Laundering sexual deviance: Targeting online pornography through anti-money laundering

Alex Antoniou and Gauri Sinha
The City Law School
City University
London, United Kingdom
e: Alex.Antoniou.1@city.ac.uk | Gauri.Sinha.1@city.ac.uk

Abstract — This paper concentration on cyber-pornography/obscenity, which encompasses online publications or distribution of sexually explicit material in breach of the English obscenity and indecency laws. After examining the major deficiencies of the attempts to restrict illegal pornographic representations, the authors aim to highlight that the debate regarding their availability in the Internet era neglects the lucrative nature of the circulation of such material, which can be also targeted through anti-money laundering. Rising profits fuel the need to recycle the money back into the legal financial system, with a view to concealing their illegal origin. Anti-money laundering laws require disclosure of any ‘suspicion’ related to money laundering, thus opening another door for law enforcement to reach the criminal.

Keywords - cyber-pornography/obscenity; online pornography revenues; anti-money laundering

I. PORNography AND Cybercrime

The ‘novel social-interactional features of the cyberspace environment’ [1] trigger new patterns of illegal activity online. Owing to the wide range of phenomena comprised by the term cybercrime, it is difficult to formulate a comprehensive definition, while attempts to define it have been rather unsystematic [2]. Although there is no universally accepted definition, three critical elements of cybercrime have emerged.

First, cybercrime is committed within electronic communication networks [3]. Second, cybercrime can be categorised by the specific function that technology fulfills in its commission. Furnell distinguishes between ‘computer-assisted crimes’ [4], in which ‘the computer is used in a supporting capacity, but the underlying crime or offence either predates the emergence of computers or could be committed without them’ [5], e.g., fraud, money laundering or pornography; and ‘computer-focused crimes’ [6], whereby ‘the category of crime has emerged as a direct result of computer technology and there is not direct parallel in other sectors’ [7], like website defacing, hacking etc. Third, cybercrime can be legally defined. Wall divides cybercrime into four categories which reflect four established bodies of law: (i) cyber-trespass; (ii) cyber-deceptions and thefts; (iii) cyber-violence and (iv) cyber-pornography/obscenity [8].

Computer-mediated activities falling within the scope of cyber-pornography/obscenity can be either explicitly prohibited by the law or deemed deviant, namely objectionable because they breach social norms without automatically attracting criminal sanctions [9]. While the debate surrounding this category is complicated by the fact that not all kinds of pornography are illegal, the primary focus of this paper is directed first, towards online representations of sexual deviance, such as indecent images of children circulated via paedophilia networks [10]; and second, towards activities that carry formal legal sanctions and can be classified as cybercrime either in a broad sense, namely where the use of computer technology is peripheral to the main offence (e.g., the circulation of extreme pornography) or in a narrow sense, where the criminal conduct is made possible through technology itself (e.g., making a pseudo-photograph of a child) [11].

II. CHALLENGES IN TACKLING INDECENT IMAGES OF CHILDREN ONLINE

In recent years, the enforcement of provisions targeting the production and distribution of indecent images of children has been dynamically pursued, yet there are significant obstacles that pose challenges in curtailing the availability of such material. Currently, the law in England and Wales criminalises the taking or making, distribution and publication [12], as well as possession [13] of indecent images of real children, including images generated by computer graphics which appear to be photographs (pseudo-photographs) [14]. While the application of the relevant law regarding ‘possession’ and ‘distribution’ offences is more straightforward and in most cases defendants plead guilty, ‘making’ an indecent image of a child remains obscure under case law, thereby allowing offenders to escape liability [15].

