International Review of Law, Computers & Technology, 2013
http://dx.doi.org/10.1080/13600869.2013.796706

Routledge
Taylor & Francis Group

The art of trolling law enforcement: a review and model for implementing 'flame trolling' legislation enacted in Great Britain (1981–2012)

Jonathan Bishop*

Centre for Research into Online Communities and E-Learning Systems, The European Parliament, Square de Meeus 37, 4th Floor, Brussels B-1000, Belgium

(*Received 16 November 2012; final version received 13 April 2013*)

The advancement of information and communications technology often results in early adoption, followed by concern over a digital divide, followed by mass adoption and then, inevitably, abuse and misuse of that platform. The most recent of these technologies is social networking services. The early adopters used Friendster and MySpace, and the masses now use Facebook and Twitter. The abuse of people on these platforms was called Cyberbullying in the case of the first two in the 2000s, and Internet trolling in the case of the second two in the 2010s. This paper reviews the legislation enacted in the UK parliament between 1981 and 2012 to deal with these offences, called 'flame trolling', for those based on transgress humour, or electronic message faults more generally. The paper presents a framework that includes a 'Trolling Magnitude Scale' based on established trolling culture, in order to link the legislative offences to the severities of those faults, as well as to the ability of specific Internet users to tolerate them or otherwise. The paper concludes that by using this framework law enforcement agencies such as the police can apply the laws more fairly and proportionally to protect free speech and at the same time be tough on the causes of electronic message faults in the form of Internet abuse and data misuse.

Keywords: Internet abuse; Internet trolling; cyberbullying; criminal law; media law

1. Introduction

With each new burst of technological saturation comes a new media panic made up of a new problem. Since the 1920s we have seen 'the Great Depression' under Stanley Baldwin, 'short-termism recessions' under Harold Wilson in the 1960s, and 'The Winter of Discontent' under Jim Callaghan in the 1970s. Equally, since these tough economic times we have seen the end of the 'post-war consensus' by Margaret Thatcher, the 'longest recession since the Great Depression' under John Major, and the so-called end of 'boom and bust' under Tony Blair. This was followed by tackling 'the credit crunch' under Gordon Brown and dealing with the 'financial deficit' and ushering in another 'age of austerity' under David Cameron. With each economic turmoil has followed a new wave of information and communications technology; each its own new innovative means of doing something *Homo sapiens* have been able to do since the day we could speak – harass others.

The new word for harassment, via communications systems, is called 'trolling' by the media, who more as storytellers than fact reporters seek to use transgressive narratives to

*Email: jonathan@jonathanbishop.com

emulate moral panics by convincing their readers that they are living in a science fiction-like dystopia where technology is a danger to those in society. This is as opposed to it being used dangerously by those in society (Driscoll and Gregg 2008). Technically, in this modern context, trolling might best be collectively referred to as the 'sending of provocative messages via a communications platform for the entertainment of oneself, others, or both'. It has been found to be helpful to differentiate between types of trolling that occur online – Internet trolling – and the types of trolling that are designed for a particular reaction regardless of the electronic medium. Those transgressive messages designed to harm others for the sender's gratification and others' discomfort are called 'flame trolls', and those designed to entertain others for their gratification are called 'kudos trolls' (Bishop 2012a, 2012b). If either of these have legal remedies for any offence they are called 'electronic message faults', whereas if they do not, then they are 'electronic message freedoms', and there is nothing stopping people from expressing free speech in this way. The use of the word 'troll' to describe those who carry out Internet abuse was popularised in 2011, which was about 7 years after the term because used to refer to transgressive humour (Bishop in press). Up until this point trolling had been clearly defined by the Internet dictionary, 'Netlingo' (Jansen and James 1995) to refer to more peaceful provocation. The change of the word troll to describe Internet abusers followed a single case study of people on the 4chan website who identified personally as 'trolls' to justify their abusive behaviour for *their* entertainment (Phillips 2011), and mistakenly the English studies student applied this to abuse on memorial pages, which were later found to be done from spite and not humour (Walter 2011). Since the media using this as part of a moral panic from 2011 and most intensively in 2012, new terms have emerged such as 'Haters' (Bishop, 2013), which might be considered to cover those trollers who are Snerts, E-Vengers and Iconoclasts (Bishop, 2012b). The latter of these, Iconoclasts, are considered by the CPS to not necessarily be performing illegal acts, even if they are offensive and cause cognitive dissonance (Starmer, 2013).

1.1. *More regulation or just more 're-wording'?*

There has long been a debate about whether the Internet is best left to self-regulate through its own means, or whether it is necessary to involve outside agencies to interfere in the 'constitution' of cyberspace in order to protect the well-being of Internet users (Bishop 2011). It is clear, however, that the appetite for introducing legislation is often driven by the media of the day and the perception of the adequacies of the police and other authorities in reacting to so-called 'moral dilemmas'. Much like one saw in John Major's time with the so-called 'video nasties' and computer hacking, the interview referred to above served the needs of the media, looking for new ways to manipulate misunderstanding around information and communications technology to further their audience figures. This was to the delight of newly-through-the-door Members of Parliament such as Steve Rotheram, the MP for Liverpool Walton, as there was now something the politicians could get their teeth into to divert from the true causes of Internet abuse, or flame trolling. Indeed, rather than accept it was caused by lack of police prioritisation and a further manifestation of economic turmoil, as had been seen on numerous occasions since the 1920s, Mr Rotheram took this out of context. He was quoted in the Liverpool Echo as saying: 'the specific abuse and misuse of these social cyber-mediums could not have been foreseen.' And that: 'The Telecommunications Act 1984 and the Communications Act 2003 both preceded the introduction of social media such as Facebook (2004) and Twitter (2006). In fact, if one were to look at Figure 1, it can be seen that the marginal increased interest in trolling and cyberbullying is

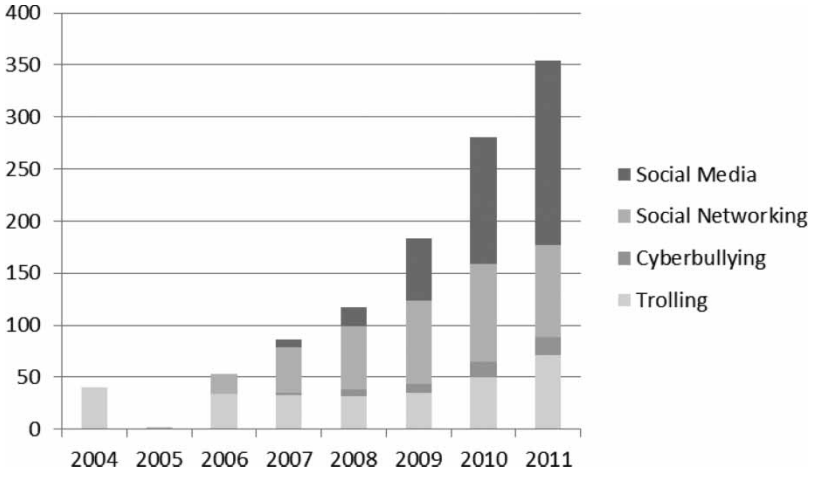

Figure 1. Trends of search terms on Google and Google News.

proportional to the increased interest in social networking and social media. So while factually incorrect, it is easy to see why legislators might not know the difference between the harassment via telecommunications under Margaret Thatcher resulting in new legislation, and harassment on the Internet and by text message under Tony Blair, again resulting in new legislation, which are merely platform based.

