Neutral Citation Number: [2017] EWCA Crim 2163

Case No: 201702412 A3 and 201702442 A3

IN THE COURT OF APPEAL (CRIMINAL DIVISION)
ON APPEAL FROM LEWES CROWN COURT (PARSONS)
HHJ Niblett
S20170166
ON APPEAL FROM WORCESTER CROWN COURT (MORGAN)
HHJ Pearce-Higgins
T20170108

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 20/12/2017

Before :

LORD JUSTICE GROSS
MR JUSTICE TEARE
and
MR JUSTICE KERR

- -

Between :

	REGINA	**Respondent**
	- and -	
	HAYDEN GRAEME PARSONS **- and -** **REGINA** **- and -** **STUART JAMES MORGAN**	**Appellant** **Respondent** **Appellant**

(Transcript of the Handed Down Judgment.
Copies of this transcript are available from:
WordWave International Limited
A Merrill Communications Company
165 Fleet Street, London EC4A 2DY
Tel No: 020 7414 1400, Fax No: 020 7831 8838
Official Shorthand Writers to the Court)

Simon Heptonstall (instructed by **Crown Prosecution Service, Appeals and Review Unit**) for the **Crown**
Paul Luttman (instructed by **David Street & Company**) for the **Appellant Parsons**
Mark Thompson (instructed by **Coulson Read Lewis Solicitors)** for the **Appellant Morgan**

Hearing date : 23 November, 2017

Judgment
As Approved by the Court

Lord Justice Gross : INTRODUCTION

1. This is the judgment of the Court to which we have all contributed.

2. The two separate cases before the Court have been listed together. Both concern prohibitions on internet access and use imposed by *Sexual Harm Prevention Orders* ("SHPOs"). The question arises as to whether the guidance given in *R v Smith* [2011] EWCA Crim 1772; [2012] 1 WLR 1316, the leading case as to restrictions on internet access and use under the predecessor *Sexual Offences Protection Orders* ("SOPOs"), requires adaptation in the light of developments in technology and everyday life. A further question is whether the decision in *R v McLellan and Bingley* [2017] EWCA Crim 1464 applies to SHPOs, *mutatis mutandis*, as well as to SOPOs.

3. The legislation governing SHPOs is found in ss. 103A and following of the *Sexual Offences Act 2003* ("the Act"). Whereas a SOPO could only be imposed where necessary to guard against a risk of "*serious*" sexual harm, it is apparent that a SHPO can be imposed where necessary to protect "….the public or any particular members of the public" from sexual harm, *simpliciter*: s.103A(2)(b)(i). This change has already been reflected in *R v NC* [2016] EWCA Crim 1448, amending the questions posed in *Smith* (at [8]) to be considered by a Court when considering the imposition of a SHPO. As formulated in *NC*, at [9], those questions are now as follows:

> " (i) is the making of an order necessary to protect the public from sexual harm through the commission of scheduled offences?; (ii) if some order is necessary, are the terms imposed nevertheless oppressive?; (iii) overall, are the terms proportionate? "

4. A further change under the SHPO regime is that "child" now means a person under 18, rather than a person under 16: s.103B(1).

GENERAL CONSIDERATIONS

5. At the outset, we underline the following:

   i) First, as with SOPOs, no order should be made by way of SHPO unless *necessary* to protect the public from sexual harm as set out in the statutory language. If an order is necessary, then the prohibitions imposed must be *effective*; if not, the statutory purpose will not be achieved.

   ii) Secondly and equally, any SHPO prohibitions imposed must be *clear* and *realistic*. They must be readily capable of simple compliance and enforcement. It is to be remembered that breach of a prohibition constitutes a criminal offence punishable by imprisonment.

iii) Thirdly, as re-stated by *NC* (*supra*), none of the SHPO terms must be oppressive and, overall, the terms must be proportionate.

iv) Fourthly, any SHPO must be tailored to the facts. There is no one size that fits all factual circumstances.

