dealt with the experts' evidence in the circumstances of this trial. I am unpersuaded that there has been "a wrong decision of any question of law" or "a miscarriage of justice on any ground" under s 668E(1) *Criminal Code* as a result of the judge's directions to the jury concerning the expert evidence. This ground of appeal is not made out.

**Did the summing-up as a whole cause a miscarriage of justice**

[92] The appellant's final ground of appeal is that the judge's directions to the jury caused a miscarriage of justice because they did not give proper assistance on how to approach and deal with the case. This follows, the appellant contended, from the cumulative effect of the other argued grounds of appeal, especially the absence of a direction as to the use of evidence in proof of particular counts and the failure to direct on the use of expert evidence. The judge simply left the case to the jury "globally" without any real assistance. This has the result that the jury may have convicted because of the absence of those directions so that the trial has not been conducted according to law.

[93] Taking into account all the matters raised by the appellant in combination, I remain unpersuaded that the joinder of the charges and the omission of the judge to give the directions identified by the appellant may have contributed to the appellant's conviction: *BRS v The Queen*.[241] The prosecution case was compelling. There was no doubt someone committed all the offences using the appellant's computer. The appellant had the skills to commit the offences. The defence hypothesis that a malicious third party may have hacked into his computer without his knowledge and committed each of the offences was extremely unlikely. Whilst Dr Schatz's evidence made clear that this was theoretically possible, even on his evidence it remained extremely unlikely that the appellant's computer, located in his bedroom in a brick house, was interfered with in this way. He found no evidence to suggest hacking. And according to Dr Schatz it was extremely unlikely that such a hacker would plant a trace file of the kkkk.avi video on the appellant's computer without being detected. The complainant, A, identified the appellant's photo as being the person on webcam who forced her to participate in the video recording of kkkk.avi. I consider there is no real chance that the matters raised by the appellant, even in combination, may have resulted in him being convicted on any count. Rather, the jury considered the evidence and on each count and rejected the possibility that someone other than the appellant used his computer to commit the offences. The appellant has not established the matters raised in his grounds of appeal against conviction have resulted in a miscarriage of justice under s 668E(1) *Criminal Code* (Qld). This ground of appeal is not made out.

---

240 Summing-up, D2-13 lines 32-36.

241 (1997) 191 CLR 275, McHugh J 306.

**Conclusion on the appeal against conviction**

[94] The appellant has not succeeded on any of his grounds of appeal against conviction. The appeal against conviction must be dismissed.

**The application for leave to appeal against sentence**

***The contentions in this appeal***

[95] The appellant contended that his effective sentence of 12 years imprisonment with a non-parole period after six years is manifestly excessive. He argued that the sentences should not have been ordered to be served cumulatively. The primary judge gave insufficient weight to his youth and prospects of rehabilitation and gave too much weight to the matters relied on by the prosecution. The appellant contended that an effective global sentence of six years imprisonment should have been imposed.

[96] Mr Copley QC for the respondent contended that the primary judge made no specific error in undertaking the sentencing process but, consistent with Mr Copley's customary balanced approach when prosecuting, fairly conceded that it was for this Court to determine whether the overall sentence was manifestly too long for a 19 year old offender with no prior criminal record whatsoever.[242]

***Counsel's contentions at sentence***

[97] In determining this application it is helpful to begin with a discussion of the sentencing proceeding. After the appellant was convicted on 12 June 2013, his sentence was adjourned and he was remanded in custody. Sentencing submissions commenced on 5 August 2013.

[98] The prosecutor's submissions included the following. The maximum penalties on counts 1, 2, and 6 were 15 years imprisonment; on counts 3, 4 and 5, 10 years imprisonment; and count 7, five years imprisonment. The appellant was 19 when he offended and 24 at sentence. He had no criminal history. He had been in custody from his conviction, a period of 55 days which should be declared as time served under the sentence. There were three serious and separate episodes of offending: the accessing and procuration of A (counts 1 and 2); making the kkkk.avi video available on the internet (count 3); and the separate serious offending against B; count 6. Neither A nor B had elected to provide a victim impact statement. Nevertheless A made clear to police in her interview that she was distressed about the offending and about the video having been placed on the internet; someone had sent her a link to it in a message on MySpace but she had not clicked on it; she hated it.