2. A review of Electronic Message Fault and associated Case Law relating to flame trolling in Great Britain

Calls for new legislation by novice MPs, such as Steve Rotheram who following the 'R.I.P Trolling' of the family of his constituent, Georgia Varley, were made in the UK Parliament (UK Hansard, HC Deb, 17 September 2012, c759). This might be considered understandable, as there where no arrests or cautions to show the family justice was being done in the case of Georgia Varley, even though they had been done in similar cases (e.g. an 18-week sentence given to Sean Duffy under the MCA for trolling Natasha MacBryde's memorial website). But equally, such calls are unnecessary, and in fact, as this paper shows, there is more than enough legislation on the statute books that can be used more effectively, as at present such legislation is being disproportionally used by the police. For instance, the Telecommunications Act 1984 was known to be widely applicable beyond its original scope, such as to the Internet (Akdeniz 1997), until it was replaced by the Communications Act 2003. Equally, the Malicious Communications Act 1988 has seen a surge in use since the introduction of Facebook, being used to penalise many people for 18 weeks in prison for R.I.P Trolling (Bishop 2012b).

2.1. *The Thatcher and Major Conservative Governments (1979–1997)*

The policy of the Thatcher Governments of the 1980s towards telecommunications was that of increased competition in order to also achieve increased access. This was evidenced by the passing of the British Telecommunications Act 1981. This was evidenced by the passing of the British Telecommunications Act 1981 (Hills 1989). This Act increased access to technology through greater private sector involvement in public communications

networks. It also resulted in increased computer and data misuse, now called trolling. Even so, at this point in history the term 'trolling' did not relate to the sending of offensive messages as it does at present. There was a need to tackle the misuse of telecommunications networks within 3 years of BT improving access to such services, which later became known as trolling, in the form of Section 43 of the Telecommunications Act 1984 (TA). This provision can, for instance, be interpreted with regards to modern conceptualisations of Internet trolling. Indeed, in the case of R v Brent (2008) in Wales, the TA was used to prosecute someone who posted menacing messages about a police officer, even at a time when the law was not regularly used for civilian victims of Internet abuse (Bishop 2012b). Debate followed about whether the case was legal, because Section 43 of the TA was repealed in 2003. It was reported in 2012 that similar abuse by an Essex police officer against a war veteran required only an apology and not the legal action Brent suffered. One could consider that the law was only being applied to those grossly offensive, menacing, obscene or indecent messages posted by people unprotected by professional codes of conduct, or without status as public sector workers.

2.1.1. *Criminal evidence and communications snooping legislation*

The Police and Criminal Evidence Act 1984 introduced a provision of making electronic documents that were tampered with through improper use of communications systems inadmissible as evidence in court. This created difficulty with regards to providing evidence of computer misuse and was later repealed by the Youth Justice and Criminal Evidence Act 1999. A year later, the Interception of Communications Act 1985 was passed to enable, as it suggests, the interception of messages sent via an electronic communications network. This was in order to overcome difficulties in gathering evidence for electronic message faults. It carried out a similar function to the far more extensive Regulation of Investigatory Powers Act 2000, which repealed and replaced much of it.

2.1.2. *Public order, malicious communications and fair comment*

The reduced application of mens rea in the Internet age has resulted in greater convictions of Internet trolling. In criminal cases where the Public Order Act 1986 is used, strict liability is often applied, where it is only for the respondent to have posted the electronic message for it to be considered a fault. It applies even if one is caught up in the moment, as the 'intention' in the form of planning the flame trolling is not necessary. Atkins v DPP [1989] Crim. L.R. 581 found that under s.4 of the Public Order Act a person had to receive a message from the sender or someone acting on their behalf, and simply being retold the message does not fall within the Act. This section of the Act has complexities in its application to flame trolling as it is uncertain whether the reference to a person outside a dwelling that needs to receive the message includes someone using ubiquitous technology such as a mobile phone.

The POA was updated in 1994 where Section 4A was inserted by the Criminal Justice and Public Order Act 1994. Section 4A now prohibits 'intentional' harassment, alarm or distress. This provision was used in 2012 to prosecute a youth who was studying at Swansea University who posted racist remarks on Twitter following being rebuked by others for posting an insensitive joke on the platform (Bishop 2012b). The youth, Liam Stacey, served half of his 56-day prison term, after being prosecuted under this provision. A related bout of racist flame trolling, by professional footballer Rio Ferdinand, who called another black footballer, Ashley Cole, the racist term 'choc ice', resulted in his being

disciplined under a professional code of conduct and not criminal law. His comment means 'white on the inside black on the outside', which Ferdinand posted because Cole had defended his team mate John Terry in court. Ferdinand received a £45,000 fine from his professional body, the English Football Association. Liam Stacey on the other hand faced a ban from Swansea University Campus in addition to being given a criminal record for what were reported by ITV News as 'drunken actions'.

The Copyright, Designs and Patents Act 1988 prohibited the misuse of the copyrightable intellectual property of others. It introduced a protection from accusations of an electronic message fault by virtue of Section 30. This section provides that 'Fair dealing with a work for the purpose of criticism or review' 'does not infringe any copyright in the work provided that it is accompanied by a sufficient acknowledgement.'

The Malicious Communications Act 1988 (MCA) prohibited the sending of a letter or an article that was indecent, offensive, or threatening with the intention of causing distress or anxiety to the recipient. Law in Great Britain generally follows a literal interpretive approach, rather than using 'proportionality' as in other jurisdictions such as Germany. This has resulted in the Act being difficult to apply to flame trolling, as it was not until the Criminal Justice and Police Act 2001, discussed in the next section, that this was explicitly applied to electronic communications. The application of the MCA in DPP v Connolly [2008] 1 W.L.R. 276 involved the respondent being found guilty of sending a grossly offensive and indecent message. The case found that a message needs to be capable of causing harm to the person (i.e. malum reus), and not simply be offensive. In this case a picture of an aborted foetus with a political message was sent to pharmacists. The court found that had it been sent to an abortion surgeon it would have just been a political message, but as it was sent to those who would find it shocking then the act was prosecutable.