6. The present matters raise individual questions of wider importance going to:

i) Blanket bans on internet access and use;

ii) Where children are concerned, whether the prohibition should extend to those under 18 or those under 16 ("the question of age");

iii) Risk management monitoring software;

iv) "Cloud storage";

v) Encryption software;

vi) The application of the decision in *McLellan and Bingley* to SHPOs.

7. We take each in turn.

8. *(1) Blanket bans on internet access and use:* While eschewing any attempt to lay down a rule for all cases (see [20]), the Court in *Smith* made plain its disapproval in general of such blanket bans. Hughes LJ (as he then was), said this (at [20] (i)):

> " A blanket prohibition on computer use or Internet access is impermissible. It is disproportionate because it restricts the defendant in the use of what is nowadays an essential part of everyday living for a large proportion of the public, as well as a requirement of much employment….."

9. We respectfully agree, adding only that the importance of the internet for everyday living has increased considerably even since the decision in *Smith*. We accept the broad thrust of Mr Thompson's submission on behalf of *Morgan*, namely, that the need for an individual to be able to access the internet and to possess devices capable of accessing the internet, has become "the established norm". The internet is now an integral part of social life, of commercial transactions and is very much encouraged in dealings between an individual and government departments or local authorities. The massive expansion of social media further highlights developments in this regard.

10. While we agree with Mr Heptonstall for the *Crown* and would be unwilling to say that a blanket ban on internet access and use can *"never"* be justified, we cannot envisage that such a prohibition would be appropriate in anything other than the most exceptional

cases. In all other cases, a blanket ban would be unrealistic, oppressive and disproportionate – cutting off the offender from too much of everyday, legitimate living.

11. *(2) The question of age:* We have already drawn attention to the fact that the SHPO regime defines a child as a person under 18: s.103B(1) of the Act. Although, at first blush, this may seem surprising because much sexual offences legislation is focused on prohibitions in respect of activity or relationships with those under 16, that is not always so and some legislation is directed to the protection of those under 18. See the discussion in *Smith*, at [21].

12. Two further examples suffice. First, for the purposes of the offence of making an indecent photograph of a child, contrary to s.1(1) of the *Protection of Children Act 1978* ("the 1978 Act"), a child is defined (by s.7(6) of the 1978 Act) as a person under the age of 18. Secondly, the same definition of a child is adopted in respect of the offence of possession of an indecent photograph of a child, contrary to s.160(1) of the *Criminal Justice Act 1988* ("the 1988 Act") – albeit that s.160A of that Act provides a specific defence for images of a child over 16 with whom the defendant was in a marriage, civil partnership or with whom the defendant was living together as part of an enduring family relationship.

13. Against this background, we can see no objection *in principle* to a prohibition geared to those under 18 - a matter plainly contemplated by the Act in respect of SHPOs. That said, we can readily understand that the facts of an individual case might point towards confining prohibitions to children under 16 (for the reasons given in *Smith,* at [21]).

14. *(3) Risk management monitoring software:* Under this heading and in respect of the discussion of "cloud storage" and encryption software (below), we acknowledge our gratitude to Mr Caithness, an expert instructed following prompting by the Court and who produced, at short notice, effectively agreed reports of the 21st and 24th November, 2017.

15. Mr Caithness took "risk management monitoring software" to mean:

> " …software which monitors the use of a computing device (including but not limited to: PCs, smart phones and tablets) for prohibited behaviours such as:
>
> 4.1 the installation of restricted software
>
> 4.2 access to prohibited resources (whether stored locally on the device or on the web)
>
> 4.3 attempts to change the device's software settings or hardware configuration"

The software may simply record that the prohibited action took place or it may block the activity altogether.

16. As explained by Mr Caithness, such software is most widely used within businesses to mitigate the risks posed by employee misconduct – which may damage the company's reputation (e.g., by accessing pornographic websites) or result in a leak of the company's intellectual property. In a corporate environment, these software solutions would usually be controlled centrally by the IT department. Mr Caithness went on to add that monitoring software could also be used at home, with a view (for example) to preventing children from accessing inappropriate and pornographic content.

