

Dealing with domain names used in connection with criminal activity
Background Report on Views Expressed

Micheál O' Floinn
Queen Mary, University of London

Preface

- I. Nominet commissioned this report asking for an independent and academically-rigorous assessment of the legal issues arising from the practice of suspension of domain names, so as to ensure a focused discussion at the issue group meeting. My terms of reference were flexible, but emphasis was placed on addressing the issues raised by respondents to the issue group brief and questions of liability. To inform my research, I conducted numerous interviews with the Nominet executive, Law Enforcement Agencies, and other associations. Throughout the report, perspectives are often attributed to these organisations, though it is to be mentioned that official positions of organisations may not accord with the view of the interviewee.

- II. The following report is, therefore, intended to be a synthesis and critical analysis of these perspectives, as well as other issues and information which I deemed relevant to the discussion. It is important to emphasise that this is an academic consultancy report, and does not constitute legal advice. Any views expressed are my own, and do not represent those of either Queen Mary or Nominet.

Executive Summary

- III. Despite many registries and registrars having abuse policies and terms and conditions concerning criminal use of domain names, publication of the issue group brief on dealing with domain names associated with criminal activity resulted in considerable concern being expressed by respondents. Some of the concerns raised related to the legitimacy of Nominet's suspensions, the perceived lack of 'fair trial' rights being afforded, and the legality of police powers of 'seizure.' Many of these comments demonstrated some misunderstanding both of the nature of the contractual relationship between Nominet and registrants, and of the legal nature of police requests for suspensions.

- IV. Other views expressed, however, demonstrated thorough understanding of the complexity of the issues raised. These included: whether suspensions by Nominet were required given powers of registrars and hosts, the types of activities with which an abuse policy should deal, the potential curtailment of the freedom of expression, whether court orders were required for seeking suspensions and, in the absence of court orders, what would constitute a legitimate request and whose authority Nominet should accept. An issue which was not mentioned or realised by an overwhelming majority of the comments, however, was the potential criminal liability which Nominet faces if it fails to suspend having been put on notice of criminality. This could take numerous forms, ranging from liability as a principal offender, or accessory, or for failing to report certain criminal activity, and will have an impact upon the answers to many of the issues raised. I address the question of liability towards the end of the report.

Section 1: Background

1. Nominet's registrant terms and conditions currently do not explicitly prohibit use of domain names for criminal purposes. This may well be implicit in the contract, and a registrant may be further bound by such terms in the registrar contract, but the issue is assuming increasing importance, since Law Enforcement Agencies (LEAs) now seek a more formalised route for requesting Nominet to suspend domain names.
2. Thus far, 2667 domains have been locked by Nominet¹, primarily in consumer protection cases such as sale of counterfeit products, and fraud and phishing scams. Instructions from the Serious and Organised Crime Agency (SOCA) and the Metropolitan Police Central e-crime Unit (PCeU) have been acted upon², though Nominet will always forward requests to the relevant registrar in the first instance, following an initial internal check by Nominet. PCeU indicated that they now generally do not approach hosts or registrars and primarily deal with Nominet when seeking suspensions. This allows PCeU to draw attention to a large number of domains at one time, rather than approaching numerous registrars individually, although since Nominet forwards instructions to registrars, this approach may be regarded as a mere transfer of the workload. SOCA, on the other hand, normally contacts the host in the first instance. The detail in police notifications varies but generally only involves the domain name and a basic outline of the crime. Of all domains suspended, Nominet has received less than 5 complaints from registrants, which were informal in nature.
3. The lack of an abuse policy is in contrast with many other registries, such as the Public Interest Registry (.org)³ and Afflias (.info)⁴, both of which list a number of acts constituting abuse, and specifically reserve the right to cancel any registration or lock a domain name for breach of these terms. As of December 2010, the registry of .co, a new domain extension, also has a rapid domain compliance process in place which can be triggered through private complaint, or following request from government or enforcement agencies.⁵ Registry-registrant agreements have similar effect with Generic Top Level Domains (gTLDs) such as .jobs⁶, .coop⁷, and .pro⁸, and Country Code Top Level Domains (ccTLDs) such as .eu⁹, .de¹⁰, .nl¹¹ and .ie¹², clearly prohibiting criminal use of domains and affording the registry a power of suspension or termination for such a breach of contract.¹³ This is also a frequent feature of registrar-registrant contracts. Of Nominet's ten most popular registrars, nine require use of the domain to be lawful, with seven providing non-exhaustive lists of the types of abuse prohibited by the agreement. These include

¹ Figures up-to-date as of 04/03/2011.

