Felipe Romero-Moreno[1]

Lecturer at Hertfordshire University, School of Law, Hertfordshire UK

The Digital Economy Act 2010: Subscriber Monitoring and the Right to Privacy under Article 8 of the ECHR

Abstract

This paper critically assesses the compatibility of s3 Digital Economy Act 2010 (DEA) with Article 8 of the European Convention on Human Rights (1950) (ECHR). The analysis draws on Ofcom's Initial Obligations and two UK cases, namely: *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills*,[2] and *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others*.[3] It argues that the implementation of this obligation allows directed surveillance of subscribers' activities without legal authorization under the Regulation of Investigatory Powers Act 2000 (RIPA).[4] It also analyses compliance with the Strasbourg Court's three-part, non-cumulative test, to determine whether s3 of the DEA: is firstly, 'in accordance with the law;' secondly, pursues one or more legitimate aims contained within Article 8(2) of the Convention; and thirdly, is 'necessary' and 'proportionate.' It concludes that unless the implementation of s3 of the DEA required the involvement of State authorities and was specifically targeted at serious, commercial scale online copyright infringement cases it could infringe part one and part three of the ECtHR's test, thereby violating subscribers' Article 8 ECHR rights.

Keywords: Digital Economy Act, Privacy, Copyright

Introduction

In June 2012, Ofcom published the Revised Draft Initial Obligations Code (hereafter 'the Ofcom Code'), outlining how the Digital Economy Act 2010 (DEA) would work. If any revisions to the Ofcom Code were to be made, Ofcom would, subject to the Secretary of State approval, produce the final Initial Obligations Code. This Code would then be laid in Parliament.[5] The DEA imposes, in s 3, an obligation on Internet Service Providers (ISPs) to notify subscribers of their alleged unlawful file-sharing based on evidence of online copyright infringement gathered by investigatory agents' monitoring software and recorded in Copyright Infringement Reports (CIRs). In order to perform subscriber monitoring, investigatory agents such as MarkMonitor use DtecNet software to monitor peer-to-peer file-sharing networks.[6] Arguably these copyright infringement detection measures amount to digital surveillance of file sharing activities and an invasion of internet users' privacy, so the goal of this paper is to review the legality of such actions.

The efficacy of MarkMonitor's copyright infringement detection system has so far been assessed on two occasions. The first review was conducted in November 2012 by the digital risk management firm Stroz Friedberg.[7] In March 2014, Harbor Labs (an internet litigation consulting firm) carried out a follow-up review.[8] It confirmed Stroz's findings that in order to detect illegal copies, MarkMonitor employees search online for possibly infringing files. Detected material is then reviewed manually or using automatic content recognition software[9] to establish if it is an existing illegal copy of the copyrighted work.[10] Concurrently, MarkMonitor's DtecNet software (the gathering tool) searches for,

downloads samples of, and creates evidence of shared copyrighted material.[11] CIRs are subsequently generated and sent to the relevant ISP who then has to identify and notify the subscriber that they have infringed copyright on the internet.[12] In this paper, I will argue that these anti-copyright infringement measures constitute covert surveillance of subscriber activities and an unjustified invasion of their privacy.

The Revised Regulation of Investigatory Powers Act 2000 (RIPA) Code of Practice provides guidance on the use by State authorities of Part II of the RIPA.[13] The Revised RIPA Code (hereafter 'the RIPA Code') is admissible as evidence in both civil and criminal proceedings.[14] The RIPA Code asserts that an individual might have a diminished expectation of privacy when in a public space, for instance in a public file-sharing network. However, it also explains that where personal data is collected via covert surveillance of that individual's activities, such an individual still has a reasonable expectation of privacy, and authorisation for directed surveillance is needed.[15] Section 26(2) of the RIPA 2000 states that directed surveillance is covert surveillance which is performed for a specific investigation; it is expected to lead to the obtaining of private data about an individual and it is 'carried out' rather than via an immediate response to circumstances or events.[16] Arguably, DtecNet monitoring software is employed for specific infringement detection since it is expected to lead to the obtaining of the subscriber uploader's IP addresses, and it is not an immediate response to online copyright infringement.

In the Court of Justice of the European Union (CJEU) decision of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU,* the Advocate General (AG) made explicit reference to the CJEU joined cases of *European Parliament v Council of the European Union*.[17] The AG noted that pursuant to

the latter ruling, State authorities could compel private persons to assist them in tackling online copyright infringement. However, Kokott highlighted that independent action by rightholders against infringement, was allowed for State security and the activities of the State in areas of criminal law.[18] Therefore, the issue here concerns the State's obligation under Article 8 of the European Convention on Human Rights (ECHR) to abstain from interfering with subscribers' right to private life and correspondence.[19] In *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others*, the Court of Appeal agreed with Parker J that the data processed by rightholders not only constituted personal data (subscriber uploader's IP addresses), but also sensitive personal data (information about consumption habits e.g., the downloading of copyrighted political or religious material) as understood in the Data Protection Act 1998.[20] Further, as demonstrated in the case of *Copland v the United Kingdom*, the European Court of Human Rights (ECtHR) observed that data obtained from personal internet usage monitoring was protected under Article 8 of the ECHR.[21] It found that the gathering of personal data concerning the claimant's internet usage, without her permission, amounted to interference with her Article 8 ECHR rights.[22]

Thus, Section 3 of the DEA clearly interferes with Article 8. This interference will violate Article 8 of the Convention unless it is 'in accordance with the law'' pursues one or more legitimate aims contained within Article 8(2); and it is 'necessary' and 'proportionate' to achieve these aims.[23] As Cameron notes, these three prongs of the ECtHR's test are non-cumulative, so that a failure to satisfy one prong constitutes a breach of Article 8 irrespective of conformity with the other prongs.[24] This paper examines part one, part two and part three of the ECtHR's test, in an effort to determine whether the steps taken to generate CIRs, which amounts to surveillance and an unwarranted invasion of privacy, could infringe subscribers' Article 8 right to privacy, under the Convention. I conclude

that unless the implementation of Section 3 of the DEA required the involvement of State authorities, e.g., the courts or the data protection supervisory authorities, (the Information Commissioner's Office - ICO) and was specifically targeted to serious online copyright infringement cases of 'commercial scale',[25] it could infringe part one and part three of the ECtHR's test, thus violating subscribers' Article 8 ECHR rights.

Covert surveillance of subscribers could be incompatible with the right to privacy under the first-part of the ECtHR's non-cumulative test

The Strasbourg Court's case-law has confirmed that for any interference with the right to privacy to be 'in accordance with the law' under Article 8 of the Convention three requirements must be met: firstly, it has to be based in domestic legislation; secondly, such legislation should also be accessible; and thirdly, it needs to comply with the ECtHR foreseeability and rule of law principles.[26] The basis in domestic legislation requirement is unproblematic since Section 3 of the DEA (written law), and *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills*[27] (case-law), provide a legitimate basis for interfering. The second requirement does not pose any problem either, as the DEA is available online. However, regarding the third requirement, this section will argue that it fails to comply with the ECtHR's foreseeability and rule of law principles. It will demonstrate this by referring to the Ofcom Code and *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills*[28].