17. Mr Caithness added the following observations as to risk management monitoring software:

> "8. Installing these solutions onto each device…to be monitored generally requires either that the device is under administrative control of a corporate network or that physical and administrative access is provided to the device in question. It will also be required that the monitoring software to be installed is compatible with the hardware and operating system.
>
> 9. These software products should be kept up to date and as new versions of operating systems are released for the monitored devices, the monitoring software should be tested for compatibility to ensure that monitoring continues unabated. This additional work creates an administrative overhead for these solutions."

18. Given the administrative burdens thus imposed and the realities of Police time and resource constraints, we would be concerned about a prohibition which assumed that a Police force would necessarily wish to insist on the installation of such software or which made the use of the device contingent on the approval by the Police force of software already installed on it; the latter prohibition could unintentionally (and by the backdoor) become a ban on usage of the device.

19. Instead and without dissent from the parties, we would prefer to approach this topic as follows. The trigger should be notification by the offender to the Police of his acquisition of a computer or device capable of accessing the internet; the Police cannot be expected to know otherwise. The device should have the capacity to retain and display the history of internet use and the offender should be prohibited from deleting such history. The device should be made available immediately on request for inspection by a Police officer (or employee) and the offender should be required to allow any such person to install risk management software if they so choose. The offender should further be prohibited from interfering with or bypassing the normal running of any such software. For our part, this is a workable and proportionate solution to the questions raised by risk management monitoring software. It is reflected in the agreed form of words ultimately adopted in the orders in both *Morgan* and *Parsons*, set out below.

20. *(4) "Cloud storage":* Mr Caithness defined "cloud storage" as "a service which allows a user of a computing device (including, but not limited to: PCs, smart phones and tablets) to store data and files in a remote location accessible over the internet." A broader definition of cloud storage could also apply to any service where storage was

offered on the internet – so that webmail could be regarded as a type of cloud storage. Cloud storage furnishes various benefits, which need not detain us here.

21. As further explained by Mr Caithness, access to cloud storage can take place using an application ("app"), through use of a web browser or via direct integration with an operating system – or a combination of these methods.

22. Examples of services offering and marketing themselves as cloud storage solutions, include (but are not limited to) Dropbox, Microsoft OneDrive, Google Drive and Apple iCloud.

23. Mr Caithness saw cloud storage as "practically ubiquitous" when considering computing devices currently available on the market. As he put it, this was due to access to cloud storage being a "built-in or pre-installed feature on the prevailing Desktop PC and Smartphone operating systems", including Windows 10, Apple's MacOS (desktop) and IOS (smartphone) and Google's Android smartphone operating system. It followed that for users following the default installation or set-up options for these operating systems, "logging into, or signing up to one these cloud storage services is implicit in the process". Accordingly and unless the user specifically configured the device not to do so, "use of the pre-installed cloud services will take place transparently (and in many cases preferentially to the use of local storage such as an internal hard drive….".

24. It is against this background that any prohibition on cloud storage falls to be considered. As expressed by Mr Caithness:

> "20. Prohibiting the use of cloud storage services would require specific configuration of a computing device in the first instance to ensure that the default and automatic access offered by an operating system was not enabled. Care would also need to be taken that updates to the devices did not re-enable access to these services.
>
> 21. The primary impact on a user prohibited from using these services would be that storage of the data and files under their control must be managed locally by said user..…... There is also a burden upon a user to maintain a configuration on current or new computing devices which disables the automatic use of these services. "

25. Accordingly, the vice against which a prohibition should be targeted is not the default or automatic use of cloud storage, "practically ubiquitous" in the devices available to consumers today. That would be altogether too blunt an approach. A prohibition too widely worded would not only be unnecessary but could readily be a trap for the unwary user of (for example) a smartphone in mass usage. The vice is instead the deliberate installation of a remote storage facility, specifically installed by an offender without notice to the police and which would not be apparent from the device he is using – and not intrinsic to the operation of any such device. As will be seen, this more targeted approach, together with a notification requirement, is reflected in the orders set out below.