The Defamation Act 1996 has made it the sysop's (i.e. website owner's) responsibility to remove content that is defamatory. This means that the sysop's prerogative in permitting free speech can be de facto removed if the threat of legal action is credible. Bunt v Tilley & Others [2007] 1 W.L.R. 1243 found that the defence is waived if the sysop is told a message is false and they do not remove the content, where they have 'knowing involvement in the process of publication of the relevant words'. This opens the sysop up to being subject to a civil injunction, for which the burden of proof is on them. They could also be criminally charged under Section 127(2)(a)-(b) of the Communications Act 2003, where the burden of proof then falls on the prosecutor. Godfrey v Demon Internet Ltd [2000] 3 W.L.R. 1020 upheld this by saying that as the internet service provider (ISP) in question, Demon, was told defamatory materials was being hosted on their platform, they were liable for not removing it. The judgement has brought into question the right of presumption of truth in free speech where a sysop or their ISP must remove anything said to be untrue and raises the issue in relation sysops as public defenders that protect free speech (discussed earlier).

2.1.3. *Privacy and computer misuse*

Privacy and computer misuse also come into the scope of sysop prerogative and consumer protection. Prior to the Data Protection Act 1984 (DPA1984), British law did not have a statutory right to privacy (Ellis and Oppenheim 1993). The DPA1984 was the first Act to address this right, albeit in the limited area of the automatic processing of personal data. This Act was introduced among a growing concern around privacy issues and a growing public and media appetite for protection (Gavison 1979).

The Computer Misuse Act 1990 (CMA) was introduced in the wake of a series of computer hacking incidents as a Private Members Bill, which was later supported by the

Government. This was despite a comprehensive report by the Law Commission, which found that as new technology comes about it does not 'challenge the effectiveness of current laws, several of which were drafted before computing became prevalent, and that victims of computer misuse should receive additional protection under the law' (Tan and Newman 1991). Whilst it was originally directed at hacking, the CMA has potential uses for electronic message faults. The appropriate provision for this was s.1, which was later amended by the Police and Criminal Justice Act 2006. An unauthorised Troller in this regard could be an 'E-Venger' (Bishop 2012b), which is a type of person that once banned from a website regains access to disrupt the community, often using a pseudonym (Bishop 2008). This was not what the CMA originally intended, which was to cover people who sent viruses or used others' credentials to gain access to a system. However, if one considers an 'Internet death penalty' to be designated to the user and not their account, then signing up to another account, especially to flame troll, could be considered unauthorised access. Equally, a Troller who is a 'Chatroom Bob', who posts kudos trolling messages to gain the trust of others in order to seduce them (Bishop 2012b) could also be covered. This could include those Chatroom Bobs who gain unauthorised access in order to seduce or abuse children (Bishop 2012c). This is often done by them deceiving as to their genuine identity. It could therefore be used more extensively than the anti-grooming laws made under New Labour and discussed later, if s.2 of the CMA is used with this or other law. Indeed, there was support in the House of Commons for using the CMA to prosecute kudos trolling by Chatroom Bobs, in particular those who use telecommunications systems to dupe unsuspecting persons into using premium telephone services. For instance, Liberal Democrat MP Richard Allen said on the 25 June 2004, 'I think that a criminal prosecution under the CMA would, in many cases, be far more effective as a discouragement for those who operate in the rogue dialler market than any fining that takes place through ICSTIS. So I hope that the Government are robust in making sure that CMA prosecutions take place.' These so-called rogue diallers could be considered Chatroom Bobs because they communicate a message pleasing to the mobile phone user (i.e. kudos trolling) in order to get them to use a premium number that costs them a lot of money.

2.2. *The New Labour Governments (1997–2010)*

In 1993, Tony Blair's New Labour movement conceived a policy of being 'tough on crime and tough on the causes of crime', to break with key aspects of past Labour policy (Downes). After the election of the successive New Labour Government, flame trolling became regarded as such a severe breach of 'Netiquette' that some Internet access providers prohibited it under penalty of 'Internet death'. That is, the threat of cutting off the offender's access and thus limiting their network neutrality rights (Robertson 2006). Such persons who are overzealous with such threats are called, 'Banhammers'. New Labour's flagship legislation for dealing with electronic message faults was the Communications Act 2003 (Datta and Acar 2010). Essential to New Labour's cybercrime agenda was acceptance of the claim that cyberspace is not simply an extension of real space and that the criminalisation of Internet abuse needed to take a different approach to hate crime than if it was committed in-person (Guichard 2009). Whether this is a reasonable approach to take is questionable, as this section will explore. Many of New Labour's laws relating to anti-social behaviour and harassment can be as equally applied to Internet misdemeanours as they can to offline misdemeanours. In particular, the usage of fixed-penalty notices and Anti-social Behaviour Orders (ASBOs) will be explored. There are many Acts not covered in this section, such as s.47 of the Wireless Telegraphy Act 2006, which have dedicated provisions to specific offences that could be used to

prosecute electronic message faults, which are too specialist to form part of this paper's general model. Some of these are discussed by Datta and Acar (Datta and Acar 2010).

2.2.1. *Protection from Harassment Act 1997 and Sexual Offences Act 2003*

The Protection from Harassment Act 1997 (PHA) was introduced due to a perception that existing legislation was not enough for the prevention of stalking, and in particular cyber-stalking. The Act criminalised harassment explicitly. Only a year previous to the enactment of the PFA, the case of R v Johnson [1996] 2 Cr App Rep 434 resulted in a ruling that the common law offence of 'public nuisance' was adequate enough for the prosecution of a person who used communications services to harass others. The Court adjudicated in relation to a man who contacted a number of women by phone who did not want to receive those calls. In order to determine whether something was a public nuisance, they said: 'It was necessary to look at the cumulative effect of the telephone calls, made to numerous ladies on numerous occasions'. This suggests support for the principle of 'pertinax reus' identified earlier.

Section 125 of the Serious Organised Crime and Police Act 2005 inserted a provision into the Protection from Harassment 1997 in the form of Section 1(1A). This made it illegal to harass someone by proxy, such as by getting a sysop to remove content they are under no legal obligation to, in order to cause harm to another. It also inserted a Section 3A into the PHA so it was possible for the right to a civil injunction against persons in breach of s.1A in the civil courts to be enacted in relation to this part. This provision is usually used as a deterrent, rather than leading to court action. Even though it offers the chance to step in where the criminal law system fails, often, the application of the common law in relation to the PHA is disjointed and inconsistent. For instance, in the case of Reece Messer, who posted a hurtful message to Olympic diver Tom Daley, he was given a harassment warning, but when Tom Daley called him and all his other follows an 'idiot' back, and also retweeted the message for all to see, he was not given a similar warning.

The Sexual Offences Act 2003 brought wide-reaching changes to previous legislation on sexual offences. It included new provisions relating to sex offences online, such as grooming. A successful prosecution under this act for grooming occurred in R v T (2005) EWCA Crim 2681, where a paedophilic Chatroom Bob was found guilty of befriending an 8-year-old girl and given an 8-year sentence. One might question whether the failure to bring cases under the Computer Misuse Act for unrealised acts of grooming was negligent on behalf of the government prior to this Act. For instance, a jury, which usually acts in the interests of justice, might be persuaded that a Chatroom Bob speaking to a child with the intention to harm them for their own pleasure over the Internet could be constituted 'unauthorised access with the intention to commit further offences', which is an offence under the CMA.