There is no mention in the Ofcom Code, that investigatory agents such as MarkMonitor use DtecNet's monitoring software to gather evidence of alleged illegal file-sharing, record it in CIRs and request that the ISP identify and notify the subscriber that they have committed an infringement. The Explanatory Notes

of the DEA state that rightholders can go online to seek content to which they have the copyright, and accordingly, rightholders can download a copy of that content and in doing so obtain the subscriber uploader's IP address in conjunction with date and time stamp identification. Nevertheless, the Explanatory Notes indicate that the rightholder is unable to link this information to data about the subscriber to whom the IP address was assigned as such data is held by ISPs.[29] Thus, under Section 3 of the DEA, the ISP is required to identify and notify the subscriber if it receives a CIR from a rightholder linked to their IP address.[30]

The Ofcom Code states that reliable evidence-gathering techniques are crucial.[31] It remarks that in the case of *Media CAT Ltd v Adams and others*,[32] in twenty-seven cases brought before Birss J, the Patents County Court was very critical of the unwillingness of ACS:Law to subject its evidence and information-gathering methods to 'judicial scrutiny'.[33] In this context, two points are worth remembering: firstly, a rightholder can only send a CIR if it has collected information which provides reasonable grounds to believe that either a subscriber contravened copyright via the internet or that he allowed another individual to do so;[34] and secondly, rightholders must submit their information-gathering methods for authorization to Ofcom before sending their first CIR.[35] Moreover, in order to review and authorise these methods, Ofcom proposes to sponsor the creation of an evidence gathering technical standard through an independent standard-setting body.[36]

It should be noted that Birss J's views in *Media CAT Ltd v Adams and others*[37] above, are similar to those of Lord Young:

'My Lords, Clause 4 sets out the requirements that must be met to produce a copyright infringement report. These reports are the mechanism by which the copyright owner brings specific apparent infringements of their copyright via a

particular IP address-and I stress 'apparent'-at a particular point in time to the attention of the relevant internet service provider. Some of these amendments seek to change the name of these reports from copyright infringement reports to copyright infringement allegation reports. Others propose a change of the wording to require the trigger leading to the creation of a CIR to be that in the 'reasonable opinion' of the copyright holder an infringement of their rights has occurred on that internet account, rather than it merely 'appearing to them' that an infringement has occurred. I recognise that the apparent infringements are not tested and proved to court standards. It will not be possible at the time the copyright infringement report is made to be able to declare with legal certainty that an infringement has occurred or that the IP address in the reports was responsible. Given this, clearly it is of the utmost importance that the standards of evidence surrounding the identification of both the infringement and the IP address of the infringing account should be as high as possible. I certainly concur with the points that the noble Lord, Lord Clement-Jones, made in relation to the standard of evidence and not presuming this is an open-and-shut case; and indeed with the point that the noble Lord, Lord De Mauley, made about speculative allegations-in other words, what is important is the standard of proof and evidence. New subsection (3) in Clause 4 already expressly recognises that the infringement described in a copyright infringement report is, as the noble Lord, Lord De Mauley, reminds us, only 'apparent'. Equally I think that the copyright infringement reports amount to more than mere allegation'.[38]

The Ofcom Code also explains that in producing CIRs and notifications, rightholders and ISPs remain subject to all present legal duties, including but not restricted to the RIPA 2000.[39] It highlights that some stakeholders have proposed that Ofcom should ask the ICO to make guidance available concerning data protection issues and that Ofcom should consult the Home Office concerning the interplay between the Ofcom Code and the RIPA.[40] Moreover, the Ofcom Draft

Costs Order notes that one ISP recommended that the systems for IP address recording and matching, created to serve the DEA obligations be employed in servicing the ISP's obligations in response to RIPA requests.[41] However, importantly, Ofcom understands that RIPA requests might involve a different set of regulations regarding security, timeliness, and data analysis.[42] Thus, it is rather worrying that Ofcom considers that the adoption of shared systems for RIPA requests and for DEA obligations, would be inefficient for the fulfilment of Section 3 of the DEA.[43] Arguably, this is especially true when the DEA allows investigatory agents to perform directed surveillance of subscriber activities, without being legally authorized to do so under RIPA.

Interestingly, the monitoring of subscribers by rightholders was explicitly addressed in *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills*. Parker J noted that pursuant to Article 15(1) of E-Commerce Directive 2000/31/EC, nothing in the DEA compelled ISPs to seek facts or circumstances, denoting unlawful activity.[44] He explained that it was the rightholder who must seek these facts or circumstances and send CIRs to the ISP. He highlighted that the only task of the ISP was to identify the alleged copyright infringer. He found that: 'if a police officer observes a motor car passing through a red light, and asks an official at the vehicle licensing authority to disclose the name and address of the registered keeper (and presumed driver) of the car, that official, in responding, would not actively be seeking facts or circumstances indicating illegal activity. She would be doing no more than identifying, in response to a specific request, the person who, according to the investigation already completed by the police officer, had infringed the traffic code'.[45] However, it is regrettable that the Court appears to have omitted relevant legal information, in particular Article 8 of the ECHR.

Lagerwall argues that compliance with the Strasbourg Court principle of foreseeability relates to the question of 'when' State authorities might use secret surveillance measures.[46] He explains that this involves an assessment of the circumstances where such measures might be carried out and against whom they can apply. Moreover, Lagerwall claims that compliance with the ECtHR principle of the rule of law refers to questions such as, 'what' discretion is given to State authorities, 'how' measures are conducted and 'who' is empowered with competence.[47] He states that this entails reviewing how State authorities' powers are employed and which control mechanisms are employed instead of focusing on the conditions under which they are used.[48] It will now be considered how the Ofcom Code could fail to comply with the ECtHR's foreseeability and rule of law principles, thus infringing the first-part of the Court's non-cumulative test (i.e., the 'in accordance with the law' test) under Article 8(2) of the ECHR.

In applying the principle of foreseeability in the judgement of *Malone v the United Kingdom*, the Strasbourg Court observed that under Article 8(2) of the Convention, the law had to be sufficiently clear in its terms to afford individuals an adequate indication of the circumstances where and the conditions upon which State authorities were permitted to use secret surveillance measures.[49] As noted above, the Explanatory Notes indicate that rightholders can go online and detect illegal copying of copyright protected content.[50] However, it can be contended that neither Section 3 of the DEA nor the Ofcom Code, specifies the circumstances in which the use of MarkMonitor's DtecNet software can be used. One could adopt an analogous view, as Parker J did in *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* that investigatory agents are like 'police officers' who ask officials (ISPs) to reveal the name and addresses of infringing drivers (alleged copyright infringers).[51] Although omitted from the Ofcom Code,

it is worth stressing however, that according to Section 28 of the RIPA, in order to engage in monitoring, these 'police officers' need to be granted authorisation.[52] The RIPA Code states that if the investigation is considered 'necessary' on one of more of the statutory grounds, the individual granting authorization for directed surveillance must conclude that it is 'proportionate' to the aim pursued.[53] This entails balancing the gravity of the privacy invasion concerning the subject of the investigation (e.g., subscribers) or any other individual who might be impacted (e.g., 'all' users) against the necessity of investigating.[54] Notably, the fact that an alleged offence might be grave is insufficient to render subscriber monitoring proportionate.[55] Thus, as Section 3 does not specify the circumstances where monitoring software measures may be ordered, as required by Section 28 of the RIPA, it arguably fails to satisfy the ECtHR foreseeability principle under Article 8(2) ECHR.