26. *(5) Encryption software:* Mr Caithness defines encryption as "the process of encoding data or information so that it should only be able to be read or accessed by an authorised party who has access to the 'key' to the data."

27. Once again, any prohibition on encryption software falls to be considered against the reality of the devices available to consumers for everyday legitimate use. That reality is expanded upon by Mr Caithness, as follows:

> "26. Anyone interacting with a modern computer system (including, but not limited to: PCs, smart phones and tablets) will likely be making use of encryption in one form or another for a significant period of that usage. Some examples of this include…..:
>
> 26.1 Access and communication with websites. Where the address of a website begins with 'https', encrypted communication shall be used by the browser…..
>
> 26.2 Many smartphones and desktop computers implement encryption of the data stored by the user. In the case of Apple iPhones, for example, this encrypted storage is mandatory and cannot be disabled….
>
> 26.3 Communication applications (apps) for text, voice and video calls widely make use of encryption to prevent eavesdropping on communications. Many of the best-known communication applications make use of encryption for communications, for example: Skype….Whatsapp….
>
> ….
>
> 27. Beyond its use in personal computing devices, encryption is used in other aspects of everyday life for example:
>
> 27.1 Mobile phone calls……
>
> 27.2 Subscription TV (such as 'Sky')….
>
> 28. Prohibiting the use of all encryption would have a great impact on the ability of a person to operate within a digital landscape, especially where data must be transmitted or received. Use of the internet would become limited and insecure…. Specific provisions would have to be made to ensure that a system did not accidentally 'stray' onto a secure website……
>
> 29. Making use of mobile communication would also be made problematic….."

28. As with cloud storage, it is readily apparent that a prohibition here must be fashioned in such a manner as neither to be a blunt instrument nor a trap for the unwary (simply using the default setting of a device in everyday legitimate use). A suitable prohibition must instead be targeted - and aimed at the installation of encryption or wiping software on any device other than that which is intrinsic to its operation. That is the approach

adopted in the orders set out below.

29. *(6) The application of the decision in McLellan and Bingley to SHPOs:* Extended discussion is unnecessary. We need say no more than that the observations in *McLellan and Bingley* (at [51] *et seq*) as to the demarcation between appeals to this Court and applications to vary or discharge SOPOs, apply equally, *mutatis mutandis*, to SHPOs. For completeness, the Crown Court's jurisdiction to vary or discharge a SHPO is furnished by s.103E of the Act.

30. *(7) Pulling the threads together:* With respect, the guidance given by *Smith* (esp., at [18] and following) remains, in general, essentially sound and should continue to be followed. However, as has been seen, in certain specific areas, developments in technology and changes in everyday living call for an adapted and targeted approach. This is so especially in relation to risk management monitoring software, cloud storage and encryption software. Moreover, it is necessary to take account of the SHPO legislation defining "child" as a person under 18 (rather than under 16).

31. With these views in mind, we turn to the individual appeals.

STUART JAMES MORGAN

Introduction

32. On 20th April 2017, in the Crown Court at Worcester before His Honour Judge Cartwright, the applicant pleaded guilty to five counts alleging the following offences: counts 1-3, making indecent photographs of a child contrary to section 1(1) (a) of the Protection of Children Act 1978; count 4, possession of an extreme pornographic image contrary to section 63(1) of the Criminal Justice and Immigration Act 2008; and count 5, possession of a prohibited image of a child contrary to section 62(1) and 66(2) of the Coroners and Justice Act 2009.

33. On 12th May 2017, before His Honour Judge Pearce-Higgins QC, the applicant was sentenced on each of counts 1-5, concurrently, to a community order for 36 months with a requirement to participate in the Community Sex Offender programme.

34. A SHPO for a period of 5 years was made pursuant to s. 103 of the Act, containing the following terms:

> "1. The Defendant is prohibited from accessing the internet or
>
> 2. Possessing any device capable of accessing the internet
>
> save in a public place, public library or under the supervision of a Police Officer or a Probation Officer.
>
> ……"

35. There was a Victim Surcharge order in the sum of £85. Forfeiture and destruction was ordered of the items the police had seized.