[99] Count 1, the prosecutor submitted, was a really serious example of an offence against s 474.26 as it involved humiliating a 13 year old child by forcing her to perform sexual acts on herself against her wishes when she was distressed. This was compounded further by forcing her to put her fingers, dirtied by the sexual conduct, into her mouth and by making her write a message on her breasts to the appellant's friend.

[100] Count 2, the prosecutor submitted, involved the appellant accessing on his computer photographs of A in a state of undress and moving them across to his computer for the purpose of facilitating the commission of count 1. A concurrent term of imprisonment was appropriate.

---

242 Appeal transcript 1-28, lines 18-20.

[101] The prosecutor contended that count 3 warranted a cumulative term of imprisonment. The video recording of A arising out of count 1 was available on the internet, albeit not without some difficulty, but it had been accessed thousands of times. The appellant placed it on the internet with enthusiasm and pride about his own cleverness.

[102] Count 4, the prosecutor argued, involved using a carriage service to access child pornography involving 125[243] still images and eight videos. Count 5 involved using a carriage service to access two images of child abuse material, seconds apart, on 26 February 2009. Count 7 involved the possession of child exploitation material. In all, counts 4, 5 and 7 involved 181 images. The prosecutor submitted that sentences concurrent with each other and with the sentences imposed on counts 1, 2 and 3 should be imposed on counts 4, 5 and 7.

[103] As to count 6, the prosecutor pointed out the history of the appellant's procuration of B. On 21 March 2009 he asked her to get naked on camera; allowed her to see him clothed on camera; asked her to take photos of herself and send them to him; and enquired if she was a virgin. The following day he again requested her to get naked on camera. On 26 March 2009 he asked if he could "fuck" her. He repeated this request on 28 March 2009 and asked if she would like to meet him. He said if he could see her naked he would go on camera for her. He repeated his desire to have sex and for her to go on camera. She refused all requests other than to send photographs of herself clothed. She told him on 21 March that she was 14 years old, turning 15. The offence was much less serious than count 1.

[104] The prosecutor referred to the applicant's youth and lack of criminal history and submitted that the appropriate sentences in those circumstances[244] were six and a half years imprisonment for counts 1 and 2; two years cumulative for count 3; 18 months for count 4; 12 months for count 5; three years cumulative upon counts 1, 2 and 3 for count 6; and nine months concurrent imprisonment for count 7, making a total sentence of 11 and a half years imprisonment. As this sentence involved two periods of cumulative imprisonment, the totality principle[245] required moderation of the cumulative sentences. To adequately reflect the totality principle, the appropriate sentence on counts 1 and 2 was five and a half years imprisonment; on count 3, 18 months imprisonment to be served cumulatively upon counts 1 and 2; 12 months concurrent imprisonment on count 4; nine months concurrent imprisonment on count 5; and six months concurrent imprisonment on count 7; and two years imprisonment for count 6 to be served cumulatively upon counts 1, 2 and 3, making a total of nine years imprisonment. There should be a non-parole period of four and a half years.

[105] After referring to relevant provisions of the *Crimes Act* 1914 (Cth), the prosecutor discussed *Tector v The Queen*[246] and *R v Asplund*.[247] The prosecutor emphasised that offences of this kind were difficult to detect and warranted a deterrent sentence.

[106] The appellant at sentence was represented by senior counsel as well as his trial counsel. Their submissions included the following. The most serious offences were counts 1 and 6. Counts 1, 2 and 3 constituted one course of conduct and should be punished by concurrent sentences. Counsel discussed *Tector* and *Asplund* and submitted that the evidence did not suggest that A was in dire fear of the appellant.

---

243 The particulars for count 4 refer to 124 still images.

244 The sentencing submissions preceded *Barbaro v The Queen* (2014) 88 ALJR 372.

245 *Mill v The Queen* (1988) 166 CLR 59

246 (2008) 186 A Crim R 133.

247 (2010) 216 A Crim R 48.

[107] The appellant commenced a Justice Administration Certificate at TAFE in 2007 but was unable to complete the course because of family responsibilities following the death of his father. He worked part-time whilst studying. He completed a diploma of business in November 2010. At the time of his arrest he was studying a dual degree in business management and information technology at the Queensland University of Technology. He was due to complete those degrees at the end of 2015.