² And very occasionally Trading Standards, and the Internet Watch Foundation. (IWF)

³ <http://www.pir.org/why/security/abuse>

⁴ <http://www.info.info/information/anti-abuse-policy>

⁵ <http://www.cointernet.co/global-responsibility/rapid-domain-compliance>

⁶ <http://www.goto.jobs/reg.agreement.asp>

⁷ <http://www.nic.coop/pages/agreements>

⁸ <http://www.registrypro.pro/legal/user-terms.shtml>

⁹ http://www.eurid.eu/files/trm_con_EN.pdf

¹⁰ http://www.denic.de/fileadmin/public/services/ENUM/DENIC-ENUM-Domain_Terms_and_Conditions.pdf

¹¹ https://www.sidn.nl/fileadmin/docs/PDF-files_UK/General%20Terms%20and%20Conditions%20for%20nl%20Registrants.pdf See in particular para. 21

¹² <http://www.domainregistry.ie/index.php/mnudomregs/regtermsandconditions>

¹³ Domain holders of .com, .net, .cc, .tv and other TLDs which are governed by the Uniform Name Dispute Resolution Policy (UDRP) also guarantee that the use of the domain name will not be in a manner which infringes the legal rights of any third parties or applicable laws and regulations. See <http://www.icann.org/en/udrp/udrp-policy-24oct99.htm> at para 2

displaying abusive, defamatory or racist materials, or using the domain to distribute viruses.¹⁴ Eight registrars reserve the right to either terminate the agreement or suspend the domain name for unlawful activity and one (123-reg) has a separate abuse policy, with details as to how abuse was to be reported. It is clear, therefore, that most registries and registrars are already empowered by their contracts with registrants to take action against abusive or criminal behaviour, and normally have the freedom to suspend, without notice, for any such breach.

4. Registration abuse is frequently cited as a major contributing factor to criminal use of domain names, and some police instructions relate entirely to drawing Nominet's attention to inaccuracies in registration information, which Nominet has the discretion to deal with through an accelerated process. At Nominet, domain names are allocated on a strictly first-come, first-served basis, with registration generally being done via registrars, since it is substantially cheaper for the registrant. There is no territoriality nexus required for applying for a .uk domain, meaning individuals from across the world can be .uk registrants, and the process involves no assessment of the veracity of any information provided. Names and addresses are published on the WHOIS, unless the registrants are non-trading individuals and opt out of having their address included.
5. Currently, the Internet Corporation for Assigned Names and Numbers (ICANN) is conducting research into the area of registration abuse, but of note for present purposes is that it is also considering the area of illicit *use* of domain names. The Generic Names Supporting Organization (GNSO) of ICANN chartered the 'Registration Abuse Policies Working Group' (RAPWG) which published its final report in May 2010, dealing with a range of issues such as: registration abuses, WHOIS access problems, uniformity of all in-scope ICANN agreements concerning registration abuse, collection and dissemination of best practices, and uniformity of reporting abuse processes. The RAPWG went to some lengths to distinguish malicious *use* of domain names, from registration abuse¹⁵, the former being outside ICANN and the GNSO's policy-making purview.¹⁶ Nevertheless, the GNSO Council on the 3rd February 2011 passed a resolution requesting a discussion paper "on the creation of non-binding best practices to help registrars and registries address the abusive registration of domain names in accordance with the Registration Abuse Policies Working Group Final Report."¹⁷ Specific issues which are to be addressed include practices for suspending domain names, and "creating anti-abuse terms of service for possible inclusion in registrar-registrant agreements by registrars who adopt them, and for use by TLD operators who adopt them."¹⁸ This discussion paper, when published, will no doubt be of significant value to all registries and registrars considering the introduction of abuse policies.
6. The adoption of abuse policies by registries and registrars is, therefore, an issue which is gaining greater prominence and it will become more controversial domestically if, or when, the amendments to the Communications Act 2003, as provided for in ss. 19-21 of the Digital Economy Act 2010, come into force.¹⁹ These provide the Secretary of State with the power to

¹⁴ An example of a detailed list of prohibited acts is the use policy for register.com, available at:

http://www.register.com/policy/acceptable_use_policy.rcmx

¹⁵ Registration Abuse Policies Working Group Final Report (29 May 2010, at 20-25) Available at:

<http://gns0.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf>

¹⁶ Though there was some dissent within the RAPWG on this point. *Ibid.* at 24

¹⁷ GNSO Resolution 20110203: Available at <http://gns0.icann.org/resolutions/#201102>. While this sentence suggests consideration of abusive registration only, the RAPWG recommendations were clearly referring to abusive *use* of domain names.