2.2.2 *Regulation of Investigatory Powers Act 2000 and Electronic Communications Act 2000*

The effect of anonymity on the Internet was one of the drivers for the Regulation of Investigatory Powers Act 2000 (RIPA), as it was difficult to prosecute offenders on the Internet where their identity was concealed and the authorities did not have sufficient powers to deal with this. Dorset County Council and other local authorities have used RIPA to ascertain whether or not families who had applied to send their children to particular schools were in fact living in the catchment area (Bryce et al 2010). There is no reason therefore why

something as much an invasion of privacy as what Dorset council did can be achieved using RIPA, why the same provisions cannot be used to identify those who commit flame trolling online.

Published the same year as RIPA, the Electronic Communications Act 2000 (ECA) introduced a new regulatory regime to allow documents signed electronically to have the same validity as printed ones. The Act is supplemented by the Electronic Signatures Regulations 2002. The technology legalised under the Act, based on an EU directive, called 'advanced electronic signatures', is a common part of desktop packages such as Adobe Reader. Such signatures, if used with websites could offer a more effective means of preventing online abuse, even permitting anonymity, if that digital signature was registered with a provider. By virtue of s.16(4) of the ECA that came into force under the 25 May 2005 and s.14, the UK Government no longer has any powers to compel this to happen, and any such use would be voluntary and market led, which creates the difficulty that RIPA will be needed to 'unmask' flame trollers, which the authorities are reluctant to use.

2.2.3. *Communications Act 2003*

The Communications Act 2003 (CA2003) was one of New Labour's strongest pieces of legislation relating to flame trolling. It introduced two whole sections in relation to it – s.127 on 'Improper use of a public electronic communications network' and s.128 on 'Notification of misuse of networks and services', much of it repeating earlier legislation. For instance, s.127 resembles the Telecommunications Act 1984, except that 'electronic communications network' is used in place of 'public telecommunication system' and if one were to compare s.43 of the TA with s.127 of this Act, one can see it was indeed a simple transfer from one to the other. A person guilty of an offence under s.127 of the CA2003 for improper use of a public communications network is liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine or to both for each offence. The test for 'grossly offensive' has been set in *DPP v Collins* [2006] 1 WLR 2223 in the House of Lords. It is on the basis of whether the message would cause gross offence to those to whom it relates, who need not be the same as those who receive it. The case of DPP v Connolly [2008] 1 W.L.R. 276 established that the persons to whom the message was directed would have to be grossly offended for a prosecution to be made as opposed to the message being grossly offensive to those who were not the intended recipients. The case of DPP v Chambers (2012) established furthermore that a message had to cause apprehension in someone who received it in order for prosecution to be brought, and that *mens rea* did not apply, as argued earlier by Bishop (Bishop 2010). These three cases establish that even if a message is offensive, unless it passes the test for *malum reus* (i.e. it causes harm to someone) then prosecution under Section 127 of the CA2003 is not possible.

2.2.4 *The Crime and Disorder Act 1998, Anti-social Behaviour Act 2003, Criminal Justice and Immigration Act 2008, Crime and Security Act 2010*

The Crime and Disorder Act 1998 (CDA) created Anti-social Behaviour Orders (ASBOs) that operate as personal injunctions for particular acts of anti-social behaviour, which if the injunction is breached can result in jail-terms of up to 2 years. The provisions relating to ASBOs in the CDA were updated by the Anti-social Behaviour Act 2003, Criminal Justice and Immigration Act and the Crime and Security Act 2010, and for simplicity the CDA will be discussed as amended by this. The definition of 'anti-social behaviour'; was left deliberately vague, and this has led to ASBOs being used in a number of situations

beyond the use for which they were originally designed, but their use has huge regional difference, and is primarily driven by local policy makers. This has the advantage that such orders could be used for persistent trolling where offenders are given a chance, outside the criminal law system in some instances, to improve their behaviour or face a 2-year jail term (Bryce et al 2010). One might argue the most effective means of using an ASBO is the civil route, which can be brought by local authorities. This route requires the same burden of proof as in criminal cases according to the UK's public prosecutor, as found in the cases of *Clingham v Royal Borough of Kensington & Chelsea [2002] UKHL 39 and R v Manchester Crown Court (ex parte McCrann)* [2003] 1 AC 787. The CDA as amended makes it clear under s.1c that in order for people under the age of 16 to receive an ASBO their family circumstances have to be taken into account. This might act as a disincentive to law enforcers who wanted to criminalise youths at a time of their life when they are often impressionable. Equally s.66A of the CDA allows for a special type of caution for youths where an offence under another Act is committed, which reduces criminalisation of them, and might be an appropriate 'short sharp shock' for those who might otherwise go too far with flame trolling.

2.2.5 *Criminal Justice Act 2003 and Serious Crime Act 2007*

The major provisions of the Criminal Justice Act 2003 in relation to electronic message faults would be those in Part 12 relating to sentencing. As has been seen there are plentiful statutes that could be used to prosecute flame trolling as an EMA. The CJA provides for certain factors to be taken into account in any trial where a case of flame trolling is being heard. This includes in the case of Section 143 the seriousness of the offence. It might be helpful to consider this Act in terms of the Serious Crime Act 2007, under which a number of flame trolling offences were brought as a result of the UK Riots in August 2011. Most notable were the cases of Jamie Counsel and Anthony Gristock, who set up Facebook pages in the heat of the moment that attempted to encourage riots to the streets of Cardiff and Swansea. The Section 44 offence of encouraging or assisting an offence appears to be the strict liability in that neither Jamie Counsel or Anthony Gristock actually caused any rioting. Their sentences were 4 years and 3.5 years imprisonment respectively, and one might question the severity of these penalties when no one was harmed, and they were unlikely to reoffend. A notable comparison is that of Sean Duffy, a perpetual flame troller who was sent to jail for 18-weeks at a time under the MCA, when an offence of persistently making use of an electronic communications network for 'the purpose of causing annoyance, inconvenience or needless anxiety to another', exists under Section 127 of the Communications Act 2003. The repeated harassment of families who set-up memorial pages might be considered to be more severe within the meaning of the CJA as compared with the offences committed by Jamie Counsel and Anthony Gristock, of which few were aware.

2.2.6 *Criminal Justice and Police Act 2001 and Police and Justice Act 2006*

The Criminal Justice and Police Act's main purpose in relating to trolling was to update the Malicious Communications Act 1998 to make it explicit that references to letters and articles contained within it included those that were electronic in nature. It did this by inserting, 'electronic form' and 'electronic communication' after these terms as per the appropriate context. The necessity of doing this was again only due to the persistence of the British legislatures and judiciary not making use of the European proportionality principle in place of the traditional

literality. Had the rule of proportionality been used to interpret the MCA then 'article' would have been easily interpreted as a message sent via a public communications network.