[108] Defence counsel tendered a number of references.[248] A letter from the appellant's mother set out his family background. She was Serbian and her husband was a Kosovar Albanian man. They arrived in Australia in October 1971. The appellant was the youngest of their four children. His siblings were aged from 28 to 43 years. Her husband was a self-employed painter who was diagnosed in October 2007 with mesothelioma/asbestos cancer and suffered for 18 months before his death on 9 March 2009. Consistent with their cultural obligations and her husband's last request, the appellant was to look after her in the family home and he did so. She suffered medical problems and was on a disability pension. The appellant helped her care for her dying husband in the family home. The appellant was traumatised because he was not present at the actual moment his father died. He become "quite depressed" after his father's death and dropped out of TAFE. He was a dedicated hardworking student with plans to start his own business consulting company in the future.

[109] A letter from the family doctor confirmed the appellant's mother was on a disability pension because of chronic lower back and scoliosis and other multiple medical problems; the appellant lived with and looked after her.

[110] Letters from the appellant's fiancée; her father's partner; a general practitioner and the appellant's sister and brother all spoke of the appellant's commendable qualities as a devoted son and hardworking student with an aptitude for computers; all considered this offending was out of character.

[111] Defence counsel emphasised the importance of the totality principle and the need to moderate cumulative sentences to avoid crushing the appellant's prospects of rehabilitation. To require him to serve four and a half years imprisonment before parole eligibility was crushing. Whilst the head sentence was a matter for the judge, parole eligibility should be set after about two years imprisonment.

[112] The sentence was adjourned until 20 August 2013. The judge invited further submissions as to the relative seriousness of counts 1 and 6 in the event that he were "to find that the conduct which was procured in count 1 should be ignored".[249] The prosecutor submitted that count 1 was more serious than count 6 because the procuration was of a younger child who was upset and unwilling to be involved. The appellant, represented on this occasion by his trial counsel, referred the judge to portions of the evidence which he contended evidenced friendly banter between A and the appellant. Counsel nevertheless submitted that on the evidence, count 1 was more serious than count 6. It was agreed that the appellant had by this time spent 71 days in presentence custody.

***The sentencing judge's remarks***

[113] The judge commenced his sentencing remarks by reciting details of the appellant's offending. In respect of count 3, his Honour noted that the appellant made child pornography material available on the internet and wrote the message

---

248 Exhibit Z3.

249 Transcript 20 August 2013, 1-2 lines 24-25.

> "I am Rofles. I destroy lives. Who wants this video? I make a girl cry. I force her to strip and fuck herself. I force her to finger her asshole and lick her fingers. I then like make her write a greetz to a mate of mine on her tits. Epic win?"

On another site he wrote "Enjoy and learn from the master" followed by

> "I have never been naked on cam – ever. It's extremely easy to get a girl to do shit. Just coax them along. Be friendly. Be nice. If that fails – OMG, check out this image, SCR. You then hack them and force the fucking bitch to do it. If they d/c or say no or anything, just wait and boom. 'Why is my computer turning off and where's my documents?' Etc etc Everything is easy. Your sensitively, your mastah Rofles."

[114] His Honour observed that these posts cannot be finally removed from the internet. They had been copied to different sites. Whilst some had expired, some had been re-copied to other sites. They were uploaded onto one site on 2 April 2013 with nearly 3,500 views in the following three and a half months.

[115] As to counts 4, 5 and 7, his Honour noted that of the 181 still images, 78 were low or medium to low level; 44 were medium to high level (penetrative sexual activity between children and adults); three were high level (sadism or bestiality) and 56 were animated or virtual. The judge stated he would not take into account in sentencing the further 16 child pornography images which had been deleted but not removed from the computer equipment.

[116] The judge noted that the appellant had used the Poison Ivy program to access other computers in respect of which no charges were brought. The appellant's counsel had conceded that counts 1 and 6 could not be regarded as aberrations. The offending fell into four groups: counts 1 and 2; count 3; counts 4, 5 and 7; and count 6.

[117] His Honour noted that A lived in southern New South Wales with her grandparents. Her mother's whereabouts were unknown and her father lived in Perth. Unbeknown to her grandparents, she posted a heavily made up photograph of herself on the Vampire Freaks website and established an email address. She was anxious to make friends, particularly on MySpace and the appellant played on that anxiety but she was not a naïve innocent. She had taken photographs of herself naked or partly naked and placed them on her computer, possibly sending at least one to the appellant. Her conversation reflected that she was "sexually aware and not inexperienced". She refused the appellant's attempt to make contact with her after 10 November 2008 and ceased using websites known to him.

