The Internet: Access Denied Controlled!

WALDEN, I; Wasik, M

The Internet: Access ~~Denied~~ Controlled!

By

Ian Walden and Martin Wasik

Reprinted from **Criminal Law Review**
Issue 5, 2011

Sweet & Maxwell
100 Avenue Road
Swiss Cottage
London
NW3 3PF
(Law Publishers)

SWEET & MAXWELL

The Internet: Access ~~Denied~~ Controlled!

Ian Walden

Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary, University of London

Martin Wasik

Professor of Criminal Justice, Keele University

Access restrictions; Enforcement; Internet; Offenders; Sexual offences prevention orders

Introduction

Access to the internet is increasingly recognised as being "as indispensable as electricity, gas or water".[1] As we have become dependent on the internet for our work, rest and play, constraints placed over our access to and use of this resource have become politically charged. The Digital Economy Act 2010 continues to be the subject of much heated debate over provisions that could allow the suspension of a subscriber's internet access service for reasons of copyright infringement[2]; while, conversely, the Coalition Government has recently announced its intention to drop internet bans in "control orders" in favour of more limited communication restrictions under the new regime.[3] This article considers this general issue, focusing upon the use of sexual offences prevention orders which frequently contain provisions prohibiting or restricting access to the internet.

Obviously, where a person has used the internet to commit a criminal offence, the courts may impose a sentence to punish and deter the individual from continuing to commit such conduct. However, as a supplement to the sentence, the court may issue a preventive order imposing one or more controls on the future conduct of the defendant.[4] Controls may be placed on the activities he engages in, the places he goes to, or the things he has. In a traditional environment such an order may, for example, prohibit the perpetrator from leaving or entering a designated geographical area, restrict his movements, or prevent him from holding a particular job or from working in a particular environment. In a cybercrime context, an

[1] "Super-fast broadband for the whole country is vital to future prosperity", former Prime Minister Gordon Brown, *Daily Telegraph*, January 8, 2010.

[2] Communications Act 2003 s.124G, inserted by the Digital Economy Act 2010 s.9. A failure to comply with a technical obligation would be subject to enforcement by Ofcom as a contravention of a condition under ss.94–96, which could result in a maximum fine of £250,000 (s.124L).

[3] See Home Office, *Review of Counter-Terrorism and Security Powers — Review Findings and Recommendations*, Cm.8004, January 2011, at p.42, para.26, vii.

[4] Such conditions may also form part of a conditional bail, where there are specific concerns that a suspect may engage in inappropriate behaviour. For example, Gary McKinnon, the alleged hacker contesting extradition to the United States, reportedly had bail conditions which ban him from using "any computer connected to the internet".

obvious subject for control is the person's use of the technologies employed in the course of his criminal activities. This may involve the confiscation and destruction of existing IT equipment,[5] or prohibitions on future conduct in respect of the use of certain ICTs.[6] In the recent guilty plea by Jon Venables, one of the killers of James Bulger, to three charges of downloading images and films depicting child abuse, in addition to the sentence of three years' imprisonment the judge ordered forfeiture and destruction of the relevant laptop computer and imposed a five-year order preventing the defendant from owning or using any computer which did not have specialist software to block images of child abuse.[7]

Such IT restrictions have been around since the early days of computer-related crime. When, in 1989, the US hacker Kevin Mitnick was convicted, the prosecution requested that he be prohibited from using or possessing all computers, software and networking equipment. This was contested by the defence, and the court eventually imposed a condition permitting him computer access only with the consent of his probation officer.[8] Indeed, during the trial itself, Mitnick was restricted as to the telephone numbers he could call.[9] Similarly, the hacker Kevin Poulsen was given the following "special conditions" when on probation,

> "… you shall not obtain or possess any computer or computer related equipment or programs without the permission and approval of the probation officer; and you shall not seek or maintain employment that allows you access to computer equipment without prior approval of the probation officer."[10]

In the United States, certain states, including Nevada, Florida and New Jersey, have statutory provisions mandating the imposition of internet restrictions on convicted sex offenders.[11] In the United Kingdom, the issue of a prohibition on accessing the internet has arisen in a number of recent sentencing decisions, particularly in relations to sexual offences prevention orders (SOPOs), which were introduced by the Sexual Offences Act 2003 ss.104 to 113, replacing powers under the Sex Offenders Act 1997 s.5A.