The Police and Justice Act 2006 (PJA) was the first successful amendment of the Computer Misuse Act 1990 (CMA) aiming to respond to the worrying level of UK cybercrime (Goel, Sharma, and Rastogi 2010). Specifically, s.36 of the PJA amended the CMA to cover distributed denial of service attacks and other potential computer misuses. Whilst it may not have been intended as such, s.2(b) could be applied to those persons who engage in disruptive trolling, and there may be opportunities for it to do so. Take the case of Iconoclasts, who engage in spamming links to other websites. It has been argued that these 'disturbances may hinder the communication' between members of the community (Zhao 2010). E-Vengers often carry out their vengeful attacks acting as what can be termed, 'Masked E-Vengers,' which is where their identity is kept secret. These could be referred to as 'forced empathic social engineers' as they seek to assert damage to a community, as a cathartic process, which may impair the trust between the site and their users, which 'hinders public acknowledgment' (Carroll 2009), and which may therefore fit within this Act.

An important part of the PJA was that it introduced a requirement for the councillors on a designated 'crime and disorder committee' of a local authority to scrutinise the effectiveness of their council at tackling crime and disorder. In terms of flame trolling this could be used to hold council officials to account if they refuse to use powers such as ASBOs and fixed penalty notices to deal with flame trolling.

2.3. *The Coalition Government (2010–)*

The Coalition Government formed in 2010 of Conservative and Unionist members and Liberal Democrats has presided over one of the greatest growths in abuse via public communications networks since the privatisation of British Telecom in 1981. Called 'trolls' by the mass media, the rise of abuse of people once not accessible, such as celebrities on Twitter, became as common as the abuse of ordinary people and, often, their families if they were deceased, even in tragic circumstances. The difference between the Coalition Government and the previous one was an acceptance that the criminal framework was adequate, but that enforcement was inadequate. The Coalition's commitment to devolving powers to the lowest level, even to citizens themselves, appears to continue more the avoidance of criminalisation seen under Margaret Thatcher and Tony Blair, and more so a continuance of the programme of Gordon Brown towards a more enabling state, as discussed by Datta and Acar (Datta and Acar 2010). Through merging or dissolving many agencies, the Coalition attempted to make it easier to have extensive laws enforced with the help of citizens in terms of putting pressure of law enforcement authorities.

2.3.1 *The Localism Act 2011 and Police Reform and Social Responsibility Act 2011*

The *Localism Act 2011* (LA) was introduced by the Coalition to make it easier for local authorities and the public to provide services at a local level. Whilst the LA made it possible for a local authority to transfer its powers to another public authority, the Act made it clear that those powers introduced by New Labour in s.9 of the Police and Justice Act 2006 had to be conducted by a local authority themselves. This required local councillors to be responsible, via a scrutiny committee to ensure that issues of crime and disorder, which could include flame trolling, are considered properly by officers. The *Police Reform and Social Responsibility Act 2011* (SRA) introduced the creation of Police Crime Commissioners in England & Wales, which means that duties once performed by the committee

of a police authority will be given to a single elected official (i.e. a PCC). This will no doubt increase the likelihood of demands being put on them to ensure Police Constables act in the interests of all and not only in the interests of those that share the same elite background as them, but also focus more on the priorities of the many. The public, no doubt with the aid of the media, will be putting huge pressure on the new PCCs to tackle issues, which may not always reflect balance, but may in fact make moral panics that much more damaging. Issues such as reducing taxes normally targeted at councils will become focused on the police, and they will be expected not only to tackle crime against those from influential white-collar backgrounds, but disadvantaged blue-collar ones also.

2.3.2. *Latest developments*

At the time of going to press, a number of Bills in relation to Internet trolling were going through Parliament. These included the Online Safety Bill, the Defamation Bill and the Crime and Courts Bill.

The Online Safety Bill sought to introduce a number of bureaucratic measures on sysops requiring them to provide a service that 'excludes pornographic images; and to require electronic device manufactures to provide a means of filtering content'. The Bill would have required sysops not to provide pornographic content unless someone opts-in. The major difficulty with the Bill is that it does not define the term, 'pornographic'. Could this include 'soft porn', like one might find on page3.com? The Bill's provision requiring producers of electronic devices to provide a means of filtering content might better be achieved through using Internet security software, which could rate content in terms of its gravity, such as whether it could be grossly offensive or just simply offensive.

In the case of the Defamation Bill, the Government through Section 5 sought to end the situation where sysops could be liable for defamation, providing that they hand over the personal details of the person making the untrue comments. The advantage of this piece of legislation would have been free speech, which may include true and honest criticisms, and which would be more protected as sysops would be less likely to remove the content. There is a huge cost to bringing defamation claims, and they are often pointless if the respondent does not have money to pay damages with. As a result, it means that sysops will be less likely to remove content, even if it is untrue and abusive, because they know it is unlikely to be challenged. This therefore means that any flame trolling on an Internet site is going to more likely be handled by law enforcement agencies such as the police.

In response to the lack of co-operation between government agencies for serious Internet trolling, like the way 'Chatroom Bobs' post flattering messages (i.e. kudos trolling) in order to gain the trust of someone to exploit them (Bishop 2012b, 2012c), the Coalition Government tabled the *Crime and Courts Bill* (CCA). This aimed to bring under one roof disjointed bodies that lacked co-operation, such as the Serious Organised Crime Agency (SOCA), the Child Exploitation and Online Protection Centre (CEOPC), and the crime fighting functions of the National Policing Improvement Agency (NPIA). The need for this new 'National Crime Agency' (NCA) could be an important response to the fact that it is ineffective, to use this example, to expect the police to gain all the knowledge of flame trolling that would be needed, and also to perform the other duties of policing, meaning an inter-agency approach such as that seen in healthcare might be the answer (Wall 2007). It has been strongly argued that national law enforcement bodies with powers such as SOCA had are better structured in terms of their abilities to understand cybercrime because of their breadth of knowledge (Segell 2007), and should adopt less of a role of informing local police and instead take over their role for prosecuting high-tech crimes such as flame

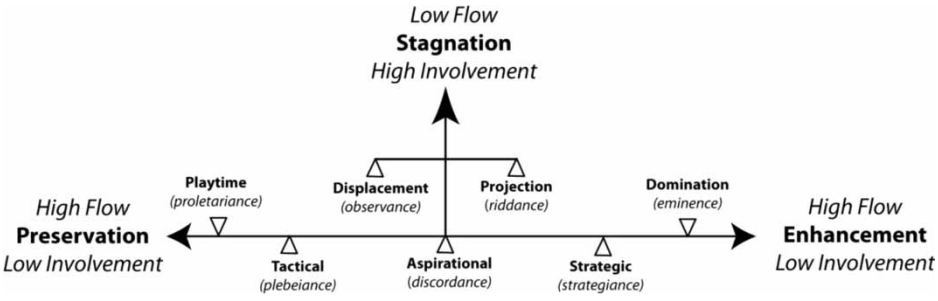

Figure 2. The persuasion continuum for trolling.

trolling (Bishop 2012b). The NCA makes this a possibility, and with the Police Crime Commissioners facing huge decisions over budgeting and the priorities of citizens, it might mean that effective use of financial resources will include involving this new crime fighting agency.