[118] In January 2009 the appellant posted a recording of the incident constituting count 1, both conversation and video, on the internet and bragged triumphantly about it. Strangers began to pester and abuse her on the internet. On 8 April 2009 police went to her school and interviewed her. She asked for her student boyfriend to be present. At that stage she had told no-one what had happened. She had no adult support and she did not seem to have been told she was not obliged to participate. Thrice during the interview she told police she did not want to talk about it but they persisted. Only after sustained questioning did she reluctantly provide details. Whilst she had not given a victim impact statement, she undoubtedly felt humiliated and embarrassed at the time of the original incident (count 1) and when the video of it was posted on the internet (count 3). There was no suggestion that anyone who knew her was aware of the incident. Her internet acquaintances knew her only by her user name.

She seemed to have dealt with the situation sensibly and there was no evidence of any continuing distress. The police interview was seriously concerning. Police made no attempt to contact her parents or grandparents. They interviewed her at school in the context where ordinary discipline required her to answer their questions. Police initially misled her as to the subject matter of the proposed interview which continued without an adult support person. She was not told she was under no obligation to answer questions. The police ignored her statement that she did not want to talk about it and continued their questioning, pressing her for answers in front of her boyfriend. The police interview was the most humiliating and embarrassing part of her whole experience. This was an example of why victims of sex crimes are often reluctant to report them.

[119] Although the police interview would not have taken place but for the appellant's offending, he should not be held responsible for the unsatisfactory police investigation. There was no evidence of any long term harm to A arising from the appellant's conduct. Her demeanour in her videotaped cross-examination two years after the police interview showed a mature young woman able to deal with the questioning without distress.

[120] As to count 6, the judge found that the appellant knew that B lived with her parents in Brisbane and was a 14 year old high school student. There was no evidence of any particular vulnerabilities although she was sensitive to her mother finding out about the incident. She did not promote a sexualised image of herself on the internet and rejected the appellant's advances which she appeared to find more disgusting than embarrassing. She was embarrassed at having to be interviewed by police. There was no evidence of any psychological injury. This offence was an example of why naïve children, unable to deal with sexual predators, should have internet connection available only in some public part of the home rather than in the bedroom.

[121] The appellant had shown no contrition; continued to deny responsibility and was proud of his own cleverness in orchestrating the offending. He did not cooperate with the authorities in the administration of justice but rather asserted that someone took control of his computer and committed the offences, making the investigation unnecessarily long and complex. A sentence which would act as a deterrent to the appellant's re-offending was required. It was difficult to make a confident finding of rehabilitation to negate the risk of recidivism.

[122] The appellant was 19 when he offended and 24 at sentence. He had completed a diploma of business and was studying at university. References spoke of his devotion to his mother. His fiancée also provided a favourable reference but this must be weighed against her failure to give evidence at trial or sentence, "given that she must have received emails calculated to raise questions about [the appellant]".[250]

[123] After conviction the appellant's counsel asked for and was granted a lengthy adjournment to enable a psychiatric or psychological report to be prepared but no evidence of any psychological disability was subsequently tendered.

[124] The appellant had no criminal history but that was common in offences of this kind; its weight was diminished by considerations of general deterrence. Apart from the tendered references, there was little evidence of rehabilitative prospects. Although young and with time for rehabilitation to occur, the appellant's denial of responsibility and lack of remorse did not suggest these prospects were promising. The appellant's failure to give evidence on sentence prevented this issue from being explored. It

---

[250] Sentencing remarks, 7 lines 26-29.

was unfortunate that the appellant's imprisonment would impact adversely on his mother but that was not a mitigating factor here. Offences of this kind were widespread and difficult to detect, particularly as victims were reluctant to report them. The maximum penalties for counts 1, 2 and 6 were relatively high.

[125] His Honour was satisfied that the appellant intended A to do exactly what he procured her to do (count 1). The fact that he carried his intention to fruition was not to be taken into account in sentencing as a separate offence could have been brought under s 210(1)(b) *Criminal Code* (Qld) as it stood at that time. It may be that he decided to post the recording on the internet (count 3) only at a later time.

[126] His Honour considered that the most serious offending was count 6 because the appellant knew that B lived in Brisbane and intended to procure full sexual intercourse. This was so even though B was older than A and the appellant made little progress in executing his intention. Nevertheless count 1 was aggravated by the fact that the appellant procured A's conduct by threats rather than by gentle persuasion. Count 2 was of equal seriousness to count 1. Count 3, punishable by a 10 year maximum term of imprisonment rather than the 15 year maximum applicable to both counts 1 and 6, was less serious than count 6 because the potentially adverse consequences of publication on the internet to those who knew A did not occur.