Again, in applying the principle of foreseeability in the ruling of *Liberty and others v the United Kingdom* the ECtHR noted that in order to avoid abuse of power under Article 8(2) of the Convention, a minimum safeguard that should be laid down by statute, was a definition of the types of individuals with respect to whom the use of surveillance measures may be ordered.[56] As outlined above, the Ofcom Code asserts that rightholders can only send CIRs if they have collected information which provides reasonable grounds to believe that a subscriber infringed copyright, or that he allowed another individual to do so.[57] Problematically, however, the Ofcom Code fails to address, much less recognize, the types of subscribers against whom the use of MarkMonitor's DtecNet software can be ordered. Section 28(3) of the RIPA states that authorisation for directed surveillance may only be granted if the authorising officer believes that it is necessary, *inter alia*, (g) for any purpose (falling outside paragraphs (a) to (f)) that is specified by an order made by the Secretary of State.[58] The use of

directed surveillance of subscribers' activities would be permitted under Section 28(3)(g) RIPA. The Revised RIPA Code explains that Section 28(3)(g) allows directed surveillance authorization to be granted, pursuant to the Secretary of State order, which complies with the criteria set out in Article 8(2) ECHR – e.g., for the protection of the rights of others.[59] However, even if this were the case, Section 3 of the DEA does not specify the types of subscribers against whom the use of monitoring software measures may be ordered. Therefore, it might be objected that it fails to comply with the ECtHR principle of foreseeability under Article 8(2) ECHR.

With regard to the rule of law principle, in *Rotaru v Romania*, the Strasbourg Court found that for secret surveillance measures to be compliant with Article 8 of the Convention they must include safeguards laid down by statute that apply to the oversight of State authorities' activities.[60] As mentioned above, in order to review and authorise the rightholders' information gathering methods, Ofcom proposes to sponsor the creation of an evidence gathering technical standard, through an independent standard-setting body.[61] However, it is regrettable that neither Section 3 nor the Ofcom Code requires that the development of this standard be subject to state authority supervision, i.e., the courts or the ICO. In the CJEU decision of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU,* the AG stressed that involving State authorities was appropriate as, unlike private persons, they are required to observe procedural safeguards, thereby preventing human rights abuses.[62] The European Data Protection Supervisor (EDPS) considers that the above data processing operations could eventually lead to criminal prosecution thereby posing specific risks to individual rights. Thus, he explains that 'national data protection authorities' should check and authorise these evidence-gathering methods before CIRs are issued.[63] He notes that the fact that this processing entails the monitoring

of internet communications is another factor requiring stronger supervision.[64] Stroz Friedberg's review found that MarkMonitor evidence is 'robust, defensible, and will stand… evidentiary challenges'.[65] However, as TorrentFreak reported in February 2013, DtecNet not only wrongly identified legitimate content from the pay television service company HBO as infringing and asked Google to censor links to HBO.com, but also some sought censorship of lawful websites that wrote reviews about HBO material.[66] Consequently, it is concerning that under the RIPA, the Investigatory Powers Tribunal cannot handle complaints against the use of private sector monitoring (MarkMonitor). Thus, since Section 3 DEA 2010 does not require that the evidence gathering technical standard be previously checked and authorised by the ICO, it is debatable whether it fails to satisfy the ECtHR rule of law principle under Article 8(2) ECHR.

Covert surveillance of subscribers could be incompatible with the right to privacy under the second-part of the ECtHR's non-cumulative test

Article 8(2) of the Convention outlines that State authorities can interfere with the right to privacy to protect, *inter alia*, one or more of the following (legitimate) aims: firstly, domestic security, public safety or the economic well-being of the country; secondly, the prevention of disorder or crime; and lastly, the protection of the rights and freedoms of others.[67] This list is exhaustive; thus, interference is only allowed on the above grounds.[68] Cameron argues that since it is relatively easy for states to satisfy the legitimate aim prong, the second-part of the ECtHR's non-cumulative test is a mere formality.[69] With that in mind, this section will argue that Section 3 of the DEA can enable pursuance of one or more of the legitimate aims contained in Article 8(2) of the Convention in compliance with the second-part of the Strasbourg Court's non-cumulative test. It will demonstrate this by referring to the CJEU case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*[70] and *R (British Telecommunications*

plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others[71].

To begin with, the UK government states that Article 8 is a qualified right, so it is legitimate under the ECHR to restrict such a right, if the restriction is in the public interest and in accordance with the law.[72] Specifically, the government explains that the DEA strikes a fair balance between subscriber rights and rightholder rights, as the qualification to Article 8 must take into account the rights of others.[73] However, when considering the compatibility of Section 3 of the DEA with the second-part of the ECtHR's non-cumulative test, it is important to note that the government makes explicit reference to the CJEU decision of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU.*[74] It emphasizes that this case not only acknowledges that effective copyright protection constitutes a legitimate aim, but also offers guidance on the steps to be taken to strike an appropriate balance between the various rights at stake.[75]

In the case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*, the CJEU observed that Article 15(1) of E-Privacy Directive 2002/58/EC provided member states with the opportunity to allow exceptions to the duty to ensure the confidentiality of IP address' traffic data[76] – (e.g., subscriber uploader's IP addresses). It explained that the exceptions in Article 15(1) include: firstly, public security, defence and national security, which constituted 'activities of the State or of State authorities'; and secondly, the enforcement of criminal law.[77] However, in assessing the compatibility of Section 3 with Article 8(2) of the Convention, the key thing to remember is the CJEU's next finding. The CJEU highlighted that Article 15(1) concluded the list of the above exceptions by making explicit reference to Article 13(1) of Data Protection

Directive 95/46/EC. It found that the latter provision also allowed member states to adopt legislative measures to derogate from the duty of confidentiality of IP address' traffic, where such restriction was required to protect the rights and freedoms of others.[78]

The CJEU's finding above differs significantly from the AG's opinion in the same decision. The AG explained that rightholders must be provided with an opportunity to defend themselves against charges of online copyright infringement.[79] Kokott also stated that this case *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU,* was not concerned with whether access to the courts was possible, but with the techniques used for detection of online copyright infringement, being made available to rightholders.[80] Crucially, in agreement with the Working Party[81] and the EDPS,[82] Kokott warned that 'the State's duties of protection are not so far-reaching that unlimited means should be made available to the rightholder for the purpose of detecting infringements of rights. Rather, it is not objectionable for certain rights of detection to remain reserved for States authorities or not to be available at all.'[83]

It should be noted that the task of the AG is to deliver independent and impartial expert opinions on decisions, which, as above, give rise to new legal issues before the CJEU. Although the AG's opinion is advisory and not legally binding on the CJEU, it is very significant and the CJEU tends to follow its recommendations. Unlike the CJEU's ruling, the AG's opinion normally addresses all possible legal solutions and questions of law, which may be particularly relevant to a decision[84] such as, the legitimacy of private surveillance by investigatory agents for the

purposes of online copyright enforcement. The impact of the AG's opinion must be interpreted over a period of time. For example, in *NV Algemene Transport en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*,[85] the CJEU was asked to decide whether the principle of direct effect should be incorporated into EU law. After considering the AG's opinion, the CJEU recognized this principle as part of Community law, meaning that individuals were effectively able to enforce EU law rights against the State.[86]

Interestingly, in *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others*, the Court of Appeal observed that Parker J, at first instance, rejected the ISPs' claim that the CJEU case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*[87] only related to the protection of property in civil proceedings where there was judicial supervision, and that no broader derogation was to be read into Article 15(1) of E-Privacy Directive 2002/58/EC in order to apply in the present context.[88] However, the Court found that, in doing so, Parker J arrived at a judicious decision.[89] It concluded that it was clear from the judgement of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*[90] that Article 15(1) of E-Privacy Directive 2002/58/EC also covered the protection of the rights and freedoms of others, including intellectual property, and therefore copyright. This was not restricted to the context of civil proceedings.[91]