3. Recommendations

In order to make more effective use of the Coalition Government's reforms, it is going to become essential for the use of the law to be prioritised so that free speech is protected and people are not unnecessarily prosecuted because they make inappropriate or offensive comments, which human beings have done for thousands of years. Strategic thinking by the police and other law enforcement agencies could mean that Minor flame trolling is distinguished from Major flame trolling, and that the choice of legislation is based on the magnitude of the offense, and its gravity in terms of how it affects other people. To understand these, an effective model that one can consider is the Persuasion Continuum (Bishop 2012b), as presented in Figure 2. This shows how those with limited expertise at using the Internet (i.e. laypersons) are as susceptible to making an instant decision to troll as those with a lot of experience (i.e. authorities). Those users who have a limited amount of knowledge on trolling (i.e. tactical trolls) manifest as Plebeians, as they know enough to have an opinion, but not enough to actually realise what they know. People at this end of the continuum are more likely to commit Minor offences, and are more likely to move onto the next step of becoming an expert, if they can overcome the 'aspiration trap', which is where because of their circumstance they are not able to achieve what they want.

Clearly the closer to Domination Trolling one gets, the less it is possible to unintentionally injure oneself through one's own actions, as the more Major offences are likely to be more carefully planned and considered actions become less viewed as minor lapses of judgement. In the context of the Persuasion Continuum, Minor refers to a guilty act where there is a less serious guilty injury (malum reus), such as a standard flame. This should avoid the misuse of the CA2003 for prosecuting anyone who says something that could be offensive even if was not intended to be, because of the test of 'grossly offensive' in DPP v Collins (2006). Major, on the other hand, refers to a guilty act where there is a more serious guilty act, such as inciting racial hatred as in the case of R v Stacey (2012), or otherwise where the actions are persistent (i.e. meet pertinax reus), or both. Table 1 provides a framework for interpreting law in the United Kingdom relating to Internet trolling to consider issues such as magnitude and potential gravity. This extends the one in Bishop (2012e) to take account of the new guidelines on prosecuting cases involving communications sent via social media by the Crown Prosecution Service (Starmer, 2013). As can be seen, this

Table 1. The Trolling Magnitude (TM) scale and offence matrix

Type	Potential Gravity	Severity	CPS score	Appropriate legal provision
TM1 – Playtime Cyber-bantering (Cyber-trolling)	In the moment and quickly regret (finem facere)	**Minor** (TM 1.00-1.49)	4	Fixed penalty notice of £75
	Grossly Offensive, Indecent, Obscene or Menacing	**Major** (TM 1.50-1.99)	4	Fixed Penalty Notice of £150
TM2 Tactical Cyber-trickery (Cyber-trolling)	In the moment but don't regret and continue (animus restituendi)	**Minor** (2.00-2.49)	1	Common law detention for breach of the peace as permitted by s.40(1) of the Public Order Act 1986
	Harassment, Alarm or Distress	**Major** (TM2.50-2.99)	2	ASBO under s.1 the Crime and Disorder Act 1998.
TM3 – Strategic Cyber-bullying (Cyber-stalking)	Go out of way to cause problems, but without a sustained and planned long-term campaign.	**Minor** (TM3.0-3.49)	2	Harassment warning under s.4 or s.4A of the Protection from Harassment Act 1997 or caution under relevant legislation.
	Harassment, Alarm or Distress (ad vita aut ademptio).	**Major** (TM3.50-3.99)	2	Custodial sentence under s.127 of the Communications Act 2003 or s.1 of the Malicious Communications Act 1988, of 26 to 52 days or up-to 18 weeks.
TM4 – Domination Cyber-hickery (Cyber-stalking)	Goes out of the way to create rich media to target one or more specific individuals	**Minor** (TM4.0-4.49)	2	Restraining order under s.5 of the Protection from Harassment Act 1997 or related court orders, such as under The Family Law Act 1996.
	Grossly Offensive, Indecent, Obscene or Menacing (ad vita aut ademptio)	**Major** (TM4.50-4.99)	3	Custodial sentence under s.127 of the Communications Act 2003 or s.1 of the Malicious Communications Act 1988, for up to 6 months for each act. Related custodial sentences for breaching a court order.

new table is updated to include courses of action recommended by CPS and the Attorney General. These include the associated 'initial assessment' scores of the CPS (ranging from 1 to 4) to determine whether a case should be brought at all against trollers (Starmer, 2013). A CPS score of 1 is met if an act of trolling may constitute credible threats of violence to the person concerned or damage to property. In the case of the modified trolling magnitude scale in Figure 1, this only falls within a TM of 2.00 to 2.49. This is because the appropriate action is to detain the person so they cannot carry out further offences. A CPS score of 2 is for those trolling acts which specifically target an individual or individuals. This correlates to TMs of 2.50 to 4.49. As can be gathered from this, there is such a wide scope to this CPS score, that law enforcement authorities might want to use the TMS for more specific guidance in order to be proportionate. The CPS score of 3 only applies to a TM of 4.50 to 4.99 and a PS score of 4 applies to TMs of between 1 and 1.99. The CPS score of 3 applies to those trolling acts which may amount to a breach of a court order and thus fall into the maximum of the TMS (TM 4.50 to 4.99). This is likely to be where the person before the court meets 'pertinax reus', through committing previous offences at a lower TM. According to Starmer (2013), a CPS score of 4 refers to communications which are not severe enough for the other grades, but which nevertheless may be considered grossly offensive, indecent, obscene or false. In the TMS these correlate to a TM of 1.00 to 1.99, which are best suited to a fixed penalty notice rather than criminal action, as these can be widely applied to a number of situations outside the scope and thresholds of statutory offences.

One can consider how the trolling magnitude scale might have been applied in 2012 when a number of young people were prosecuted for Internet trolling. In the case of Playtime Trolling, the cases of Reece Messer and Matthew Woods are most salient. Messer was given a harassment warning for telling Olympic Diver Tom Daley that he let his late father down by not winning a medal at the London Olympics. It would have been more proportionate for Messer to have been given a fixed penalty of £75, if at all, as being a welfare claimant this would have affected him more than the criminalising of him by a society that has already turned his back on him. In the case of 19-year-old Matthew Woods, he was sentenced to 12-weeks in prison for making offensive jokes on his own personal Facebook page for his friends to see, which were about missing children Madeline McCann and April Jones. If one considers some of the offensive things said on televisions or in public houses, criminalising someone for being inappropriate with their words is totally out of proportion. The most Woods would have faced for a TM of 1.5 (CPS 4) is a fixed penalty of £150. This would also have been the most appropriate outcome in the cases of Liam Stacey and Daniel Thomas. In the case of the former he served 26-days in prison for posting racist remarks, whereas in the case of the second he faced no legal action for posting homophobic remarks of equal severity,