36. Having been convicted of an offence listed in Schedule 3 of the Act, the applicant was required to comply with the provisions of Part 2 of the Act (notification to the police) for 5 years.

37. The applicant applies for leave to appeal against sentence. His application has been referred to the full court by the Registrar. We give leave and refer to him hereafter as "the appellant".

The facts

38. The facts are as follows.

39. The appellant is now aged 49. He is of previous good character.

40. On 10th May 2017, police entered the appellant's address with a warrant to search. Various items of computer and computer-related equipment were seized. He told the officers, *"I've been deleting some stuff I've found from emule"* (a peer-to-peer sharing network).

41. Later that day he was interviewed. He explained that he had a lifetime's collection of pornography which he obtained from the network and stored on his hard drives. He viewed pornography on a daily basis. Over time, he had accidentally downloaded indecent images of children, some of which he had viewed and some he had deleted.

42. Following an analysis of the items seized from his address – consisting of computers, three hard drives, and a box of discs - he was interviewed again. He accepted that he had copied indecent images and videos of children onto CDs and DVDs, although he thought he had since destroyed them by copying over the indecent material.

43. The indictment covered the period from 2002 to 2017. The material involved 172 category A moving images of a child (count 1), 7 category B moving images of a child (count 2); 2 category C moving images of a child (count 3), 144 extreme images and 602 extreme moving images portraying a person performing an act of intercourse or oral sex with an animal (count 4) and one prohibited image (namely an indecent cartoon image of a child) (Count 5).

44. It was noted that there was an attempt to dispose of or conceal the images and evidence of systematic storage and organisation of the collection.

45. There was a pre-sentence report, stating that the appellant admitted that having initially encountered indecent images and movies involving children by accident, whilst searching for adult pornography, he thereafter searched for, downloaded and stored

material involving children using the "emule" "peer to peer" internet sharing network. He accepted that he gained sexual gratification from such images and also from images involving animals.

46. He was assessed as being highly sexually preoccupied. He only worked two days a week and spent the rest of his time watching films and pornography. His lifestyle was isolated and revolved around his computer.

47. Even though he had viewed images of children as young as three years, his preference was for children aged between 9 and 13 years. He appeared detached and unemotional about the effect his offending behaviour might have on others.

48. He was assessed as posing a medium risk of re-offending. He was considered as presenting a high risk of harm to children because his offending behaviour supported an exploitative industry.

Sentence

49. Sentencing the appellant, the Judge gave full credit for his guilty plea. He commented that for many years, the appellant's life had been dominated by online activity, living in an unreal world on the internet.

50. Having read the pre-sentence report, the Judge considered that the best way to address the appellant's problems, and to protect society in the future, was to impose a 36 months' community order, with a requirement to attend the Community Sex Offenders programme as directed by the responsible probation officer, on each count concurrently.

51. In relation to the SHPO, the Judge's view was that the appellant was unlikely to make much of a recovery until he started living a real life rather than an online life.

52. To achieve this, the Judge considered he should be prevented from using or having access to a computer except in a public place such as a public library or under the supervision of the police or a probation officer as part of the community programme.

53. It may be noted that the Judge's approach in this regard was unsupported by the submissions of either counsel. The prosecution, while seeking a SHPO, highlighted that the authorities were against the making of a blanket ban on accessing the internet. Defence counsel, in sustained submissions, contended that such a "blanket prohibition" on computer use or internet access was neither permitted nor proportionate; he relied, *inter alia*, on *Smith (supra)*.

54. The Judge accepted that authority appeared to be against a blanket prohibition on use of any computer. Nevertheless, he observed that every case was different. In this case, it was necessary to remove the temptation if there was to be any prospect of significant rehabilitation. Draconian measures were necessary. The Judge agreed that the order would restrict the appellant, but said it was for his own benefit and that of society. He

drew an analogy with an alcoholic and emphasised the appellant's lifestyle.