Sexual Offences Prevention Orders

A court may make a SOPO where an offender has been convicted of a sexual offence listed in Sch.3 to the 2003 Act or a sexual offence listed in Sch.5 where the content of the offence gives rise to concern over the risk of future sexual offending.[12] A SOPO takes effect either for a fixed period of not less than five years, as specified in the order, or until further order.[13] An order for less than five

[5] For examples of courts ordering forfeiture of the defendant's computer as a form of punishment, see *Sheppard and Whittle* [2010] 2 Cr. App. R. (S.) 455 and *Townsend-Johnson* [2010] EWCA Crim 1027. The relevant provision is the Powers of Criminal Courts Act 2000 s.143.

[6] e.g. a "prohibited activity" requirement issued as a requirement of a "community sentence", under the Criminal Justice Act 2003 s.203.

[7] *The Times*, July 24, 2010.

[8] See *www.freekevin.com* [Accessed September 2006]

[9] K. Hafner and J. Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (Simon and Schuster: New York, 1991), p.342; B. BloomBecker, *Spectacular Computer Crimes* (Dow Jones-Irwin: Illinois, 1990).

[10] Letter from Marc J. Stein, US Probation Officer to Kevin Poulsen, May 22, 1996, quoted in D. Thomas, "Criminality on the electronic frontier" in D. Thomas and I. Loader (2000), p.30.

[11] See generally, E. Brant, "Sentencing 'cybersex offenders': Individual offenders require individualised conditions when courts restrict their computer use and internet access" (2009) 58 Cath. U. L. Rev. 779.

[12] SOA 2003 s.104(1).

[13] SOA 2003 s.107(1).

years is therefore unlawful. General practice now is to make the length of the SOPO commensurate with the period of sex offender notification which arises automatically upon conviction under the 2003 Act.[14] A SOPO can only be made where the court is satisfied that it is "necessary" to make such an order, for the purpose of "protecting the public or any particular members of the public from serious sexual harm from the defendant".[15] In turn, "serious sexual harm" means "serious physical or psychological harm caused by the defendant committing one or more offences listed". A SOPO may prohibit the offender from doing *anything* described in the order, provided that the restrictions imposed are "necessary" in the above sense. This means that a SOPO may include little more than might be set out in standard licence conditions, but in some cases the requirements can be very restrictive. They may involve engagement with the person's right to privacy (art.8) and right to freedom of expression (art.10) under the European Convention on Human Rights (ECHR).[16] Breach of a SOPO is a criminal offence, irrespective of whether the facts disclosed by the breach would constitute a criminal offence in themselves. If a person, without reasonable excuse, does anything prohibited by a SOPO, they are liable to a term of imprisonment not exceeding five years.[17]

In *Terrell*[18] the offender pleaded guilty before the magistrates to making indecent images of a child, and was committed for sentence. The Court of Appeal quashed the sentence of imprisonment for public protection (IPP) imposed by the Crown Court judge. The Court of Appeal agreed that there was a clear risk that the defendant would continue to offend in a similar way in future, but found that there was no evidence that his conduct would escalate to photographing children, or to abusing them. In the circumstances the defendant was not sufficiently "dangerous" to qualify for an indeterminate custodial sentence. The Court therefore substituted a determinate custodial sentence, saying that in cases such as the present it may be possible to avoid an indeterminate sentence by imposing "apt and effective restrictions" in a SOPO, such as "use of a computer, internet access [and] possibly contact with individuals or children" which would address the degree of risk and the seriousness of harm".[19] *Terrell* has been followed in later sentencing decisions which show that, for the most part, offenders convicted of downloading and viewing child pornography are appropriately dealt with in that way.[20] The distinction drawn in *Terrell* between cases appropriate for IPP and those which can better be dealt with by a SOPO has, however, given rise to a subsequent conflict in different divisions of the Court of Appeal in sentencing cases. On one view indeterminate sentences and SOPOs must be regarded as mutually exclusive.[21] On another view the two orders can, and often should, be imposed together.[22]

[14] *Hammond* [2008] EWCA Crim 1358; *Smith* [2009] EWCA Crim 1795; *Hemsley* [2010] EWCA Crim 225.
[15] SOA 2003 s.107(2).
[16] The imposition of pre-trial constraints, such as those imposed on *McKinnon* (see fn.4), may also engage art.6 "fair trial" issues, such as the requirement of "adequate facilities" to prepare a defence (at 6(3)(b)). However, such considerations are beyond the scope of this article.
[17] SOA 2003 s.113(1) and (2).
[18] *Terrell* [2008] 2 Cr. App. R. (S.) 49.
[19] *Terrell* [2008] 2 Cr. App. R. (S.) 49 (p.307).
[20] *Waller* [2010] EWCA Crim 728; [2010] 2 Cr. App. R. (S.) 101; [2010] Crim. L.R. 655.
[21] *Bolton* [2010] EWCA Crim 1177; *R. v L* [2010] EWCA Crim 2046.
[22] *R v N* [2010] EWCA Crim 1624 contains a clear statement to that effect.