Furthermore, the new Directive 2011/92/EU [16] introduces the obligation on Member States to remove ‘child pornography’ [sic] [17] webpages hosted in their territory and to take appropriate steps to have them removed, if hosted abroad. Member States may also take measures aimed at blocking access to webpages containing or disseminating ‘child pornography’ by users within their own territory. However, it can be argued that blocking is counterproductive, since only accidental access is prevented and objectionable websites remain online, without getting to the root of the problem. Additionally, pressure from Internet Service Providers and civil libertarians has diluted the text of the Directive, making it almost ‘meaningless’ [18].
The British police have been active in combating paedophile rings operating over the Internet [19], but the complexity and the sheer volume of resources have severely obstructed the policing operation in the past [20]. The issue of enforceability has been tested through the UK’s largest police hunt against paedophiles and online indecent images of children, Operation Ore. In 2002, thousands British residents of a list comprising 7,272 suspects were falsely branded paedophiles, while it became clear later that a significant portion of those who were convicted of related offences had committed no crime whatsoever. Moreover, electronic data did not prove to be indisputable, since many of the accused had been the victims of identity theft [21]. ‘Thousands of cases under Operation Ore have been built on the shakiest of foundations [22],’ as many unknowing Britons fell victims of fraud by website owners who acquired or traded in stolen credit card details. Rather controversially, 39 of the accused committed suicide under the pressure of investigations [23].

Notwithstanding the serious nature of the offences at issue, surprisingly few prosecutions have commenced in the Crown Court in England and Wales in respect of the more serious offence of possession with intent to distribute and taking an indecent photograph of a child [24]. Additionally, sentencing demonstrates that offenders are perceived as ‘relatively harmless’ and judges fail to acknowledge the potential dangerousness of the defendants convicted of possession or distribution, despite the fact that research demonstrates a connection between ‘child pornography’ and child sexual abuse [25].

Finally, the Coroners and Justice Act 2009 (CJA 2009) created an offence of possession of prohibited images of a child [26]. The new law outlaws computer generated images, manga images, as well as private cartoons and drawings involving children [27]. It remains unclear though how a drawing of a 17 year old will be distinguished from a drawing of an 18 year old. More important, the offence is broadly defined and raises serious concerns over its potential application beyond individuals whom the Government is seeking to target. While any pornographic representation in which participants have not provided an informed and valid consent is a legitimate subject of criminal law, the new offence may criminalise those who cause no harm to others and detract attention from tackling the circulation of indecent images, in which minors are actual victims of sexual abuse [25].

III. TARGETING ADULTS’ EXTREMEITY

According to the Obscene Publications 1959 Act (OPA) [28], the primary legislation for the regulation of sexually explicit content of any kind in England and Wales, a publication shall be deemed obscene, if its effect is such as to ‘tend to deprave and corrupt’ its likely audience [29]. The Criminal Justice and Public Order Act 1994 amended the OPA, so as to take into account graphic content in computer data format [30], but where illegal material is hosted overseas, there are difficult jurisdictional issues to be dealt with [31].

Being couched in imprecise language, the existing obscenity test is notoriously obscure, as the terms employed invite a great degree of subjectivity and uncertainty. The history of the 1959 Act is littered with unsuccessful cases [32], with the recent acquittal in R v Peacock [33] being ‘the final nail in the coffin for the OPA in the digital age [34].’ Overall, the obscenity law in England and Wales is deemed ‘puritanical’ and ‘unworkable’ [35], as presently constructed.

Furthermore, the UK Parliament legislated in the Criminal Justice and Immigration Act 2008 (CJIA 2008) to create a new criminal offence of possession of extreme pornographic images [36]. Possession is key to the offence and viewing material accessed via the Internet on computers or mobile phones may also be covered [37]. In order for an image to fall foul of the new law, it must be deemed pornographic [38], be ‘grossly offensive, disgusting or otherwise of an obscene character [39]’ and portray in ‘an explicit and realistic way [40]’ a life-threatening act or an act resulting in serious injury to a person’s anus/breasts/genitals or an act involving necrophilia or bestiality [41].

The new offence is aimed at addressing the contemporary challenges that the current legal framework faces: controlling the source of obscene/pornographic publications is no longer effective in the Internet age, since the global nature of the Internet makes it very difficult to prosecute those who are operating from abroad [42]. Instead of tackling the problem of supply, the law targets the demand for such material. In a nutshell, it shifts criminal responsibility from the producer to the consumer. However, as currently drafted, the new provisions have attracted much censure for being fundamentally intrusive, ‘knee-jerk and ill-considered [43].’