Discussion and conclusions

55. The grounds of appeal focused entirely on the blanket prohibition in the SHPO on the appellant's use of the internet. We should note that, despite the exception for a public place, public library or the supervision of a Police or probation officer, we entertain no doubt that the SHPO passed did entail an effective blanket prohibition on the appellant's access to and use of the internet. By way of simple example, the exception confines the appellant to sending a simple, legitimate e-mail either in a public place or under the supervision of a Police or probation officer.

56. Notwithstanding Mr Heptonstall's valiant attempt to defend the SHPO as passed, we are satisfied that it cannot stand. The present case is not, in any sense, a truly exceptional case. The blanket ban was well-intentioned but it is unrealistic, oppressive and disproportionate. That would have been the case at the time of *Smith;* for the reasons already given, it is all the more so now.

57. We accordingly quash the SHPO imposed on the appellant (*Morgan*) and substitute a SHPO, for the same period of time, in the terms set out below. It may be noted that no questions of prohibition of contact arose in the case of this appellant.

58. The terms of the substituted SHPO are as follows:

> " The Defendant is prohibited from:
>
> (1) Using any computer or device capable of accessing the internet unless:
>
> (a) He has notified the police VISOR team within 3 days of the acquisition of any such device;
>
> (b) It has the capacity to retain and display the history of internet use, and he does not delete such history;
>
> (c) He makes the device immediately available on request for inspection by a Police officer, or police staff employee, and he allows such person to install risk management monitoring software if they so choose.
>
> This prohibition shall not apply to a computer at his place of work, Job Centre Plus, Public Library, educational establishment or other such place, provided that in relation to his place of work, within 3 days of him commencing use of such a computer, he notifies the police VISOR team of this use.
>
> (2) Interfering with or bypassing the normal running of any such computer monitoring software.
>
> (3) Using or activating any function of any software which prevents a computer or device from retaining and/or

displaying the history of internet use, for example using 'incognito' mode or private browsing.

(4) Using any 'cloud' or similar remote storage media capable of storing digital images (other than that which is intrinsic to the operation of the device) unless, within 3 days of the creation of an account for such storage, he notifies the police of that activity, and provides access to such storage on request for inspection by a police officer or police staff employee.

(5) Possessing any device capable of storing digital images (moving or still) unless he provides access to such storage on request for inspection by a police officer or police staff employee.

(6) Installing any encryption or wiping software on any device other than that which is intrinsic to the operation of the device."

59. The diligence of the Court of Appeal Office, for which we are, as always, most grateful, has also brought to light two aspects in which the sentence passed was or may have been unlawful:

i) As not all the offending commenced after the 1st October, 2012, the imposition of the Victim Surcharge Order of £85 was unlawful. We quash the Victim Surcharge Order.

ii) With regard to the Community Order, the difficulty relates to the Programme Requirement if and insofar as the offending under counts 1 - 3 pre-dated the coming into force of the relevant provisions of the *Criminal Justice Act 2003*, on 4th April, 2005. The simplest solution which makes no practical difference to the outcome is to quash the sentence on counts 1-3 and impose no separate penalty. We do so. The Community Order imposed in respect of counts 4 and 5, remains in force and unaffected.

60. To the extent indicated, the appeal of *Morgan* is allowed.

HAYDEN GRAEME PARSONS

Introduction

61. The appellant is aged 31 and on 12 April 2017 pleaded guilty before the magistrates to one count of making indecent photographs of a child and to one count of possessing a class B drug. He was committed to the Crown Court for sentence and, on 10 May 2017, he was sentenced by HHJ Niblett, sitting in the Crown Court at Lewes, to 12 months' imprisonment on the first count, suspended for 24 months, and to one month's imprisonment, consecutive, on the second count, also suspended for 24 months. In

addition, there were supervision and programme requirements and the appellant was made subject to a SHPO for 10 years. Still further, a Victim Surcharge of £115 was imposed. The appellant, who has previous convictions but none relevant to the present offending, appeals to this Court by leave of the Single Judge.