Article 8(2) of the Convention confirms that State authorities can interfere with the right to privacy in order to protect national security, public safety or the economic well-being of the country.[92] This legitimate aim was accepted in the Strasbourg Court decision of *Uzun v Germany*.[93] As discussed earlier, under Section 28(3) of the RIPA, authorisation for directed surveillance may be granted

(a) in the interest of domestic security; (c) the economic well-being of the UK; and (d) public safety.[94] In the case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* the CJEU observed that, under Article 15(1) of E-Privacy Directive 2002/58/EC, member states might implement legal measures to limit the scope of the duty to ensure the confidentiality of subscriber uploader's IP addresses, if such measures were appropriate, necessary and proportionate to protect State security as stated in Article 13(1) of Data Protection Directive 95/46/EC. However, the CJEU correctly highlighted that this constituted 'activities of the State or of State authorities'.[95] Moreover, in this decision, the AG also noted that the domestic security and public policy exception could just be raised if a sufficiently grave and genuine threat existed, affecting one of the fundamental interests of society, such as the protection of copyright.[96] Resultantly, although rightholders' interests were mainly private, not public, Kokott suggested that unlawful file-sharing genuinely threatened copyright protection.[97] However, importantly, she stressed that it was unclear that private file-sharing, especially if it occurred 'without any intention to make a profit', threatened copyright protection sufficiently seriously to justify this exception.[98] Thus, as Section 3 of the DEA can justify recourse to the domestic security, public safety or the economic well-being of UK exception, it is arguable that it may constitute a legitimate aim under Article 8(2) ECHR. However, it would require the involvement of State authorities, such as, the courts or the domestic data protection supervisory authorities, (e.g., the ICO).

Article 8(2) of the ECHR elaborates that State authorities can interfere with the right to privacy for the prevention of disorder or crime.[99] This legitimate aim was discussed in the ECtHR decision of *Klass and others v Germany*.[100] Equally, as noted earlier, Section 28(3)(b) RIPA states that authorisation for directed surveillance may be granted to prevent or detect crime or to prevent disorder.[101]

As stated above, in the case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*, the CJEU observed that Article 15(1) of E-Privacy Directive 2002/58/EC gave member states the opportunity to allow exceptions to the duty to ensure the confidentiality of subscriber uploader's IP addresses when these measures were appropriate, necessary and proportionate in criminal prosecution cases, as stated in Article 13(1) of Data Protection Directive 95/46/EC.[102] Here too, the AG acknowledged that whilst under Article 15(1) member states might allow IP address traffic data to be transmitted to State authorities to initiate civil and criminal proceedings against illegal file-sharing, they were not compelled to do so.[103] Kokott pointed out that criminal liability was not precluded, as was evident from Article 16 of the Intellectual Property Rights Enforcement Directive 2004/48/EC and Article 8(1) of the Copyright Directive 2001/29/EC; domestic law must decide whether and in what form contraventions of copyright were punished.[104] However, notably, she stated that involving State authorities was appropriate since, unlike private persons, they must reinforce procedural safeguards, thereby preventing violations of human rights.[105] Importantly, she concluded that unlike State authorities, rightholders had no interest in taking into account circumstances that exonerate the subscriber accused of online copyright infringement.[106] Thus, since Section 3 of the DEA can justify recourse to the prevention of disorder or crime exception, it could potentially constitute a legitimate aim under Article 8(2) ECHR. However, this would require online copyright infringement via file-sharing to become a criminal offence and the intervention of State authorities to be implemented.

Article 8(2) of the ECHR adds that State authorities can interfere with the right to privacy for the protection of the rights and freedoms of others.[107] This legitimate aim was accepted in the ECtHR decision of *Copland v the United Kingdom*.[108] RIPA does not expressly covers the rights of others exception. It is

worth noting, however, that Section 28(3)(g) RIPA would do so. As noted before, the RIPA Code states that under this provision directed surveillance authorization might be granted, pursuant to an order by the Secretary of State that complies with the criteria set out in Article 8(2) ECHR.[109] In the case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*, the CJEU pointed out that Article 15(1) of E-Privacy Directive 2002/58/EC concluded the list of exceptions by making explicit reference to Article 13(1) of Data Protection Directive 95/46/EC. The Court explained that this latter provision also permitted member states to implement legal measures to derogate from the duty of confidentiality of subscriber uploader's IP addresses if such derogation was necessary to protect the rights and freedoms of others. The CJEU found that, as they failed to indicate the rights and freedoms involved, the requirements of Article 15(1), had to be understood as reflecting the EU legislative's intent not to preclude from their scope intellectual property protection or situations where creators sought to acquire such protection in civil cases.[110] Therefore, as Section 3 of the DEA can justify recourse to rights and freedoms of others exception, it is clear that it may constitute a legitimate aim, under Article 8(2) of the ECHR.

Covert surveillance of subscribers could be incompatible with the right to privacy under the third-part of the ECtHR's non-cumulative test

The last issue to be examined in this paper, is whether Section 3 of the DEA complies with the third-part of the Strasbourg Court's non-cumulative test. The ECtHR's case-law has confirmed that under Article 8(2) of the Convention, measures of secret surveillance are 'necessary in a democratic society', if they respond to a 'pressing social need' and are proportionate to the legitimate aim pursued.[111] Moreover, the Court has noted that the reasons given by the state to justify them, must be 'relevant and sufficient'.[112] Yet whilst State authorities enjoy a certain margin of appreciation, the final assessment as to the necessity and proportionality of these measures remains subject to review by the Court.[113]

In this section, it will be argued that the use of monitoring software measures fails to satisfy the necessity and proportionality principles. This will be demonstrated by considering the Ofcom Code and *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others*[114].

The Ofcom Code states that Section 3 of the DEA compels an ISP that receives a CIR to identify the subscriber to which the CIR is related and issue notifications. Accordingly, to ensure that the procedure of linking IP addresses to subscribers is robust and accurate, the Ofcom Code notes that ISPs should, before sending their first warning letter, give Ofcom a quality assurance report. Ofcom indicates that this report should specify the systems and procedures employed by the ISP, to match data contained in CIRs to subscriber accounts.[115] The Ofcom Code explains that the ISP is required to publish that report as soon as reasonably possible, after it is issued to Ofcom.[116] It concludes that upon receipt of a CIR from a rightholder, the ISP is under an obligation to identify and notify the subscriber to which the IP address detailed in the CIR related at the time of the alleged copyright contravention.[117] Notably, as flagged above, this can be contrasted with Parker J's 'policeman analogy' in *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills*. Parker J found that pursuant to Article 15(1) of E-Commerce Directive 2000/31/EC, nothing in the DEA compelled ISPs to investigate and analyse the information transmitted to them by rightholders.[118]

The Ofcom Code also states that a time-based three strikes notification process is adequate.[119] Firstly, the initial notification is sent after the first-matched CIR in 12 months; secondly, the intermediate notification is sent after the second-

matched CIR in 12 months; thirdly, the infringement list notification is sent after the third-matched CIR in 12 months; and fourthly, the further infringement list notification is sent after a new-matched CIR in 12 months.[120] It is worth pointing out that Ofcom considers that 1 month is a reasonable minimum time between one warning letter being sent and the next being issued by a CIR.[121] Moreover, importantly, Ofcom stresses that the goal of the DEA is to tackle mass online copyright infringement by changing subscriber behaviour over time, and 'excluding persistent low-level infringers', does not satisfy this condition.[122] However, in assessing the compatibility of Section 3 with the third-part of the Strasbourg Court's non-cumulative test, under Article 8(2) of the Convention, one could argue that there should be some monitoring of the volume of CIRs, not only persistence of the infringement. It should be emphasized that in the Ofcom Draft Initial Obligations Code Consultation document, BIS suggested a volume-based three strikes notification process, where the first notification was triggered by 10 CIRs; the second by 30 CIRs; and the third by 50 CIRs.[123]