SOPOs and the internet

SOPOs regularly include restrictions on the defendant's future use of a computer and access to the internet. In many of the earlier cases total bans on owning or using a computer, or on accessing the internet were imposed. Given, however, that the only prohibitions which should be included in a SOPO are those which are "necessary" to achieve the statutory purpose, in later cases the prohibitions have been more tailored to fit the particular offender, and the particular risk that he appears to represent. In *Smith (Edmund)*,[23] a general ban on the use of a computer or access to the internet was overturned on the grounds that it was unnecessary and disproportionate, and in *TO*[24] a complete ban was said to be "draconian". In *Halloren*,[25] an order was quashed on the grounds that the sentencing judge had not adequately considered the statutory criteria or whether the order was strictly "necessary" to achieve the statutory objectives. In *Hammond*,[26] the court amended a SOPO in terms of its duration and its scope, holding that the general downloading restriction was too wide, and should be limited to photographs and pseudo-photographs of persons under the age of 18. Another example is *Smith (Paul)*[27] where the defendant pleaded guilty to possession of indecent images of children and received nine months' imprisonment together with a SOPO. The Court of Appeal upheld an order which prohibited the defendant from downloading, saving or viewing any material from the internet save "for purposes of lawful employment, study, leisure or social interactions with persons over the age of 18".[28] In *Spratley*[29] no objection was taken to a prohibition preventing the defendant "from accessing, viewing, downloading or saving, images from any child internet site, accessing any internet-based chat rooms or similar communication group or network".[30] Other authorities suggest that if the offender represents a risk to children of a particular age, or gender, any preventive order should properly be limited so as to restrict only his access to children of that group.[31]

In *Collard*,[32] the defendant was found guilty of offences of making and possessing indecent images of children. As well as imposing a term of imprisonment, the court also made a restraining order under the then Sex Offenders Act 1997 s.5A, the terms of which were,

> "… that you be prohibited from owning, using, possessing or having any access to any personal computer, laptop computer or any other equipment capable of downloading any material from the Internet. That prohibition does not apply to any such equipment which you have and use for the purpose of any lawful employment at and only at a place of such employment."

[23] *Smith (Edmund)* [2008] EWCA Crim 3083.
[24] *TO* [2010] EWCA Crim 2511.
[25] *Halloren* [2004] EWCA Crim 233; [2004] 2 Cr. App. R. (S.) 57; [2004] Crim. L.R. 392.
[26] *Hammond* [2008] EWCA Crim 1358.
[27] *Smith (Paul)* [2009] EWCA Crim 1795.
[28] *Smith (Paul)* [2009] EWCA Crim 1795 at [8].
[29] *Spratley* [2010] EWCA Crim 1411.
[30] *Spratley* [2010] EWCA Crim 1411 at [24]. The order originally referred to "news groups", but was amended on appeal to encompass the ejusdem generis.
[31] *R. v C* [2008] EWCA Crim 2691; [2009] 2 Cr. App. R. (S.) 5; [2009] Crim. L.R. 302; *Buchanan (Kevin Mark)* [2010] EWCA Crim 1316.
[32] *Collard* [2004] EWCA Crim 1664.

The defendant appealed against the scope of this order. The court allowed the appeal, noting that such a wide prohibition would also effectively deprive his wife and children from access to the internet, and therefore amended the order in the following terms,

> "… that you be prohibited from downloading any material from the Internet, that prohibition not applying to downloading for the purpose of any lawful employment or lawful study."