[127] His Honour noted that the appellant had not re-offended during the four year period since the offences occurred.

[128] Cumulative sentences were appropriate for each of these three groups of offending. The total maximum sentence for these three groups would be 40 years imprisonment but this would be disproportionate and unwarranted. His Honour recited the sentences suggested by the prosecution. No sentence other than imprisonment was appropriate. The appellant's youth was an important factor. Ignoring questions of totality, his Honour would have imposed eight years imprisonment for count 6; with five years imprisonment for each of counts 1 and 2 concurrent with each other but cumulative on count 6; and a further five years cumulative imprisonment for count 3, producing a total of 18 years imprisonment. That would not be a crushing sentence as the appellant would be released on parole aged 33 and continue his life. It would however be more than his criminality warranted and should be moderated. The appropriate total sentence was 12 years imprisonment.

[129] Accordingly, his Honour sentenced the appellant to five years and four months imprisonment to commence immediately on count 6; three years and four months imprisonment on each of counts 1 and 2 concurrent with each other but to commence at the end of the sentence for count 6; three years and four months imprisonment to commence at the end of the sentences for counts 1 and 2; and 18 months imprisonment for count 4 and 12 months imprisonment on each of counts 5 and 7, all to commence immediately. His Honour fixed a non-parole period of six years and declared the 71 days of presentence custody to be time already served under the sentences imposed for counts 6, 4, 5 and 7.

[130] In determining whether the judge gave too much weight to the exacerbating features relied on by the prosecution and too little weight to the mitigating features relied on by the appellant so that the effective sentence of 12 years imprisonment with parole after six years was manifestly excessive, it is helpful to consider the few comparable cases for offending of this type. The two cases relied on by the parties both at sentence and in this appeal were *Tector* and *Asplund*.

*R v Tector*

[131] In *Tector*, the applicant was convicted after trial of three counts of using a carriage service to transmit a communication with the intention of procuring a person under 16 to engage in sexual activity under s 474.26(1) *Criminal Code* (Cth). Tector emailed a 12 year old boy inviting him to engage in sexual activity for money. He assumed a pseudonym and subsequently pursued the boy by repeatedly seeking his mobile telephone number and then phoning him. He was sentenced to 11 years imprisonment with a non-parole period of seven years. The maximum penalty was 15 years imprisonment.

[132] The New South Wales Court of Criminal Appeal held that a communication that expresses an intention to engage in sexual intercourse in contrast to a lesser form of sexual activity is a relevant circumstance in assessing the gravity of an offence of this kind. However, an email suggesting a lower level of sexual activity may be part of a grooming process so that the sentencing judge was not required to accept the terms of an email as a true reflection of the accused person's intended level of sexual activity. The judge was entitled to consider the nature of the proposed sexual activity as one of a number of factors to take into account in determining the objective seriousness of the offending and the extent of the criminality upon consideration of the relevant evidence. The maximum penalties were relevant.

[133] Pertinent circumstances in *Tector* included the offer of money as an inducement; his persistence in pursuing the boy; the fact that the child was well below 16; and the steps taken to preserve the offender's anonymity. These matters made the offence an objectively serious one.

[134] Tector gave evidence at trial denying the commission of the offences. He had previous relevant convictions. In 1995 he was convicted of two counts of indecent assault upon a child under 10 and sentenced to nine months imprisonment with a 15 month release subject to supervision. In 1998 he was convicted of homosexual intercourse with a male under 10 years and indecent assault (under age 10 years); act of indecency with a person under 16; and aggravated indecent assault and sentenced to an effective term of two years imprisonment.

[135] A psychological report was tendered which referred to Tector's unusually high level of insight into his problems suggesting favourable indicators for therapy. A relevant factor was the extent of the age differential between Tector, aged 54, and the 12 year old victim. He not only used a false name but also anonymous email addresses and public telephones. Nonetheless a sentence of 11 years imprisonment with a non-parole period of seven years was outside the appropriate range. The Court of Criminal Appeal allowed the appeal and substituted a head sentence of eight years imprisonment with a non-parole period of five years.