The necessity and proportionality of monitoring software measures like MarkMonitor, was expressly examined in *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others*. The Court of Appeal observed that the appellants relied upon the EDPS's opinion on the legality of a 'three strikes internet disconnection policy'.[124] The Court noted that in paragraph 52 of this opinion, the EDPS recognized that the gathering of target-specific evidence, specifically in cases of a grave infringement, may be necessary to establish and exercise a legal claim. However, it explained that the EDPS questioned the lawfulness of large-scale investigations entailing the processing of vast amounts of user information. Interestingly, the Court highlighted that it was hard to see why following the EDPS's opinion, the application of Article 8(2)(e) of the Data Protection Directive 95/46/EC, should depend upon the scale of the infringement. It

concluded that, in any case, the EDPS's opinion was 'not binding'.[125] However, since the EDPS's opinion is notably consistent with the ECtHR's case-law the Court's finding appears questionable.

In the CJEU case of *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, the AG observed that the Strasbourg Court had not yet had the chance to pronounce on the compatibility of measures designed to monitor electronic communications with the Convention. However, he remarked that considering its jurisprudence on telephone tapping, these measures were tantamount to interferences with the right to privacy, as guaranteed by Article 8 of the Convention.[126] The ECtHR's case-law has confirmed that, under Article 8(2) ECHR, factors to be taken into account when assessing the necessity and proportionality of secret surveillance measures include: firstly, whether minimally invasive techniques have been tried and proven to be ineffective;[127] secondly, whether these measures are limited in time;[128] and thirdly, the gravity of the offence.[129]

In terms of the first requirement, using the example of *Uzun v Germany*, the Strasbourg Court observed that under Article 8(2) of the Convention, in assessing the necessity of secret surveillance measures, less invasive techniques should have been tried and proven to be ineffective.[130] Similarly, the RIPA Code states that no activity is proportionate if the evidence could reasonably be acquired in a less-invasive way.[131] As outlined above, Ofcom remarks that the aim of the Act is to tackle mass online copyright infringement, and 'excluding persistent low-level infringers', fails to satisfy such a condition.[132] However, it is concerning that this differs significantly from the EDPS' warning that regarding the necessity of an enforcement measure interfering with privacy rights, it is essential to establish

first whether subscriber monitoring could be carried out in a less invasive way.[133] Importantly, the EDPS opinion underlines that IP enforcement can also be attained through the monitoring of a specific number of users allegedly involved in 'non-trivial' online copyright infringement.[134] He indicates that following the commercial scale rule contained in Article 8 of the Intellectual Property Rights Enforcement Directive 2004/48/EC, rightholders can perform targeted monitoring of specific subscriber IP addresses: firstly, to confirm the scale of the infringement; and, secondly, to keep track of CIRs for that purpose. However, he concludes that such data can only be used after having confirmed its scale. He illustrates this point by referring to cases of obvious online copyright abuse, which aim to achieve economic benefits.[135] Thus, as Section 3 of the DEA does not require that less invasive targeted subscriber monitoring be tried, it is arguable that it fails to satisfy the ECtHR necessity principle under Article 8(2) ECHR.

As far as the second requirement is concerned, in *Kennedy v the United Kingdom*, the ECtHR noted that, under Article 8(2) of the ECHR, in order to avoid abuse of power, domestic legislation had to lay down, by statute, a limit on the duration of secret surveillance measures.[136] Likewise, the RIPA Code states that concerning the duration of authorisations, a written authorisation expires (unless renewed or cancelled) after three months.[137] In the CJEU decision of *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, the AG made explicit reference to the technical expert report, which assessed the technical feasibility of the anti-infringement solutions suggested by SABAM.[138] The technical expert report stressed that, unlike website-blocking injunctions, the investigation techniques employed to enforce online copyright infringement on file-sharing systems (e.g., MarkMonitor's DtecNet software), were more complex to carry out, but provided better outcomes. Notably, the report indicated that in the medium to long term, these anti-infringement methods were the best type of investment, in order to guarantee respect for copyright law.[139] However,

to counter this, one could claim that the technical expert report regrettably appears to disregard the fact that in detecting infringing activity MarkMonitor's DtecNet software, never stops snooping on alleged copyright infringers. Crucially, in paragraph 20 of *EMI Records (Ireland) Ltd v Eircom Ltd*, Charleton J revealed that 'continually scanning and rescanning internet communications', DtecNet software, identified the content being communicated in various directions from P2P, or similar swarms and followed the P2P communication down the line, until it ended up in a specific PC and recorded its IP address.[140] Indeed, in November 2012, Stroz Friedberg reviewed MarkMonitor evidence and confirmed that DtecNet has specific inherent and added system redundancies that ensure that it carries out 'continuous and consistent scanning'.[141] Therefore, since Section 3 of the DEA places no limit on the number of hours of subscriber monitoring, it is debatable whether it fails to comply with the ECtHR proportionality principle under Article 8(2) ECHR.

With regard to the third requirement, in *Weber and Saravia v Germany,* the ECtHR found that, in order to assess whether secret surveillance measures were proportionate under Article 8(2) ECHR, the gravity of the offence had to be considered.[142] Again, the RIPA Code indicates that an offence might be so trivial, that any use of covert techniques would be disproportionate.[143] As stated above, unlike BIS volume-based approach, the Ofcom Code emphasizes that a time-based, three strikes notification process is adequate.[144] However, it is to be regretted that this notably fails to take into account the CJEU judgement of *L'Oréal SA and others v eBay International AG and others*. Here, the CJEU held that in assessing whether the offender surpassed the realms of a private activity and acted 'in the course of trade', the 'volume' and 'frequency' of infringing acts, were vital considerations.[145] The EDPS recognizes that, pursuant to the commercial scale rule in Article 8 of Intellectual Property Rights Enforcement

Directive 2004/48/EC, subscriber monitoring might be proportionate, in the context of restricted, individual, ad hoc cases, where strong suspicions of online copyright infringement on a commercial scale exist.[146] He explains that only this specific type of subscriber monitoring can be considered proportionate to prepare legal claims, including litigation.[147] He clarifies that 'commercial scale' would not only exclude actions performed by subscribers acting in good faith, but also those performed for personal and not-for-profit purposes.[148] However, importantly, he remarks that general or random monitoring, concerning not-for-profit or minor, small-scale online copyright infringement would be disproportionate and violate Article 8 of the ECHR.[149] This is a view shared by Kokott in her discussion of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*.[150] Thus, since under Section 3 of the DEA, monitoring software measures are not specifically targeted to serious online copyright infringement cases of 'commercial scale', an argument can be made that it fails to satisfy the ECtHR proportionality principle, under Article 8(2) ECHR.