Latest figures indicate a substantial fall in the number of prosecutions under the OPA [44]. Ironically, it is just after this that prosecutions under the new extreme porn law have dramatically increased [45]. Enforcement so far indicates that it is doubtful whether the new provisions will put the violent porn genie back in the bottle, while this censorship in disguise serves to increase the cultural interest in the banned content. The disappointing conclusion must be that in addition to the current restrictive obscenity laws, the UK Government has resorted to more repressive measures, like the CJA 2009 and the CJIA 2008, which severely impact on individuals’ rights to privacy and freedom of expression.

Moreover, concerns over the inadvertent exposure of minors to adult-oriented content have promulgated several legislative initiatives. The UK government has favoured the self-control of the service providers and the adoption of filtering systems for online content, while the Internet Watch Foundation (IWF), the independent self-regulatory body [46] which provides the UK Internet Hotline for the public to report criminal online content, announced the development of rating systems in 1998 [47].

However, such systems have come under censure for being ‘the perfect tool for cyber-censorship [48]:’ they are partially effective against sexually explicit websites [49] and they can exclude socially useful websites [50] or speech related to sexual minorities [51]. Overall, such mechanisms are impracticable [52] and ‘more likely to interfere with the free exchange of ideas than to encourage it [53].’ Notwithstanding the fact that such tools are not a sound response to content problems, the Online Safety Bill, currently before the UK
Parliament, contains provisions that require electronic device manufactures to provide customers with a means of filtering content [54].

Finally, recent research showed that British Telecom (BT) services’ CleanFeed system, which blocks access to a register of illegal websites, can be used by technically skilled users as an ‘oracle’ to allow access to the secret content of the blacklist provided by the watchdog IWF, thereby turning CleanFeed into a pornography index [55]. The increasingly popular peer-to-peer file-swapping software also ‘allows individuals to search for and trade any manner of digital media, turning every hard drive connected to the Internet into a potential porn distribution hub [56].’ Additionally, the freely available Freenet software allows the creation of websites and online file sharing with complete anonymity, by hiding both the identities of Freenet users and the fact that someone is using Freenet at all in any online environment [57]. Thus, the rapidly developing nature of new technology is one step ahead of legislative proposals even as they are being drafted and increasingly generates novel and complex problems, for which conventional solutions are evidently unsuitable.

IV. EXTREME PROFITS

‘Lust motivates technology [58].’ The high level of demand for the erotic has been the driving force behind the rapid development of technologies. ‘With little cash to spare and its nose to the ground, pornography is often first to sniff out the practical uses of new media, leading the way for profitable investment by the mainstream [59].’ The Internet has been no exception. It is estimated that pornography ‘makes up 30% of the total data transferred across the Internet [60].’ While successful prosecutions are rare, it appears that the porn industry is mushrooming since the massive expansion and commercialisation of the Internet in the mid-1990s.

Estimated revenues are extremely high, suggesting that the profits of the industry exceed those of the top technology companies combined: Microsoft, Google, Amazon, eBay, Yahoo!, Apple, Netflix and EarthLink [61]. The global pornography industry was worth $97bn (£61bn) in 2006 [62], while some Internet pornography companies may now be found on the NASDAQ stock exchange list [63]. In 2006, the adult-video business in the US has seen record revenues of some $13.3bn [64], with the online subscription and sales generating $2.8bn [65]. The American adult entertainment industry records more revenue each year than ‘legitimate’ Hollywood [66]. Additionally, the Adult Industry Trade Association estimated that the UK porn industry was worth £1bn in 2005 [67]. According to statistics from respected news and research organisations, every second $3,075.64 is being spent on pornography [68].

Moreover, ‘images of teens at or near 18th birthday have been proven to be highly popular and lucrative subject for online pornography business [69].’ Between 2002 and 2004 the number of paedophile websites doubled to 19,246 [70], the majority of which were of commercial nature. Latest figures indicate that the number of websites offering ‘child pornography’ has reached 100,000 within two years [71], which amounts to an increase of roughly 520%. In 2004, it was estimated that the online trade of indecent images of children was worth approximately $3bn per annum [72].

In the first case of its kind in England and Wales, an investigation into a paedophile ring, which began in 2005, resulted in the convictions of four men in June 2011. The offenders admitted distributing millions of indecent images of children to over 40 countries globally via an international illegal news service, to which users subscribed, downloaded and circulated images or video clips of child abuse. The men pleaded guilty to various charges and they are reported to have made over £2.2 million over a period of seven years [73].