Such considerations, attempting to minimise collateral interference with home life and the rights of others, should clearly be in the mind of the judge when drafting the terms of such an order. It has also been held that a restriction on the defendant's IT usage that involves or requires the co-operation of a third party, such as the owner of the device, may well be unacceptable.[33] A parallel can be drawn here with the statutory restrictions in the Criminal Justice Act 2003 on inserting a curfew requirement or an electronic monitoring requirement into a community order or suspended sentence, where such requirement would adversely affect the rights of third parties, including those living in the same accommodation.[34]

It would seem obvious from what has been said already that a SOPO should not be made routinely, as an uncontested "add-on" to the sentence. A batch of recent Court of Appeal decisions on appeal against sentence, however, show that SOPOs are sometimes imposed in this way—made "on the hoof", as Henriques J. expressed it in *R. v R.*[35] The cases show that a draft order is sometimes produced, and agreed to, at the sentencing hearing with little or no opportunity given to the defence, or to the judge, to consider the proposed requirements properly. In a busy court list, such an order might be made without full attention being given to it. On appeal against sentence in *Buchanan*,[36] where the draft order had been provided to the court moments before the sentencing hearing, the Court of Appeal stressed the importance of proper time and consideration being given to the terms of a SOPO. The Court suggested that if, by the conclusion of a trial or the opening of a plea of guilty the judge has formed a provisional view as to the imposition of a SOPO, when the judge directs the preparation of a pre-sentence report, and a consideration of the risk of dangerousness, it will usually be helpful to invite the probation service to consider whether management of risk could be assisted by a SOPO, and what restrictions might be appropriate. Counsel for the prosecution should be in a position to submit draft proposals to the court, and to the defence, in good time before the hearing. If there is insufficient time for defence counsel and the defendant to consider the order the matter should be put back for proper consideration to be given. This group of cases shows the Court of Appeal getting to grips with poorly drafted or ill-considered requirements in SOPOs, in much the same way that in earlier cases the Court has deprecated inappropriate, over-inclusive, vague, or poorly drafted requirements in anti-social behaviour orders.[37] In fact, it turned out in *Buchanan*[38] that there was no justification for including prohibitions on the

[33] *Hemsley* [2010] EWCA Crim 225.
[34] Criminal Justice Act 2003 s.215(2).
[35] *R. v R* [2010] EWCA Crim 907.
[36] *Buchanan* [2010] EWCA Crim 1316.
[37] *P (Shane Tony)* [2004] 2 Cr. App. R. (S.) 343; *Boness* [2006] 1 Cr. App. R. (S.) 690.
[38] *Buchanan* [2010] EWCA Crim 1316.

defendant's access to the internet. The sentencing court had lost track of the fact that charges of downloading child pornography had not been proceeded with in that case, and the offences proved against the defendant were of a different character, not justifying an internet ban at all.

Monitoring and enforcement

In the important case of *Mortimer*[39] the defendant was convicted after trial of three counts of sexual assault on a child under 13, and one count of causing or inciting a child to engage in sexual activity. The defendant had a history of sex offences against children. The judge described him as an "exceptionally dangerous paedophile" who presented a significant risk to young girls. A sentence of imprisonment for public protection was passed, with a minimum term of three years, together with a SOPO, imposed until further order, containing some 16 prohibitions in all. This was another case where the judge was handed a ready-prepared draft order, with the proposed prohibitions set out. The judge made the order in those terms. On appeal to the Court of Appeal complaint was made about prohibitions 11 to 16, which all concerned restrictions on the defendant's possession of a computer or mobile phone with internet facility, and his access to the internet. They were as follows:

(11) possessing a computer;
(12) using the internet or its successor for purposes other than work, study or seeking employment;
(13) operating a private internet account;
(14) subscribing to, accessing or attempting to access the internet;
(15) downloading and /or viewing on any computer any image of young persons under 16 unless with permission from a parent or guardian;
(16) possessing a mobile phone or other technology capable of capturing an image which has been obtained via the internet.

The Court of Appeal struck out or reformulated these provisions, on the basis (i) that they were not necessary for the protection of the public; or (ii) they were oppressive and disproportionate, or (iii) that they were almost impossible to police or enforce. The first two of these grounds are familiar from the authorities referred to above. The third ground addresses the important practical point of enforcement. Of course, court orders are there to be obeyed, and breach of a SOPO is a criminal offence. On the other hand, it is naive for a court to expect "an exceptionally dangerous paedophile" to confine his use of the internet to do his on-line grocery shopping and to refrain from accessing child pornography sites. Judges are required to instruct members of a jury that, although the internet is part of their daily lives, they must not use it to research the case, nor use any social networking site to exchange views about the case. A juror can be expected to use the internet when they leave court, but to refrain from researching the case. Most jurors can be expected to perform their duties conscientiously and in conformity with judicial