Covert surveillance of subscribers could constitute a violation of their right to privacy under Article 8 of the Convention

This paper has examined the compatibility of the s3 DEA obligation to notify subscribers of CIRs with Article 8 of the ECHR. A growing body of research has investigated whether relying on human rights as a benchmark the DEA is a proportionate response to the problem of online copyright infringement.[151] To date, however, there has been very little research conducted on the legality of the Act from the context of the UK's duties, under the Convention, specifically Article 8. If this research has not been undertaken, the input of the cyberlawyer in this area would be missing.[152] I conclude that unless the implementation of Section 3 of the DEA required the involvement of State authorities (e.g., the

courts or the ICO) and was specifically targeted to serious online copyright infringement cases of 'commercial scale', it could infringe part one and part three of the ECtHR's test, thereby violating subscribers' Article 8 ECHR rights. Thus, perhaps the time has come for the UK government to require the ICO to check and authorise the evidence gathering technical standard. The RIPA Code states that for monitoring to be proportionate, it is essential to balance the scope of the monitoring against the gravity of the offence.[153] To make this effective, the ICO should follow the EDPS's opinion ensuring that subscriber monitoring is limited in scope (specific, existing or future court proceedings); in time (at only certain times or days); and in the number of monitored users (only commercial scale copyright infringers).[154] Additionally, the ICO should also observe Harbor Labs' recommendation ensuring that MarkMonitor implements supplementary security measures such as, which personnel can access data, how long data is to be stored, how data is to be destroyed, and how data is to be properly protected from theft.[155] Indeed, this is particularly the case when the Strasbourg Court has stressed that for domestic legislation to be compatible with Article 8 of the Convention, it must have in place minimum safeguards concerning third party access, data retention duration, data destruction, and data confidentiality and integrity.[156] On the contrary, the violation of subscriber privacy by the private sector (e.g., MarkMonitor) will be routine, disproportionate and illegal, and the UK law could face potential legal challenges at the EU or ECtHR level. In my view, this is indeed alarming because eventually, these subscriber monitoring practices could become a widely-accepted practice. However, no matter how sophisticated the surveillance methods adopted, opposition from subscribers will result in tactics to frustrate IP address gathering being employed and improved. For instance, the EDPS stresses that file-sharing systems can evolve, ensuring that information is exchanged privately in different ways, such as not employing Peer IDs or permitting double secured hops for each portion of bytes transmitted.[157] However, even if the ICO were to check and authorise the evidence gathering technical

standard, and require MarkMonitor to adopt supplementary security measures, the question remains as to when subscribers might become commercial scale copyright infringers. Expert research shows that approximately 100 initial uploaders, (those individuals who first upload copyrighted content in file-sharing networks) publish 67 percent of the material. This represents 75 percent of all downloads.[158] However, importantly, it reveals that while these initial uploads trigger billions of downloads, such initial uploaders use platforms, such as, the Pirate Bay to attract millions of BitTorrent users to their websites 'for financial gain' by displaying the embedded URL to them at different moments of the download.[159] Thus, there seems little the UK government can do other than to start taking seriously Kokott's recommendation in the case of *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* that the collection of subscriber uploader's IP addresses should be limited to 'particularly serious cases such as… offences committed with a view to making a profit, that is, an illegal use of protected works which substantially impairs their economic exploitation'.[160] Indeed, even more so when Ofcom itself has proposed that 'alternatively', rightholders could exclusively target initial uploaders by analysing newly introduced files to ascertain not only their identity, but also their location.[161] What remains to be seen is, however, whether targeting initial uploaders can be done effectively. Expert research indicates that since initial uploaders can access the internet using anonymity tools, investigatory agents could mistakenly detect a middlebox, (i.e., proxies, Network Address Translators, IPv6 gateways, etc), as an initial uploader.[162] Yet, as TorrentFreak has noted, NSA-like surveillance technology is currently being employed to monitor users using multiple proxies.[163] The effect of this concerning subscribers' rights is that as will always be the case, it is impossible to guarantee absolute privacy on the internet. Meanwhile, expert research shows that whilst the top 10 initial uploaders are hosting companies located in France and Germany, concluding that the users behind such initial uploaders live in these countries is erroneous, since their

servers are hired by individuals residing in other countries.[164] In *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* Parker J himself found that, taken together, both Article 8 of the Intellectual Property Rights Enforcement Directive 2004/48/EC and the EDPS's opinion, online copyright infringement might be tackled by targeting big, commercial scale copyright infringers.[165] Thus, it may seem disproportionate to not particularly target at those who bear the greatest responsibility, (e.g., initial uploaders). However, in my opinion, nothing may be more disproportionate than the fact that in the reverse situation, Section 3 of the DEA violated subscribers' Article 8 ECHR rights under the Convention.

[1] Lecturer in Law at University of Hertfordshire. Special thanks to Dr Karen Mc Cullagh for her suggestions and comments that significantly contributed to improving the quality of this manuscript.
[2] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin).
[3] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232.
[4] Regulation of Investigatory Powers Act 2000.
[5] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 6.
[6] MarkMonitor, Accessed 15 April 2015. https://www.markmonitor.com/services/antipiracy.php
[7] Stroz Friedberg. ''Independent Expert Assessment of MarkMonitor Antipiracy Methodologies'' (1 November 2012).
[8] Harbor Labs, ''Evaluation of the MarkMonitor AntiPiracy System'' (3 March 2014).
[9] For example, Audible Magic's fingerprinting technology Audible Magic, Accessed 15 April 2015. https://www.audiblemagic.com/
[10] Stroz Friedberg. ''Independent Expert Assessment of MarkMonitor Antipiracy Methodologies'' (1 November 2012) p. 4 and 5.
[11] including IP address, time/date, size, port, PeerID and hash values, thus documenting subscribers' activities *Ibid*., 4 and 6.
[12] *Ibid*., 5.
[13] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 5.
[14] *Ibid*., 6.
[15] *Ibid*., 12-13.
[16] Regulation of Investigatory Powers Act 2000 Section 26(2).
[17] Case 317/04 and Case 318/04 *European Parliament v Council of the European Union* [2006] ECR I-4721.
[18] Advocate General's Opinion in Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 101].
[19] *Copland v the United Kingdom* (App no 62617/00) (2007) 45 EHRR 37 [39].
[20] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232 [75].
[21] *Copland v the United Kingdom* (App no 62617/00) (2007) 45 EHRR 37 [41].
[22] *Ibid*., [44].
[23] European Convention on Human Rights 1950 Article 8(2).
[24] Cameron. 2006. *An Introduction to the European Convention on Human Rights* 105. 5th edn Uppsala.
[25] 'Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.' Agreement on Trade Related Aspects of Intellectual Property Rights 1994 Article 61.