Pornography, violent or not, has exploded beyond anyone’s imagination. It appears that a considerable number of individuals spend non-trivial resources to access pornography. Millions seek porn and spend billions for it.

V. MONEY LAUNDERING AND PORNOGRAPHY

‘There’s no business like porn business [74].’ Closely linked to this multibillion dollar industry is the phenomenon of money laundering. In simple terms, money laundering is a process by which the origin of illegal earnings is disguised. The European Commission of Justice and Home Affairs defines money laundering as ‘the conversion or transfer of money, assets and property derived from criminal activities to apparently legitimate status by disguising their origin through a variety of financial manoeuvres [75].’ This could be a simple lie as to the provenance of money or an asset, or involve complex property movements through many countries, institutions, entities, assets and individuals. The means may be varied, but the essence remains the same: the creation of a false impression that something was legitimately acquired [76]. To this end, money laundering is essentially aimed at the injection of ‘dirty money [77]’ into the legal economy, ‘to spend and enjoy [78]’ this money. This invariably stems from a criminal’s desire of achieving a financial reward that can be used either for personal gain, or to finance a further criminal activity [79]. In the words of MacKrell, ‘money laundering helps make crime worthwhile [80].’

The illegal nature of money laundering makes it difficult to measure accurately the amount of money laundered. The International Monetary Fund (IMF) has estimated that the global amount of laundered money is the equivalent of between 2 to 5 per cent of the world’s gross domestic product (GDP) [81]. Commenting on this exponential growth, the Managing Director of the IMF indicates:

[… the estimates of the present scale of money laundering transactions are almost beyond imagination. This scale poses two sorts of risks: one prudential, the other macroeconomic. Markets and even smaller economics can be corrupted and destabilized [82].}
VI. THE PROCESS OF MONEY LAUNDERING

Money laundering has broadly been understood to consist of a three stage process, namely (i) placement; (ii) layering; and (iii) integration. Thus, a full ‘washing cycle’ typically runs through three stages and across many national borders [83].

The first stage, that is placement, primarily aims at introducing the criminal proceeds into the financial system [84], for example, by depositing the illegal gains from pornography in a bank. Apart from ‘primary placement’ of money in the financial system, this stage could also be manifested through ‘secondary placement [85]’ by indirect infiltration of money supply into the bank system, for instance, by intermediaries in the pornography business. Since this is the stage when cash enters the legal financial system, the placement stage has been held to the most crucial process for the launderer [86], which deserves ‘continued focus and attention.’

Once proceeds have been safely deposited into the financial system, it is then followed by the layering stage. This stage involves more complex concealment measures to disguise the illicit funds, for example, through the use of multiple electronic funds transfers through bank accounts in numerous countries [88]. For this reason, it has been called the ‘main wash’ stage. The more often money gets transferred around the globe in this phase, the less traceable are its criminal origins [89].

Finally, the stage of integration follows successful layering. Here, the aim is to create a justification for the origin of the proceeds, e.g., by creating false legal documents or using the gains arising from pornography in third party transactions [90]. Similarly, the transformed illegal money in this stage may be used for financial investments (deposits, stocks) or property (investment in real estate or companies) [91]. This could also be termed as ‘parking of illegal money,’ which shows no connection to pornography and is fully ‘converted’ into a visible asset [92]. The funds have now finally been provided with a ‘gloss’ to look legitimate [93].

However, the past decade has seen the constant overlap of these three stages, with money laundering now being transformed into ‘cyber-laundering.’ Lovet pertinently describes this trend as the ‘big cyber-laundering machine’ [94].’ Not only is the internet an effective tool for circulating pornography, it is also popularly being used for ‘laundering’ the gains to escape the eyes of law enforcement. New payment technologies (such as wire transfers) permit the transfer of illegal funds more rapidly and make law enforcement work even more complicated [95]. This, coupled with the transnational nature of online commerce and finance, provides an opportunity for criminals to create a borderless environment and misuse financial systems across national borders through the Internet [96]. Cyber-laundering is believed to be the latest (and most advanced) technique in money laundering typologies [97]. Figure 1 demonstrates the process through which profits from illegal cyber-pornography are laundered.