[39] *Mortimer* [2010] EWCA Crim 1303.

instruction, even though there will be the occasional act of defiance.[40] It might be thought, however, that to permit a sex offender access to the internet for some purposes but not for others involves an unrealistic assumption about such a person's capacity for self-control.[41]

To address the problem of enforcement, the Court of Appeal in *Mortimer* redrafted the requirements so as to prohibit the defendant from having ownership or possession of any computer or mobile phone with access to the internet without first notifying, within three days, the relevant monitoring police or probation officer of such acquisition; and to prohibit the defendant from using any computer, iPhone or mobile phone capable of accessing the internet, where such device does not have the capacity to retain and display the history of internet use, and from making any attempt to delete such history, and from refusing to show such a history to a police officer if so requested.[42] This decision is important because it recognises that levels of compliance with internet bans, whether these are expressed generally or involve restrictions tailored to the facts of the case and the risk posed by the offender, may well be low.

In the past there have been calls from the police to be given "unlimited powers to examine the computers" of sex offenders within their homes, to prevent re-offending.[43] In *Thompson*,[44] however, the Court struck down a requirement which had purported to allow the police unannounced access to the defendant's home for the purpose of checking his computer equipment, storage medium and internet use. The trial judge had already narrowed the scope of the order, by reducing the time during which the police could demand such access to 12 hours a day, from 08.00 to 20.00. The Court of Appeal concluded that the condition, which effectively granted the police a continuing search warrant, was unjustified. They said that it amounted to conferring on the police an extremely wide power to enter the defendant's home to check his computer—a draconian power since it may be executed repeatedly and without the need to demonstrate any further justification, over a period of five years. The Court refused, however, to rule out the possibility that such an order could be justified in appropriate circumstances.[45] A similar line was taken in *Christopher Smith*,[46] where the SOPO had prevented the defendant from owning, having access to, or using, any computer having access to the internet save in the course of his business or at a place of employment or educational establishment, and further preventing the defendant from "denying police officers access to his home address in order to check the above conditions are being complied with". The Court of Appeal said that such a requirement was problematic in a number of ways. First, according to s.117(1)(a), a SOPO was meant to "prohibit" the defendant from doing certain things, but this prohibition in reality was a mandatory requirement that he grant access to police officers who would otherwise need permission to enter his home. It was a "device" to circumvent

[40] *Thompson* [2010] EWCA Crim 1623; [2010] 2 Cr. App. R. 27, considering *Mirza* [2004] 1 A.C. 1118 HL; [2004] 2 Cr. App. R. 8. See also *Karakaya* [2005] EWCA Crim 346; [2005] 2 Cr. App. R. 5; [2005] Crim. L.R. 574; *Marshall* [2007] EWCA Crim 35; [2007] Crim. L.R. 562, and *Thakrar* [2008] EWCA Crim 2359; [2009] Crim. L.R. 357.

[41] See D. Wilson and T. Jones, "'In my own world': A case study of a paedophile's thinking and doing and his use of the Internet" (2008) 47(2) *Howard Journal of Criminal Justice* 107.

[42] *Mortimer* [2010] EWCA Crim 1303 at [15]. See also *TO* [2010] EWCA Crim 2511.

[43] Police "need full access to sex offenders' PCs", *The Scotsman*, March 26, 2007.

[44] *Thompson* [2009] EWCA Crim 3258.

[45] See also *Hemsley* [2010] EWCA Crim 225.

[46] *Smith (Christopher Robert)* [2009] EWCA Crim 785; [2009] 2 Cr. App. R. (S) 110.

the statutory wording. There were also strong arguments to say that if the legislature had intended to grant power to law enforcement agencies to enter a defendant's home to monitor compliance with the order, it would have said so expressly in the Act. Further, this particular term of the SOPO was too wide, in that it did not limit when the police could demand entry, at what times, or how often. It did not require the police to have reasonable suspicion of an offence, but it appeared that the defendant must permit entry, however unreasonable, or risk prosecution for breach. In the end, the Court in *Christopher Smith* chose to strike down the requirement to grant access to the police on the basis that the defendant's limited level of offending on the facts could not justify such a requirement, but Keith J. specifically stepped back from holding that such a requirement could never be justified. It is also interesting to note that the Court in *Thompson* felt that "any provision for monitoring the applicant's use of computers and the Internet" was unjustifiable in this case, but was content with a different stipulation in the order that, as well as requiring prior notification to the police, the defendant must allow "the programme 'Net Nanny' or similar programme to be installed". Such programmes are generally referred to as "filtering" programmes and operate so as to monitor a person's use of the internet, similar in kind to a person's browsing history referred to in *Mortimer*, but with substantially greater functionality.