62. It is the terms of the SHPO which are the subject of this appeal. The prohibitions were as follows:

> " (1) Living in the same household as any child under the age of 18 or entering or remaining in any household where a child under 18 is present unless with the express approval of Social Services for the area in which he resides.
>
> (2) Having any unsupervised contact or communication of any kind with any child under the age of 18 other than:
>
> (i) such as is inadvertent and not reasonably avoidable in the course of daily life, or
>
> (ii) with the consent of the child's parent or guardian (who has knowledge of his convictions) and with the express approval of Social Services for the area.
>
> (3) Using any device capable of accessing the internet unles:
>
> (i) It has the capacity to retain and display the history of internet use, and
>
> (ii) He makes the device available on request for inspection by a police officer, and
>
> (iii) Using any computer or other electronic device capable of accessing the internet unless the device is installed with risk management monitoring software approved by the police force responsible for monitoring the Defendant, save for computer(s) at the Defendant's place of work or computer(s) at the Defendant's local library which must be notified and approved by the risk management officers responsible for monitoring the Defendant prior to use.
>
> (4) Utilising any 'cloud' or similar remote storage media unless he declares such use (provides account details) to the Public Protection Unit of the area in which he resides and provides access to it on request for inspection by a police officer.
>
> (5) Deleting such internet history on any device as detailed above.
>
> (6) Possessing any device capable of storing digital images unless he makes it available on request for inspection by a police officer.
>
> (7) Purchasing, downloading, obtaining, owning or using any encryption or wiping software and possessing any media or other storage device which is encrypted. If any device is password

protected, passwords must be made available to the Public Protection Officer or any officer acting in the course of their duty. Any device authorised must be made available for inspection by the Public Protection Officer or an officer acting in the course of their duty upon request."

Before us, objection was taken to prohibitions 1, 2, 3(iii), 4 and 7. There was no issue as to prohibitions 3(i), (ii), 5 and 6.

The facts

63. The facts of the offences to which the appellant pleaded guilty were these. On 5 December 2016 police officers attended at the appellant's home address and seized a laptop and a mobile phone. They also found 8 grams of herbal cannabis.

64. On the mobile phone were found 27 category A images, 48 category B images and 2161 category C images. There was a mix of still photographs and moving images. The forensic report shows that examples of the images in category A involved female children aged between 3 and 10 years old, that examples of the images in category B involved female children aged between 3 and 10 and that examples of the images in category C involved female children aged between 3 and 14. The vast majority depicted female children under 10. The forensic report shows the presence of search terms which indicated searching for the images in question and also websites which could be used for online chats with young children. The image files appear to have been created between 31 March 2016 and 22 November 2016.

65. On the laptop were found 39 category A images, 52 category B images and 1879 category C images. There were a mix of still photographs and moving images, The forensic report shows that examples of the images in category A involved female children aged between 4 and 8 years old, that examples of the images in category B involved female children aged between 5 and 8 and that examples of the images in category C involved female children aged 7. The forensic report shows the presence of search terms which indicated searching for the images in question and also websites which could be used for searching for such images. The image files appear to have been created between 29 March 2013 and 13 March 2015.

66. The only examples of male children were found on the phone. There were amongst the samples of category B images an image of male child, aged 15-16 (with a female child aged 4-5) and an image of a male child aged 8-10 (with a female child aged 6-8).

Sentence

67. Passing sentence, the Judge stated that it needed to be brought home to the appellant, by a programme of therapeutic treatment, that every one of the images was of a real child being abused. A custodial sentence was to be imposed but the Judge was satisfied that it could and should be suspended.

68. As to the SHPO, all the prohibitions were necessary to protect young children from further harm from the appellant, albeit he did not harm them directly.

Discussion and conclusions

69. We were grateful to both Mr Luttman, for the appellant and Mr Heptonstall, for the Crown, for their respective submissions on the prohibitions in dispute (namely, 1, 2, 3(iii), 4 and 7). We can state our views relatively shortly.

70. *(I) Prohibitions 1 and 2:* Three matters were here in issue: (1) Whether any prohibitions on contact were justified? (2) If so, whether contact should be prohibited in respect only of female children rather than all children? (3) Whether any such prohibition should relate to children under the age of 18 or whether the prohibition should be limited to children under the age of 16?