VII. FOLLOWING THE PROFITS OF PORNOGRAPHY THROUGH ANTI-MONEY LAUNDERING

In the UK, anti-money laundering laws hinge on the reporting of suspicious activities. In the context of illegal pornography, all regulated institutions/firms/professional persons are required to report any ‘suspicious activity’ linked with the crime that they encounter in their day-to-day business, which could have the potential to launder profits of the business.

These reports, in turn, are passed on to the Serious Organised Crime Agency (financial intelligence unit of the UK), which has described financial reports as ‘a vital weapon in the UK’s armoury to prevent and detect crime and to protect the integrity and reputation of the UK financial system’ [98].’ If the report leads to further investigation, it greatly increases the chances of law enforcement to reach criminals engaged in the circulation of illegal pornography.

The post 9/11 era in the UK saw money laundering laws taking a new and modern direction with the Proceeds of Crime Act 2002 (POCA). This created a single set of money laundering offences applicable to the proceeds of all crimes. Part VII of the POCA which is dedicated to money laundering, sets out three principal money laundering offences: concealing, disguising, converting or transferring criminal property [99]; becoming concerned in arrangements that facilitate the acquisition, retention, use or control of criminal property [100]; and, acquiring, possessing or using criminal property [101].

Not only is the requirement to report the possibility of money laundering mandatory under UK law, the failure to report has also been criminalised. Thus, a person would commit an offence if, in the course of his/her business, fails to disclose to the authorities when he ‘knows’ or ‘suspects’ or has reasonable grounds for knowing or believing that another person is engaged in money laundering [102]. In essence, if a person/firm fails to detect or suspect money laundering, the person may be guilty of a criminal offence, thereby criminalising ‘negligence’ to suspect [103].
Running parallel to the POCA, the **Money Laundering Regulations 2007** have further expanded the ambit of the law. The Regulations apply to persons acting in *the course of business* in the following areas: credit institutions; financial institutions; auditors, insolvency practitioners, external accountants and tax advisors; independent legal professionals; trust or company service providers; estate agents; high value dealers; and casinos [104]. This clearly reflects the broad range of professions/sectors placed with the responsibility of identifying money laundering.

Additionally, there have been three European Union (EU) Directives which have been seen as landmarks in their attempt to counter money laundering. A key feature of the Third Money Laundering Directive [105] was the reporting of suspicious transactions. The Directive, in line with the domestic legislation, requires mandatory reporting of suspicious transactions by the institutions to the State’s financial intelligence unit, where they suspect or know or have reasonable grounds to suspect that money laundering is being or has been committed or attempted [106].

In the fight against money laundering, banks have appropriately been referred to as one of the key gatekeepers [107]. Criminals use the ‘opacity and confidentiality’ of banks to conceal their illegal money [108]. This is reinforced by the House of Lords Report which estimates that two-thirds of organised crime in the UK is laundered by ‘banks and other bodies [109].’

Laying stress on the role of banks, Lord Woolf has remarked in the case of *Bank of Scotland v A* [110]:

> Money laundering is an increasingly common problem of large scale crime. It is of the greatest importance, in the public interest, that the police should be supported by financial institutions in their attempts to prevent money laundering and to detect it when it happens [111].

Thus, there is an increasing trend towards the need for banks to shoulder the primary responsibility to report any suspicion regarding money laundering. The commitment to this objective has been revisited very recently in March 2012 when the Financial Services Authority fined Coutts & Company £8.75 million for breaches of money laundering rules after 3 years of serious and systemic problems in handling customers vulnerable to financial crime [112]. This has been the largest ever fine imposed by the Authority in its capacity as the UK financial regulator.

An interesting parallel of the link between money laundering through bank accounts can be seen in the United States, with the **recent conviction of two Philadelphia-based companies owned by the ‘King of Porn’ [113] under charges of money laundering.** For their illegal activities, the two companies received payments in the form of money orders, checks, credit cards and wire transfers and the subscription fees were deposited into various company accounts. Holding the companies guilty of money laundering with fines and forfeitures totalling $6.4 million, the U.S. law authorities have set an example of tracing the assets of criminals involved in pornography. In contrast, money laundering convictions in the UK still largely comprise of drug traffickers [114], thus portraying the need to spread to other forms of organised crime, including pornography.