Filtering programmes are complex, but can be seen as essentially comprising two key elements. First, they contain data lists, usually supplied and updated by the software supplier, but also customisable by the user (such as a parent), detailing the content, sites and services that are considered acceptable ("white lists") and/or, those that are unacceptable ("black lists"). The data lists may relate to the content of a communication, such as keywords or image-related content, or may relate to the location of content available over the internet, such as IP address or Uniform Resource Locator ("URL"). Secondly, they can monitor both the communication requests made by the user (egress traffic), as well as the content being received from the internet (ingress traffic). The record of such usage is then available for review, including remotely, either in real time[47] or at a later date. As such, acceptance by the Court in *Thompson* of the requirement to install and operate such a programme constitutes the real and effective monitoring of the defendant's internet activities. In such an environment, the need for on-going police access to the defendant's premises becomes a much less necessary element of the enforcement regime, and perhaps only really important in examining materials received through the post.

In addition to the installation of filtering or monitoring programmes on the defendant's computer equipment or device, an alternative record of online activities will often be retained by the person providing the defendant with access to the internet, such as an employer[48] or an internet service provider ("ISP"). Such historical "logs" of internet use may have to be retained on a statutory basis, such as by ISPs subject to the Data Retention (EC Directive) Regulations 2009[49] or,

[47] e.g. Net Nanny TM 6.5 offers real time text alerts to a parent's mobile phone.

[48] e.g. in December 2005, Gary McKinnon's bail conditions were altered to permit internet access on condition that he notifies the authorities of his IP address and obtains a letter from his employer.

[49] SI 2009/859. A "public communications provider", once notified by the Secretary of State (r.10(1)), must retain communications data, including that concerning internet access, internet email or internet telephony (Sch., Pt 3), for a period of 12 months (r.5).

more commonly, by the ISP for organisational or commercial purposes, such as network management, customer profiling and marketing.[50] To obtain access to such retained data, the police would need to comply with the procedures for accessing "communications data" under Pt I, Chapter II of the Regulation of Investigatory Powers Act 2000 ("the RIPA").[51] There are problems, however, in that such procedures can be costly in terms of the payment which has to be made to ISPs for the data,[52] and they are not designed for the type of on-going monitoring and spot-checks likely to be required for SOPO supervision and enforcement.

The existence of data held by a third party returns us to consideration of the Digital Economy Act 2010 and the issuing of suspension orders. As well as the controversy over the idea of suspending an individual's internet access service, considerable disquiet had been raised by the ISP industry about their role in such an enforcement regime.[53] The provisions represent interference in the private law relations between an ISP and their subscriber, purportedly justified on grounds of public interest in protecting the rights of copyright owners against online infringement.[54] If such an argument is eventually accepted, then it would seem equally arguable that ISPs should be required to support the enforcement of SOPOs imposed on convicted criminals. An ISP could be required to filter the traffic of a specific account of a person subject to a SOPO, as well as maintain and make available appropriate activity logs. UK-based ISPs already filter the web requests of all their customers against a list of addresses where "potentially illegal child sexual abuse" content is located.[55] While enforcement of SOPOs through ISP monitoring may be permissible under European Union law,[56] serious questions remain about whether such an approach would be viewed as proportionate under the ECHR, as well as desirable.

A final enforcement concern may be that a defendant could install some form of technical mechanism, such as software, to prevent a supervising officer from examining material stored on a computer or related device. In October 2010, for example, Oliver Drage was given a 16 week custodial sentence for refusing to disclose his password during an investigation into child sexual abuse.[57] In terms

[50] Subject to compliance with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) rr.7 and 8.

[51] The probation service is not currently an authorised authority under this part: see the Regulation of Investigatory Powers (Communications Data) Order 2003 (SI 2003/3172).

[52] See, for example, BBC News, "Child abuse unit paying for data" (January 21, 2009), which reported that the Child Exploitation and Online Protection Centre had paid more than £170k to ISPs since 2006.