*R v Asplund*

[136] In *Asplund* the applicant was convicted after trial of two counts under s 474.27(1) *Criminal Code* (Cth) punishable by a maximum penalty of 12 years imprisonment. The first involved the use of the internet to transmit indecent material to a girl under 16 intending to procure her to engage in sexual activity with him. The second count was in similar terms but their communication was by mobile phone. He met the girl in an internet chat room and enquired about her sexual experience. After they exchanged mobile phone numbers, he phoned and texted her, sending a photograph of his erect penis and other messages suggestive of grooming for sexual activity. He was 61 and

believed she was 14 although she was only 13. He told her he was 27. He had no prior criminal history. He denied the offences and at trial attempted to blame his 15 year old son. There was evidence that he suffered from cognitive impairment and severe depression.

[137] He was sentenced to nine months imprisonment on count 1 and three years imprisonment on count 2, with the sentence structured so that it was effectively one of three years six months imprisonment with a non-parole period of one year and nine months.

[138] Both parties pursued appeals. The New South Wales Court of Criminal Appeal noted that such offences were frequently committed by persons of otherwise good character but they were hard to detect and general deterrence was a paramount consideration in sentencing. There was no suggestion Asplund's depressive condition contributed in any material way or reduced his moral culpability. Offences of this kind had the potential to do great damage to young people. The courts needed to protect children and young people by the imposition of appropriately severe sentences.

[139] Count 2, the more serious offence, involved more than 640 text and multi-media messages including an explicit sexual photo of his erect penis. He sought to arrange a meeting with her in an Adelaide hotel "for a spa, for sex and for a blow job".[251] His pursuit of her was unrelenting. He groomed her and inveigled her sense of dependence on him by gifting sums of money, well beyond the original purpose of providing credit for her mobile phone, the last of which was $2,500. He was separated from his wife and living with his 15 year old son.

[140] The Court of Criminal Appeal concluded that Asplund's offending was a determined and continuous history of communications designed to procure the victim to engage in sexual activity. It was an exacerbating feature that he forwarded money to the complainant; sent images of his penis and encouraged her to send him images of her naked.[252] The offending continued over a significant time and involved a high level of criminality placing it in the more serious category of offences. He pleaded not guilty, gave no indication of accepting responsibility for his offending, and sought to deflect responsibility to his son. The sentences failed to adequately reflect his criminality and his response to the offending; they were insufficient to adequately deter others. The court allowed the Crown appeal and substituted a sentence of three years imprisonment on the first count and four years cumulative imprisonment on the second count, that is, an effective term of seven years imprisonment, with a non-parole period of four years imprisonment.

**Conclusion on the application for leave to appeal against sentence**

[141] The learned sentencing judge rightly identified that he could not take into consideration the prosecutor's statement of opinion as to the appropriate sentence: *Barbaro v The Queen*.[253] His Honour also correctly identified the three separate groups of offending for which cumulative sentences could be imposed. However watching the video with which counts 1 and 3 are concerned, I respectfully disagree, however, with his Honour's assessment that the most serious offending was count 6. I consider the more serious of the offending was that in counts 1 and 3.

[142] It is true that the appellant intended in committing count 6 to procure this 14 year old girl to have sex with him. But unlike in *Tector* and *Asplund*, this appellant and B were

---

251 (2010) 216 A Crim R 48, 51.

252 Above, 61.

253 (2014) 88 ALJR 372.

relatively close in age (14 and 19) rather than 12 and 54 (Tector) or 61 and 13 (Asplund). Ordinarily, a court must give considerable weight to the immaturity of offenders, particularly youthful first offenders. That is principally because the youthful offender's prospects of rehabilitation with developing maturity are likely to be better than those of a mature recidivist. Here, the appellant also had many people who spoke well of him and who considered this conduct was out of character, a supportive family, and he is completing tertiary studies which should aid in his rehabilitation. Second, the detrimental impact on the victim may be less in offences of this kind when the offender and the victim are closer in age. Fortunately for the appellant and no doubt because of B's good sense, his criminal predatory efforts rendered him no success and the offending did not continue over a lengthy period. Whilst he did not disclose his full name, he used his unusual first name and sent photos of himself so that he was relatively easily traced by police and then identified by B. Count 6 was a much less serious example of offending of this type than in either *Asplund* or *Tector*. B always appeared in control of their online relationship. He did not threaten or cajole her into doing anything against her will. When she tired of his nuisance importuning, she stopped their online communication. She was not apparently detrimentally affected by the offending. But as count 6 concerned a different victim and discrete offending, the judge was entitled to impose a cumulative sentence.