[26] *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [151]; *Rotaru v Romania* (App no 28341/95) (2000) 8 BHRC 449 [52]; *Liberty and others v the United Kingdom* (App no 58243/00) (2008) 48 EHRR 1 [59]; *Iordachi and others v Moldova* (App no 25198/02) (2009) ECHR [37]; *Leander v Sweden* (App no 9248/81) (1987) 9 EHRR 433 [50].
[27] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin).
[28] *Ibid*.
[29] Digital Economy Act 2010 c. 24 Explanatory Note [41].
[30] *Ibid*., [42].
[31] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 44.
[32] *Media CAT Ltd v Adams and others* [2011] EWPCC 006.
[33] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 44.
[34] *Ibid*.
[35] *Ibid*., 45.
[36] *Ibid*., 46.
[37] *Media CAT Ltd v Adams and others* [2011] EWPCC 006.
[38] Hansard, HL Vol.716, col. 441 (January 12, 2010).
[39] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 46.
[40] *Ibid*., 63.
[41] Ofcom, ''Online Infringement of Copyright: Implementation of the Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2012'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/onlinecopyright/summary/condoc.pdf, p. 35.
[42] *Ibid*.
[43] *Ibid*., 36.
[44] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) [115].
[45] *Ibid*., [118].
[46] Anders Lagerwall. ''Privacy and Secret Surveillance from a European Convention Perspective'' (Thesis, Stockholm University 2008) p. 34.
[47] *Ibid*.
[48] *Ibid*.
[49] *Malone v the United Kingdom* (App no 8691/79) (1984) 7 EHRR 14 [67]; see also *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [152]; see also *Huvig v France* (App no 11105/84) (1990) 12 EHRR 528 [54] [55]; *Valenzuela Contreras v Spain* (App no 27671/95) (1999) 28 EHRR 483 [46]; *Kopp v Switzerland* (App no 23224/94) (1998) 27 EHRR 91 [64].
[50] Digital Economy Act 2010 c. 24 Explanatory Note [41].
[51] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) [118].
[52] Regulation of Investigatory Powers Act 2000 Section 28.
[53] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 25.
[54] *Ibid*., 25-26.
[55] *Ibid*.
[56] *Liberty and others v the United Kingdom* (App no 58243/00) (2008) 48 EHRR 1 [62]; see also *Huvig v France* (App no 11105/84) (1990) 12 EHRR 528 [34]; *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [95]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [65]; *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [152]; *Amann v Switzerland* (App no 27798/95) (2000) 30 EHRR 843 [76]; *Valenzuela Contreras v Spain* (App no 27671/95) (1999) 28 EHRR 483 [46]; *Prado Bugallo v Spain* (App no 58496/00) (2003) [30]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App no 62540/00) (2007) ECHR [76].
[57] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 44.
[58] Regulation of Investigatory Powers Act 2000 Section 28(3)(g).
[59] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. 1https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 46.
[60] *Rotaru v Romania* (App no 28341/95) (2000) 8 BHRC 449 [59]; see also *Klass and others v Germany* (App no 5029/71) (1979-80) 2 EHRR 214 [55]; *Amann v Switzerland* (App no 27798/95) (2000) 30 EHRR 843 [60].
[61] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 46.
[62] Advocate General's Opinion in Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 114].
[63] Opinion of the European Data Protection Supervisor (EU) of 5 June 2010 'on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)' [2010] in paragraph 47.
[64] *Ibid*.
[65] Stroz Friedberg. ''Independent Expert Assessment of MarkMonitor Antipiracy Methodologies'' (1 November 2012) p. 1.
[66] TorrentFreak, ''HBO wants Google to censor… HBO.com'' Accessed 15 April 2015. http://torrentfreak.com/hbo-wants-google-to-censor-hbo-com-130203/
[67] European Convention on Human Rights 1950 Article 8(2).

[68] *Golder v the United Kingdom* (App no 4451/70) (1979) 1 EHRR 524 [44]; see also Anders Lagerwall. ''Privacy and Secret Surveillance from a European Convention Perspective'' (Thesis, Stockholm University 2008) p. 17.
[69] Cameron. 2006. *An Introduction to the European Convention on Human Rights* 105. 5th edn Uppsala.
[70] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271.
[71] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232.
[72] Department for Culture, Media and Sport and Department for Business, Innovation and Skills, ''Digital Economy Bill – Memorandum to the Joint Committee on Human Rights'' Accessed 15 April 2015. http://www.parliament.uk/documents/upload/govtmemodeb.pdf, p. 4.
[73] *Ibid*.
[74] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271.
[75] Department for Culture, Media and Sport and Department for Business, Innovation and Skills, ''Digital Economy Bill – Memorandum to the Joint Committee on Human Rights'' Accessed 15 April 2015. http://www.parliament.uk/documents/upload/govtmemodeb.pdf, p. 5.
[76] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271[49].
[77] *Ibid*., [51].
[78] *Ibid*., [53].
[79] *Ibid*., [AG 120].
[80] *Ibid*.
[81] Article 29 Data Protection Working Party document (EU) of 18 January 2005 'on data protection issues related to intellectual property rights' [2005] p. 7.
[82] Opinion of the European Data Protection Supervisor (EU) of 24 April 2012 'on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America' [2012] in paragraphs 44-45.
[83] Advocate General's Opinion in Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 121].
[84] Stina Haglund, ''The role of the Advocate General and the development of direct effect'' Accessed 15 April 2015. https://eulaworebro.wordpress.com/2012/08/13/the-role-of-the-advocate-general-and-the-development-of-direct-effect/
[85] Case 26/62 *Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* [1963] ECR I.
[86] Stina Haglund, ''The role of the Advocate General and the development of direct effect'' Accessed 15 April 2015. https://eulaworebro.wordpress.com/2012/08/13/the-role-of-the-advocate-general-and-the-development-of-direct-effect/
[87] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271.
[88] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232 [81].
[89] *Ibid*.
[90] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271.
[91] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232 [81].
[92] European Convention on Human Rights 1950 Article 8(2).
[93] *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [77].
[94] Regulation of Investigatory Powers Act 2000 Section 28(3).
[95] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [49].
[96] *Ibid*., [AG 104], [AG 105].
[97] *Ibid*., [AG 105].
[98] *Ibid*., [AG 106].
[99] European Convention on Human Rights 1950 Article 8(2).
[100] *Klass and others v Germany* (App no 5029/71) (1979-80) 2 EHRR 214 [48].
[101] Regulation of Investigatory Powers Act 2000 Section 28(3)(b).
[102] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [49].
[103] *Ibid*., [AG 112].
[104] *Ibid*., [AG 103].
[105] *Ibid*., [AG 114].
[106] *Ibid*., [AG 116].
[107] European Convention on Human Rights 1950 Article 8(2).
[108] *Copland v the United Kingdom* (App no 62617/00) (2007) 45 EHRR 37 [34].
[109] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 46.
[110] Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [53].
[111] *Peck v the United Kingdom* (App no 44647/98) (2003) 36 EHRR 41 [76]; *S and Marper v the United Kingdom* (App no 30562/04 and 30566/04) (2008) ECHR 1581 [101]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [78]; *Leander v Sweden* (App no 9248/81) (1987) 9 EHRR 433 [58]; *Messina v Italy (no 2)* (App no 25498/94) (2000) ECHR 2000-X [65].
[112] *Ibid*.
[113] *S and Marper v the United Kingdom* (App no 30562/04 and 30566/04) (2008) ECHR 1581 [101]; *Coster v the United Kingdom* (App no 24876/94) (2001) 33 EHRR 20 [104].
[114] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232.
[115] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 44.
[116] *Ibid*., 51.
[117] *Ibid*.
[118] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) [115], [118].