[53] In July 2010, BT and TalkTalk commenced an action for judicial review of these provisions, including on grounds of it being a disproportionate measure: *R (on the application of British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Business Innovation and Skills*, Administrative Court Ref. No.CO/7354/2010. On November 11, 2010, the High Court granted permission to proceed with the action on all of the grounds raised by the claimants.

[54] Lord Mandelson, Secretary of State for Business, Innovation and Skills, *Hansard*, December 2, 2009; Col 745: "the need for government and for the law to protect the rights of content holders, so we are creating two new obligations on internet service providers".

[55] The list created, maintained and made available by the Internet Watch Foundation. See further I. Walden, "Porn, Pipes and the State: Censoring Internet Content", *The Barrister*, No.44, April–May 2010, pp.16–17.

[56] See Directive 00/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 at recital 47: "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation." In March 2010, the Commission issued a proposal for a directive "on combating the sexual abuse, sexual exploitation of children and child pornography", which includes a provision, at art.21, requiring Member States to take measures to block access to websites containing child pornography, (COM(2010)94 final).

[57] e.g. BBC News, "Man jailed over computer password refusal", October 5, 2010.

of post-conviction preventive orders, further prohibitions may be imposed to address such concerns. In April 2007, for example, Andrew Hadwin was imprisoned for distributing pornographic images and was reported as having being banned "from having a password to a private home computer".[58] The forensic challenge of dealing with such "protected" data is a recognised problem for cybercrime investigations and has been specifically addressed in Part III of the RIPA.[59]

Conclusion

As recent decisions clearly indicate, where a court wishes to control the future online activities of convicted sex offenders, a simple outright prohibition of a person's access to the internet will be struck down on appeal, both for offending proportionality and because it is unrealistic. Meeting the statutory criterion of "necessity" and the general principle of proportionality, including considerations of collateral interference, are high thresholds. These are likely to rise further as the internet becomes ever more integrated into our daily lives. As such, the experience of our courts with SOPOs does not bode well for the enforceability of the proposed suspension orders under the Digital Economy Act.

In future, sexual offence prevention orders will surely need to be couched less in terms of specific devices, such as computers and mobile phones (let alone brands, such as the iPhone referred to in *Mortimer*), and should focus instead on the functionality of accessing the internet and internet-based services. Usage-based restrictions, whether negative (e.g. not to communicate on-line with any person under 16 years of age) or qualified (e.g. permitting access to the internet for work and study purposes), must become more closely integrated with techniques of enforcement. In principle, technology has the capacity to monitor, record, and disclose every aspect of our on-line activities.[60] Technological monitoring may well be less intrusive than permitting periodic access by the police to check on-line usage. More work would need to be done, however, on specifying the access regime by which the police or probation service can review the records generated.

There is a difficult balance to be struck between the effective monitoring of a preventive order such as a SOPO, and unacceptable intrusion into the defendant's life and the lives of his family and others. As the large number of recent sentencing appeals in relation to SOPOs makes clear, piecemeal development in this area is not satisfactory, and different divisions of the Court of Appeal sometimes say different things. It is submitted that guidelines should be drawn up by the new Sentencing Council and issued to assist counsel and the courts in setting the content of requirements in SOPOs. The Sentencing Guidelines Council, in its work on breach of ASBOs, also addressed the "key principles and considerations applicable to the *making* of an ASBO".[61] A similar task is required here. The guidelines should further set out best practice for dealing with the monitoring and enforcement issues considered in this article. Because a SOPO is generally now set to the same length as the relevant notification period under the Sexual Offences Act 2003, a defendant

[58] "Child porn 'too easy to find'", *The Oxford Mail*, April 18, 2007.
[59] See further I. Walden, *Computer Crimes and Digital Investigations* (Oxford: OUP, 2007) at paras 4.275 et seq.
[60] See further M. McGuire, "Online surveillance and personal liberty" in Yvonne Jewkes and Majid Yar (eds), *Handbook of Internet Crime* (Willan, 2009), Ch.23.
[61] SGC, *Breach of an Anti-Social Behaviour Order*, December 2008, Annex A.

in breach of one of these provisions is likely to be in breach of both. The Court of Appeal has suggested recently that guidelines on sentencing for breach of SOA notification requirements would be helpful.[62] Logically, that could also be part of the same project.

[62] *Grosvenor* [2010] EWCA Crim 560; [2010] 2 Cr. App. R. (S.) 100.