In the case of Tactical Trolling, there were a number of possible miscarriages of justices that would have been more appropriately dealt with under this magnitude. In the cases of Jamie Counsel and Anthony Gristock, these youths set up pages on Facebook during the UK riots of 2011 asking people to bring the riots to Cardiff. Few people saw these pages, but they resulted in the pair being sentenced to 4 and 3.5 years in prison respectively. It would have been more appropriate in both cases, where there was a TM of between 2 and 2.49 (CPS 1) for them to have been detained as soon as they posted their pages, but without charge and for a short period, to communicate the severity of their actions. A TM of between 2.5 and 2.99 (CPS 2) where an ASBO would have been served would have been more appropriate in the case of Joshua Cryer. In this instance the youth goaded Stan Collymore, who is a controversial footballer, known for his domestic violence against TV personality

Ulrika Johnson and his posting of sexual text messages, or 'sexts', was prosecuted under the CMA2003, but only served a community sentence in any case. Cryer's actions involved posting racist messages, and were isolated to Collymore. They were, however, conscious and sustained, with Cryer calling his actions 'a new hobby', unlike those of Liam Stacey which were in the moment. The judge in the case said Cryer was 'stupid' and that he should have 'known better'. As the flame trolling was sustained, it would have been more effective for Cryer to have been given an ASBO, which would have served as a deterrent as he would have faced 2 years in jail if he had reoffended.

In terms of Strategic Trolling, there have been a number of legal cases that could fall within this category of trolling. In terms of a TM of 3 to 3.49 (CPS 2), Staffordshire Police issued a harassment warning on an unnamed youth, who set up a fake Facebook profile to taunt the mother of a boy who had died tragically in a moped accident. The mother at first though her son was actually alive, until her abuser posted remarks saying her son had 'gone to hell'. A harassment warning of this kind might be appropriate for a single campaign against one person. However, as the Attorney General found later, the additional trauma in Agar's case might make the instance more substantial, putting it in the 'major' class of strategic trolling, as opposed to 'minor,' as was originally awarded. This is because it passes the test for 'pertinax reus' as it is "persistent" and thus falls within the Communications Act 2003. In 2012 Reece Messer trolled Olympic diver Tom Daley, saying that Daley let his late father down by not winning a medal, and was given an harassment warning. Using the new guidance in Starmer (2013), this message is more of the Iconoclastic in-the-moment kind (TM 1 to 1.99, CPS 4) and nowhere near the TM of 3.00 to 3.49 (CPS 2) that is necessary for a harassment warning. Consider the case of the musician, Adele, to whom – on the announcement of the birth of her baby – trollers posted vile remarks. One Twitter user said, 'Aw Adele gave birth to a baby. Is it fat and handicapped lol? Just murder it already lol', and another said, 'I'll go see her in the UK and kill her. And kill her baby.' Whilst other people might not find this offensive, to the target of this message it is. If one applies the case of DPP v Collins, it can be seen that even if a message was not received by the individual or group it was about; if they would be severely affected by it then the offence is prosecutable. These messages against Adele were not simply free speech, as they went beyond what one might expect within the meaning of DPP v Collins. A borderline case where an electronic message fault might fall below a TM of 3.5 (CPS 2) was that of Azhar Ahmed, a 19-year-old youth who posted on Facebook, 'all soldiers should die and go to hell'. Soldiers are among some of the most 'thick skinned' in society, even if a message of this kind about any other protected group might fall within the 3.5 to 3.99 (CPS 2) range.

The balance between whether an offence is in the TM range of less than 3.5 or greater than 3.99 could be done using the Equality Acts of 2006 and 2010 (EA2006, EA2010). If the individual targeted by a troller has a protected characteristic within the meaning of Section 4 of the EA2010, or a member of group within the meaning of Section 10 of the ES2006, then it would fall within this range, whereas if they do not, it falls below it. So as Adele had the protected characteristic of 'pregnancy and maternity' her troller should have been prosecuted, but as soldiers had no such characteristic then Azhar Ahmed at most should have faced a fixed penalty notice of £150 for a TM of 1.5 to 1.99 (CPS 4). It should be expected that members of the armed forces should be able to withstand such abuse within the meaning of DPP v Connolly, because they will have a very high tolerance. Even if Adele is a public figure capable of having a 'thick skin', celebrities according to Starmer (2013) are no less vulnerable or less deserving of respect than anyone else and a hierarchy of protected and unprotected groups might be inappropriate. If someone is not

used to being abused then they will have a low tolerance and be more open to feeling or being grossly offended.

Domination Trolling is the most severe of electronic message faults, where people go out of their way to be severely abusive. Considering the first grade of a TM of 4 to 4.99 (CPS 3), there are a number of cases that could have been dealt with more fairly under these provisions. One of the most obvious is that of Lee Francis Ball. Ball subjected his ex-girlfriend to a nine-month campaign where he verbally abused, belittled and humiliated her online. He left 'disgusting and demeaning' messages about her on Facebook, questioning her appearance, and had cosmetic surgeons contact her. The court punished Ball with two years of prison, which was not appropriate in this case as the TM was below 4.5. As Ball was unlikely to target anyone but his former partner, then it would have been more effective to have placed a restraining order under section 5 of the PHA, and he would only face prison for if he broke this, taking him over the 4.5 threshold.

4. Discussion

This paper has shown that, since the 1980s, successive governments in the United Kingdom have called it right in relation to legislation to tackle electronic message faults, regardless of what they are called by the media. The Telecommunications Act 1984 was the first act to make the distribution of grossly offensive, indecent or menacing messages through a communications platform. It was used in a number of cases before being replaced by the Communications Act 2003, which has identical provisions. With legislation such as the Public Order Act 1986, the Malicious Communications Act 1988 and the Protection from Harassment Act 1997 being used to prosecute electronic message faults such as Internet trolling, the question is not whether the police have the powers, but how they should use those powers to protect people from Internet abuse without their actions being seen to have a chilling effect on free speech.

This paper has proposed a Trolling Magnitude Scale in order to assess the severity and gravity of an electronic message fault, such as flame trolling. Using established principles in Internet and multimedia studies, four categories are presented to conceptualise an act and how it may give rise to a legal obligation, or otherwise. The scale suggests how the least severe of cases, where someone posts something they quickly regret, should have the least strict punishments, in this case a fixed penalty notice. This extends to the most severe, at a TM of 4, where the person committing the electronic message fault would have to go out of their way to perform the act, such as a long-term campaign of hate, or the production of a multimedia rich abuse message that took a lot of time to produce.

4.1. *Limitations and directions for future research*

This paper has reviewed the legislation that has existed since the 1980s in relation to electronic message faults such as flame trolling. It has considered the possibility of using a 'trolling magnitude scale' to allow the law enforcement to judge whether it is in the public interest to pursue an act of flame trolling through a particular piece of legislation, based on it meeting different thresholds for gravity and effort (i.e. flow/involvement). Future research could empirically verify this, such as to assess whether it is the case that the lowest and highest magnitudes place people more at risk from suffering from perceived grossly offensive, indecent and menacing messages. The paper has presented a number of case studies of youth Internet trollers. Future research could look at whether it is actually

youths that cause most flame trolling, or whether this is based more on media bias or public appetite for scapegoats.