[119] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 59.
[120] *Ibid*., 59-60.
[121] *Ibid*., 59.
[122] *Ibid*., 60.
[123] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 Draft Initial Obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf , p. 22.
[124] *R (British Telecommunications plc and TalkTalk Telecom Group plc) v Secretary of State for Culture, Olympics, Media and Sport and others* [2012] EWCA Civ 232 [78].
[125] *Ibid*.
[126] Advocate General's Opinion in Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [AG 82].
[127] *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [78]; see also *Informationsverein Lentia and Others v Austria* (App no 13914/88) (15041/89) (15717/89) (15779/89) (17207/90) (1993) 17 EHRR 93 [39].
[128] *Liberty and others v the United Kingdom* (App no 58243/00) (2008) 48 EHRR 1 [62]; *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [152]; see also *Huvig v France* (App no 11105/84) (1990) 12 EHRR 528 [34]; *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [95]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [65]; *Amann v Switzerland* (App no 27798/95) (2000) 30 EHRR 843 [76]; *Valenzuela Contreras v Spain* (App no 27671/95) (1999) 28 EHRR 483 [46]; *Prado Bugallo v Spain* (App no 58496/00) (2003) [30]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App no 62540/00) (2007) ECHR [76].
[129] *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [115]; see also *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [159]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [80].
[130] *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [78]; see also *Informationsverein Lentia and others v Austria* (App no 13914/88) (15041/89) (15717/89) (15779/89) (17207/90) (1993) 17 EHRR 93 [39].
[131] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 26.
[132] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 60.
[133] Opinion of the European Data Protection Supervisor (EU) of 5 June 2010 'on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)' [2010] in paragraph 42.
[134] *Ibid*., in paragraph 43.
[135] *Ibid*., in paragraphs 43 and 45.
[136] *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [152]; see also *Liberty and others v the United Kingdom* (App no 58243/00) (2008) 48 EHRR 1 [62]; *Huvig v France* (App no 11105/84) (1990) 12 EHRR 528 [34]; *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [95]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [65]; *Amann v Switzerland* (App no 27798/95) (2000) 30 EHRR 843 [76]; *Valenzuela Contreras v Spain* (App no 27671/95) (1999) 28 EHRR 483 [46]; *Prado Bugallo v Spain* (App no 58496/00) (2003) [30]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App no 62540/00) (2007) ECHR [76].
[137] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 15 April 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 48.
[138] Advocate General's Opinion in Case 70-10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2012] ECDR 4 [AG 20].
[139] *Ibid*., [AG 21].
[140] *EMI Records (Ireland) Ltd v Eircom Ltd* [2010] IEHC 108 [20].
[141] Stroz Friedberg. ''Independent Expert Assessment of MarkMonitor Antipiracy Methodologies'' (1 November 2012) p. 2.
[142] *Weber and Saravia v Germany* (App no 54934/00) (2006) 46 EHRR SE5 [115]; see also *Kennedy v the United Kingdom* (App no 26839/05) (2010) 52 EHRR [159]; *Uzun v Germany (*App no 35623/05) (2010) 53 EHRR 852 [80].
[143] Home Office, ''Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.'' Accessed 10 May 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 26.
[144] Ofcom, ''Online Infringement of Copyright and the Digital Economy Act 2010 – Notice of Ofcom's proposal to make by order a code for regulating the initial obligations'' Accessed 15 April 2015. http://stakeholders.ofcom.org.uk/binaries/consultations/online-notice/summary/notice.pdf, p. 59.
[145] Case 324/09 *L'Oréal SA and others v eBay International AG and others* [2011] ECR I-0000 [55].
[146] Opinion of the European Data Protection Supervisor (EU) of 5 June 2010 'on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)' [2010] OJ C147 in paragraph 44.
[147] *Ibid*., in paragraph 46.
[148] Opinion of the European Data Protection Supervisor (EU) of 24 April 2012 'on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America' [2012] in paragraph 41.
[149] *Ibid*., in paragraph 25.
[150] Advocate General's Opinion in Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 119].
[151] See generally G.H. Griffin, J. The effect of the Digital Economy Act 2010 upon 'semiotic democracy'. *International Review of Law Computers & Technology* 24, 2010; Edwards, L. Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights. *WIPO* 2011; Cusack, N. Is the Digital Economy Act 2010 the most effective and proportionate way to reduce online piracy? *European Intellectual Property Review* 33, 2011; Suzor, N and Fitzgerald, B. The Legitimacy of Graduated Response Schemes in Copyright Law. *UNSW Law Journal* 34, 2011; Bridy, A. Graduated Response American Style: 'Six Strikes' Measured Against Five Norms. *Fordham Intellectual Property, Media & Entertainment Law Journal* 23, 2012; Horten, M. The Digital Economy Act in the dock: a proportionate ruling? *Journal of Intellectual Property, Information Technology & E-Commerce Law* 3, 2012; Mendis, D. Digital Economy Act 2010: fighting a losing a

battle? Why the ‘‘three strikes’’ law is not the answer to copyright’s latest challenge. *International Review of Law Computers & Technology* 27, 2013; Giblin, R. Evaluating Graduated Response. *Columbia Journal of Law & the Arts* 37, 2013.

[152] In terms of my own research, see also Romero-Moreno, F. The Three Strikes and you Are Out Challenge. *European Journal of Law and Technology* 3, 2012; Romero-Moreno Felipe, ‘‘The Digital Economy Act 2010 and the proportionality of tracking software technologies’’ Accessed 24 August 2014. http://bileta.ning.com/profiles/blogs/the-digital-economy-act-2010-and-the-proportionality-of-tracking; Romero-Moreno, F. Unblocking the Digital Economy Act 2010; human rights issues in the UK. *International Review of Law Computers & Technology* 27, 2013. Romero-Moreno, F. Incompatibility of the Digital Economy Act 2010 subscriber appeal process provisions with Article 6 of the ECHR. *International Review of Law Computers & Technology* 28, 2014; Romero-Moreno Felipe and G.H. Griffin James ‘‘BILETA response to IPO consultation to changes to penalties for online copyright infringement’’ Accessed 24 August 2014. http://uhra.herts.ac.uk/bitstream/handle/2299/16326/BILETA_Response_to_IPO_Consultation_on_Changes_to_Penalties_for_Online_Copyright_Infringement.pdf;jsessionid=DE7641813BC0B9C5F08B3293FEDC25E1?sequence=2 .

[153] Home Office, ‘‘Covert Surveillance and Property Interference – Revised Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000.’’ Accessed 15 April 2015. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf, p. 26.

[154] Opinion of the European Data Protection Supervisor (EU) of 24 April 2012 ‘on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America’ [2012] in paragraph 25.

[155] Harbor Labs, ‘‘Evaluation of the MarkMonitor AntiPiracy System’’ (3 March 2014) p. 2.

[156] *S and Marper v the United Kingdom* (App no 30562/04 and 30566/04) (2008) ECHR 1581 [99]; *Rotaru v Romania* (App no 28341/95) (2000) 8 BHRC 449 [57]-[59]; *Liberty and others v the United Kingdom* (App no 58243/00) (2008) 48 EHRR 1 [62]-[63].

[157] European Data Protection Supervisor, ‘‘EDPS response to the Commission’s Consultation on its Report on the application of IPRED’’ (8 April 2011) Accessed 15 April 2015. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2011/11-04-2011_IPRED_EN.pdf, p. 8.

[158] Ruben Cuevas and others, ‘‘Unveiling the Incentives for Content Publishing in Popular BitTorrent Portals’’ Accessed 15 April 2015. http://eprints.networks.imdea.org/463/1/06381497.pdf , p. 1.

[159] *Ibid*., 2.

[160] Advocate General’s Opinion in Case 275/06 *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* [2008] ECR I-271 [AG 119].

[161] Ofcom, ‘‘Digital Economy Act Online Copyright Infringement Appeals Process - Options for Reducing Costs’’ Accessed 15 April 2015. http://www.culture.gov.uk/images/publications/Ofcom-appeals_cost_advice_with_redactions.pdf , p. 17.

[162] Stevens Le Blond and others, ‘‘Angling for Big Fish in BitTorrent’’ Accessed 10 May 2014. http://hal.inria.fr/docs/00/45/12/82/PDF/bt_angling.pdf, p. 5.

[163] TorrentFreak, ‘‘NSA Authorized Monitoring of Pirate Bay and Proxy Users’’ Accessed 15 April 2015. http://torrentfreak.com/nsa-authorized-monitoring-of-pirate-bay-and-proxy-users-140218/

[164] Stevens Le Blond and others, ‘‘Angling for Big Fish in BitTorrent’’ Accessed 15 April 2015. http://hal.inria.fr/docs/00/45/12/82/PDF/bt_angling.pdf, p. 6.

[165] *British Telecommunications Plc & Anor, R (on the application of) v The Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) [241].