71. *(1) Prohibitions on contact:* As explained in *Smith,* at [22] – [23], it is "not legitimate to impose multiple prohibitions on a defendant just in case he commits a different kind of offence". There must be "an identifiable risk of contact offences" before prohibitions on contact can be justified.

72. The present case is close to the borderline. The appellant's relevant offending comprised making indecent photographs of children. That said, the facts (set out above) disclosed his browsing or searching for websites which could be used for online chats with young children. Such searches could have been a first step towards the commission of predatory offending, seeking out children for sexual purposes. In the circumstances, we are persuaded that the inclusion of some contact prohibitions in the SHPO was necessary and proportionate.

73. *(2) All children or only female children?* The gravamen of the appellant's offending related to female children. On the material before us, the images of male children were incidental to the appellant's interest in female children. Accordingly, we are of the view that prohibitions 1 and 2 should be confined to female children.

74. *(3) Female children under the age of 18 or under the age of 16?* Given the particular nature of the appellant's offending and the definition of "child" now contained in the SHPO legislation, we are not persuaded to interfere with the prohibition restricting contact in respect of (female) children under 18.

75. *(II) Prohibitions 3(iii), 4 and 7:* For reasons which will already be apparent from our earlier and more general discussion, these prohibitions require amendment. With regard to prohibition 3(iii), we are concerned about the administrative burdens which it imposes and the unintended consequences which might flow therefrom. As drafted, both prohibitions 4 and 7 are too blunt and create a trap for the unwary user, in a manner going well beyond the mischief intended.

76. *(III) The substituted SHPO:* We accordingly quash the SHPO as imposed on the appellant (*Parsons*) and substitute for the same period of time (10 years) a SHPO in the

following terms (which are the same as those in *Morgan,* above, save for the addition of the contact prohibitions):

" The Defendant is prohibited from:

(1) Living in the same household as any female child under the age of 18 or entering or remaining in any household where a female child under 18 is present unless with the express approval of Social Services for the area in which he resides.

(2) Having any unsupervised contact or communication of any kind with any female child under the age of 18 other than:

(i) such as is inadvertent and not reasonably avoidable in the course of daily life, or

(ii) with the consent of the child's parent or guardian (who has knowledge of his convictions) and with the express approval of Social Services for the area.

(3) Using any computer or device capable of accessing the internet unless:

(a) He has notified the police VISOR team within 3 days of the acquisition of any such device;

(b) It has the capacity to retain and display the history of internet use, and he does not delete such history;

(c) He makes the device immediately available on request for inspection by a Police officer, or police staff employee, and he allows such person to install risk management monitoring software if they so choose.

This prohibition shall not apply to a computer at his place of work, Job Centre Plus, Public Library, educational establishment or other such place, provided that in relation to his place of work, within 3 days of him commencing use of such a computer, he notifies the police VISOR team of this use.

(4) Interfering with or bypassing the normal running of any such computer monitoring software.

(5) Using or activating any function of any software which prevents a computer or device from retaining and/or displaying the history of internet use, for example using 'incognito' mode or private browsing.

(6) Using any 'cloud' or similar remote storage media capable of storing digital images (other than that which is intrinsic to the operation of the device) unless, within 3 days of the creation of an account for such storage, he

notifies the police of that activity, and provides access to such storage on request for inspection by a police officer or police staff employee.

(7) Possessing any device capable of storing digital images (moving or still) unless he provides access to such storage on request for inspection by a police officer or police staff employee.

(8) Installing any encryption or wiping software on any device other than that which is intrinsic to the operation of the device."

77. *(IV) Unlawful sentence:* Once again, we are indebted to the Criminal Appeal Office. It is unnecessary to say more than that having regard to the dates of the offending, the correct Victim Surcharge was £100 rather than £115. We quash the order for the payment of £115 and substitute an order for the payment of £100.

78. In the various respects and to the extent indicated, we allow the appeal of *Parsons*.