[143] By contrast, count 1 was a concerning example of vicious, bullying power play over the internet. The appellant took advantage of a vulnerable young teenager, not quite 14 years old, and forced her to participate in humiliating sexual behaviour on webcam for his gratification. He knew she was upset, was not freely consenting, and that she complied only to avoid him damaging her valued computer and in an attempt to get more friends on MySpace. He made her persist in penetrating her body even when she said it was painful. He was boastfully and selfishly triumphant about his offending. His predatory and intimidating behaviour was likely to have a detrimental impact on her. He did not disclose his identity but he sent photos of himself and appeared on the webcam so that it was relatively easy for police to locate him and for A to identify him. Count 1 was a moderately serious example of an offence of this kind.

[144] As to count 3, the appellant deliberately posted on the internet the video recording of the complainant taken in the circumstances outlined in count 1. He showed no remorse or insight into the seriousness of his actions and their potential impact on A. The video remains on the internet and could have been viewed by countless others. The video has not yet been connected to A's real identity but there is no guarantee that this will not happen, even many years into the future. There is no evidence that A has been detrimentally impacted by the offending in count 1 but it has the potential to do so and will forever remain a concern for her.

[145] Counts 4, 5 and 7 were in themselves serious but they were not the most serious examples of offending of that kind. It is rightly common ground that the judge correctly imposed shorter concurrent sentences for these offences.

[146] The real issue is whether the effective sentence of 12 years imprisonment with a non-parole period of six years was manifestly excessive in light of the appellant's youth, prior good history, absence of any subsequent offending and efforts to rehabilitate. He does not have the benefit of cooperation with the administration of justice. The aggravating features were the number of serious offences concerning different victims and his complete lack of remorse for and insight into his conduct. Despite the number of offences committed against different victims, the appellant's youthful immaturity, prior and subsequent good history and his relative closeness in age to A and B place him in a very different category to both Tector and Asplund.

[147] Although not the only appropriate sentencing approach, I would not interfere with the primary judge's imposition of two sets of cumulative sentences. It is uncontroversial that cumulative sentences may warrant moderation under the totality principle explained in *Mill v The Queen*[254]. The sentence imposed, however, was in the circumstances crushing and manifestly excessive so that this Court should resentence the appellant. After considering the competing aggravating and mitigating features discussed above, I consider an effective total sentence of eight years imprisonment with a non-parole period of four years should be substituted. This remains a severe penalty for any 19 year old first offender of this kind. It stands as a firm deterrent to him and others who would use the internet to criminally prey on young people, whilst still reflecting his youthfulness and supporting his rehabilitative prospects.

[148] The orders I propose are:

1. The appeal against conviction is dismissed.

2. Grant the application for leave to appeal.

3. Allow the appeal against sentence in respect of counts 1, 2, 3 and 6.

4. Set aside the sentences imposed below on counts 1, 2, 3 and 6 and instead order that:

   (i) on each of counts 1 and 2 the appellant is imprisoned for three years to commence on 20 August 2013;

   (ii) on count 3 the appellant is imprisoned for three years to commence at the end of the sentences for counts 1 and 2; and

   (iii) on count 6 the appellant is imprisoned for two years to commence at the end of the sentence for count 3.

5. The declaration that the presentence custody be time already served under the sentences imposed for counts 6, 4, 5 and 7 is vacated.

6. Instead it is declared that pursuant to s 159A *Penalties and Sentences Act* 1992 (Qld) the appellant was held in presentence custody for 71 days between 8 April 2009 and 9 April 2009, and 12 June 2013 and 20 August 2013. This Court declares the whole of those terms are imprisonment already served under the sentences imposed for counts 1, 2, 4, 5 and 7.

7. In respect of all other counts a non-parole period of four years is fixed.

8. The Court directs that an explanation of the purpose and consequences of fixing that non-parole period be handed to the appellant in writing forthwith and a copy thereof marked "Explanation" for identification.

9. The sentence imposed below is otherwise confirmed.

[149] **FRASER JA:** I have had the advantage of reading the reasons for judgment of the President. I agree with those reasons and with the orders proposed by her Honour.

[150] **ALAN WILSON J:** I agree with Margaret McMurdo P's reasons, and with the orders her Honour proposes.

---

254 (1988) 166 CLR 59.