**VIII. Conclusion**

Since 1959, the law and technology have advanced to a stage at which the legal position on the regulation of illegal pornography remains blurred, thereby making effective enforcement difficult. Furthermore, recent attempts to curtail the availability of representations of sexual deviance online have led to the introduction of more draconian measures. However, tackling the problem of representations of sexual deviance in a borderless electronic environment requires a two-fold approach. Instead of fully or solely concentrating efforts on the regulation of online content, the Internet needs to be understood as a convenient tool for sexual deviants, abusers or victimizers, not as the cause for their existence. Thus, along with unambiguous and up-to-date legislation, law enforcement agencies need to take into account that pornography is well entrenched in the market economy and the industry is a reliably lucrative business in the Internet age.

The increasing profit margin in the pornography business makes the crime particularly vulnerable to money laundering. This creates a vicious cycle of engaging in the circulation of pornography, receiving illegal gains, laundering the money and finally, reinvesting the laundered money back in the crime. Money laundering thus gives economic power to criminals by allowing them to use the proceeds of their crimes to further their criminal activities [115]. Additionally, ‘there is the contamination bred by contempt for the law, because if one aspect of the law is broken, other financial infringements seem easier to make [116].’ From an *unknown legal concept* till the 1980s, to one of the ‘buzz phrases […] in the 1990s [117],’ money laundering has now emerged with a ‘veritable roar [118].’ In this light, this paper has stressed on the need to ‘harmonise’ the legal efforts against sexual deviance on the Internet with anti-money laundering measures, enabling the law to reach the criminal by tracing the path of his money.

**REFERENCES**

[5] Ibid.
[6] Ibid.
[7] Ibid.


[14] Section 7(7) of the Protection of Children Act 1978, as amended by section 84(3)(c) of the Criminal Justice and Public Order Act 1994, defines a pseudo-photograph as “an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph.”


[20] Following Operation Cathedral for instance, which exposed the sophisticated Wonderland club, the analysis revealed that the 750,000 indecent images of children seized portrayed 1,200 different children, of which only 18 were identified and discovered; see R. Downey, “Victims of Wonderland,” Community Care, vol. 1412, pp. 30-1, 2002.


[25] Ibid.

[26] A prohibited image is one which is pornographic, focuses solely on a child’s genitals or anal region or portrays a sexual act with or in the presence of a child and which is grossly offensive, disgusting or otherwise obscene character; see section 62(2) of the Coroners and Justice Act 2009. The offence came into effect in April 2010 and is punishable by up to three years imprisonment.

[27] Indecent (pseudo)photographs of children and tracings or derivatives of (pseudo)photographs of minors are not covered.


[29] Section 1 of the OPA.

[30] Section 1(3)(b) of the OPA: “where the matter is data stored electronically,” the Act reads, a person “publishes” an articles when transmits that data.”


[38] Section 63(3) of the CJA 2008.


[40] Interestingly, “explicit and realistic” – section 63(7) of the CJA 2008 - means that the offence is not limited to images of real criminal offences.

[41] See section 63(7) of the CJA 2008 for a more detailed wording.

[42] Legislation over internet content comes under the jurisdiction of the country of source; thus, prosecutions under the Obscene Publications Acts 1959 & 1964 would be possible, only if a website was based in the UK.


[45] Ibid.

[46] Funded by the EU and the online industry.

[47] IWF, “Rating and Filtering Internet Content – A United Kingdom Perspective,” (March 1998). Its decision was favoured by the then UK government; see House of Commons Debate 2 March 1998, vol. 307, col. 466 (statement by the then Minister of State in the Home Department, Alun Michael).


[54] Section 1 of the OPA.

[55] Section 1(3)(b) of the OPA: “where the matter is data stored electronically,” the Act reads, a person “publishes” an articles when transmits that data.”

Section 329 of the Proceeds of Crime Act 2002.

Section 330 of the Proceeds of Crime Act 2002.


Reg. 3 of the Money Laundering Regulations 2007.


Ibid., Article 22.