Acknowledgements

The author would like to recognise the assistance of all persons who provided feedback on earlier versions of this paper. The Centre for Research into Online Communities and E-Learning Systems is an affiliate of Swansea University's Institute for Life Sciences, and supports a number of projects including the Trolling Academy and the Free Digital Project, the former focusing on online safety, and the latter the rights of young people in the information age.

References

Akdeniz, Y. 1997. "Governance of Pornography and Child Pornography on the Global Internet: a Multi-layered Approach." *Law and the Internet: Regulating Cyberspace* 223–241.

Barlow, J.P. 1996. *A Declaration of the Independence of Cyberspace*. San Francisco, CA: Electronic Frontier Foundation.

Bishop, J. 2008. "Increasing Capital Revenue in Social Networking Communities: Building Social and Economic Relationships Through Avatars and Characters." In *Social Networking Communities and Edating Services: Concepts and Implications*, edited by C. Romm-Livermore and K. Setzekorn. Hershey, PA: IGI Global.

Bishop, J. 2010. "Tough on Data Misuse, Tough on the Causes of Data Misuse: A Review of New Labour's Approach to Information Security and Regulating the Misuse of Digital Information (1997–2010)." *International Review of Law, Computers & Technology* 24 (3): 299–303.

Bishop, J. 2011. "All's WELL that ends WELL: A Comparative Analysis of the Constitutional and Administrative Frameworks of Cyberspace and the United Kingdom." In *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*, edited by A. Dudley-Sponaugle and J. Braman. Hershey, PA: IGI Global.

Bishop, J. 2012a. "The Psychology of Trolling and Lurking: The Role of Defriending and Gamification for Increasing Participation in Online Communities Using Seductive Narratives." In *Virtual Community Participation and Motivation: Cross-Disciplinary Theories*, edited by H. Li. Hershey, PA: IGI Global.

Bishop, J. 2012b. "Scope and Limitations in the Government of Wales Act 2006 for Tackling Internet Abuses in the Form of 'Flame Trolling'." *Statute Law Review* 33 (2): 207–216.

Bishop J. 2012c. "Taming the Chatroom Bob: the Role of Brain-Computer Interfaces that Manipulate Prefrontal Cortex Optimization for Increasing Participation of Victims of Traumatic Sex and Other Abuse Online."

Bishop J. 2012d. Tackling Internet abuse in Great Britain: Towards a framework for classifying severities of 'flame trolling'. In *The 11th International Conference on Security and Management (SAM'12)*, 16–19 July 2012, Las Vegas, USA.

Bishop, J. 2013. The effect of deindividuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater. International Journal of Cyber Criminology 7(1): 28–48.

Bishop, J. In Press. Representations of 'trolls' in mass media communication: A review of media-texts and moral panics relating to 'Internet trolling.' *International Journal of Web Based Communities*.

Bryce, T., M. Nellis, A. J. Corrigan, H. Gallagher, P. Lee, and H. Sercombe. 2010. "Biometric Surveillance in Schools: Cause for Concern or Case for Curriculum? *Scottish Educational Review* 42 (1): 3–22.

Carroll, J. M. 2009. "Conceptualizing a Possible Discipline of Human-Computer Interaction." *Interacting with Computers* 22 (1).

Datta, P., and W. Acar. 2010. "Software and Human Agents in Knowledge Codification." *Knowledge Management Research & Practice* 8 (1): 45–60.

Downes, D. "Toughing it Out: From Labour Opposition to Labour Government." *Policy Studies* 19 (3-4): 191–198.

Driscoll, C., and M. Gregg. 2008. "Broadcast Yourself: Moral Panic, Youth Culture and Internet Studies." *Youth Media in the Asia Pacific Region* 71–86.

Ellis, S., and C. Oppenheim. 1993. “Legal Issues for Information Professionals, Part III: Data Protection and the Media—Background to the Data Protection Act 1984 and the EC Draft Directive on Data Protection.” *Journal of Information Science* 19 (2): 85–97.
Gavison, R. 1979. “Privacy and the Limits of Law.” *Yale Law Journal* 89: 421.
Goel, A. K., G. R. Sharma, and R. Rastogi. 2010. “’Knowledge Management Implementation in NTPC: an Indian PSU.” *Management Decision* 48 (3): 383–395.
Guichard, A. 2009. “Hate Crime in Cyberspace: The Challenges of Substantive Criminal Law.” *Information & Communications Technology Law* 18 (2): 201–234.
Hills, J. 1989. “Neo-Conservative Regimes and Convergence in Telecommunications Policy.” *European Journal of Political Research*, Vol. 17, 1, 95–113.
Jansen, E., and V. James. 1995. *NetLingo: The Internet Dictionary.* Netlingo Inc.
Jansen, E., and V James. 2002. *NetLingo: The Internet Dictionary.* Netlingo Inc.
Kuipers, G. 2006. “The Social Construction of Digital Danger: Debating, Defusing and Inflating the Moral Dangers ff Online Humor and Pornography in the Netherlands and the United States.” *New Media & Society* 8 (3): 379.
Lessig, L. 1999. “The Law of the Horse: What Cyberlaw Might Teach.” *Harvard Law Review* 113 (2): 501–549.
Phillips, W. 2011. “LOLing at Tragedy: Facebook Trolls, Memorial Pages and Resistance to Grief Online.” *First Monday* 16 (12–5).
Robertson, R. 2006. “The Increasing Monopolization of Identity by the State: The Case of the UK and the US.” *Nationalism and Ethnic Politics* 12 (3): 373–387.
Segell, G. M. 2007. “Reform and Transformation: the UK’s Serious Organized Crime Agency.” *International Journal of Intelligence and CounterIntelligence* 20 (2): 217–239.
Starmer, K. 2013. *Guidelines on prosecuting cases involving communications sent via social media*. London, UK: Crown Prosecution Service.
Tan, L. M., and M. Newman. 1991. “Computer Misuse and the Law.” *International Journal of Information Management* 11 (4): 282–291.
Wall, D. S. 2007. “Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace.” *Police Practice and Research* 8 (2): 183–205.
Walter, T., R. Hourizi, W. Moncur, and S. Pitsillides. 2011. “Does the Internet Change how we Die and Mourn? An Overview.” *Omega: Journal of Death & Dying* 64 (4): 12.
Whine, M. 1997. “The Far Right on the Internet.” *The Governance of Cyberspace: Politics, Technology, and Global Restructuring*, 209–27. Oxford: Hart Publishing.
Zhao, Z., S. Feng, Q. Zeng, J. Fan, and X. Zhang. 2010. “Personalized Knowledge Acquisition Through Interactive Data Analysis in E-learning System.” *Journal of Computers* 5 (5): 709.