¹⁸ *Ibid.*

¹⁹ Section 48(3) provides that these sections will come into force on such day as the Secretary of State may appoint.

appoint a manager of a domain registry, or to compel alteration of the constitution of a registry upon application to court, if there is a serious relevant failure by the registry to comply with practices that are to be prescribed.

7. This should give further impetus for consideration of Nominet's role in the prevention of abuse, and if Nominet does ultimately introduce an abuse policy following this current process, it is likely to have much wider implications for the registry and registrar industry. Nominet is, after all, considered to be a benchmark of excellence for registry providers, and .uk is widely seen as one of the most trusted domains.²⁰ This is reflected in the fact that Nominet currently has over 9 million .uk registrations meaning it is the fourth largest Top Level Domain (TLD) in the world, and second largest Country Code Top Level Domain (ccTLD).²¹ Nominet undoubtedly wishes to maintain this status, and further its vision of making the internet a trusted space.²² However, judging from the comments received following publication of the issue group brief²³, articulation of any new abuse policy, or maintenance of its current position, is going to require extremely careful consideration, and public transparency. A difficult path must be navigated between perceptions of .uk becoming an instrument of a police state, which fails to respect basic human rights norms, and perceptions of Nominet being indifferent to an increasing volume of e-crime²⁴, which carries with it its own risk of criminal liability for Nominet, as will be discussed at the end of section two.

Section 2: Spectrum of Views and Issues to Consider

a. Is there a need for an abuse policy?

8. As mentioned, suspension of a domain name can occur through the registrar's 'investigation lock', and some of the comments received expressed the view that this power was sufficient. Nominet's role was seen as superfluous, since the registrar not only had the same power, but would also have more information than Nominet, and as such be in a better position to track the individual for the purposes of a criminal investigation.²⁵ Alternatively, police could request action from the hosting provider, and it was argued this would be a more appropriate action for some crimes. For example, hosting providers could remove individual malicious pages, while the rest of the website would continue to resolve. This was seen to be a more sophisticated and proportionate approach, with less likelihood of collateral impact on innocent registrants. Indeed, examples already exist of inadvertent suspensions with a recent action against 10 websites²⁶, in a joint operation between the Department of Justice (DOJ) and U.S. Immigration and Customs Enforcement (ICE), resulting in an estimated 84,000 web sub-domains being affected.²⁷ Another argument made against Nominet taking action pointed to its ineffectiveness since individuals

²⁰ See Nominet's 'Domain Name Industry Report' (2010) at 31. Available at: http://www.nominet.org.uk/digitalAssets/46541_DNIR10.pdf

²¹ http://www.verisigninc.com/assets/Verisign_DNIB_Nov2010_WEB.pdf

See also Domain Name Industry Report. *Ibid.* at 8

²² <http://www.nominet.org.uk/about/background/nominetonapage/>

²³ <http://www.nominet.org.uk/policy/issuegroups/current/domainsassociatedwithcrime/>

²⁴ The Detica report, *The Cost of Cyber Crime*, commissioned by the Cabinet Office and published on the 17th February 2011, estimated that cybercrime is costing the UK economy £27 billion a year. Available at:

<http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf>

²⁵ This certainly appears to be the position of the German registry, Denic, who state on their site: "Since DENIC is only responsible for the registration of domains, we are unable to counteract illegal contents of websites or spam." Available at:

<http://www.denic.de/en/background.html>

²⁶ http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm

²⁷ <http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959>

can easily take their activities to another TLD, with advice now freely available as to how to avoid countries that are proactive in suspensions.²⁸

9. On the other hand, some LEAs and rights-holders' representatives saw Nominet as bearing greater responsibility, given its overarching role in the registration process, and suggested a two-pronged approach, which would ensure that Nominet could be relied upon for suspensions, with an enhancement of 'due diligence' obligations of registrars also being proposed.²⁹
10. These conflicting comments demonstrate the challenge of fitting Nominet within what has been described as the "value chain" between end-users and other providers of information society services.³⁰ Accessing and utilising a particular website implicates numerous different entities including internet access and hosting providers, search engines, platform providers, and facilitators of financial transactions. All of these parties could take action which would curtail or prevent criminal use of a domain and the difficulty is in determining when action is required from each, and when duties of care arise.³¹ Recent studies³² demonstrate that increasing attention is being paid to a 'value-chain' orientated approach and there are strong arguments against a concentration of responsibility since it can cause an imbalance which stifles the provision of services and innovation.³³ A "joint, well balanced responsibility of the stakeholders in the value chain"³⁴ has been advocated, and there are already signs of parties in the value chain, such as platform providers, who may not be under specific legal duties to act, assuming responsibility and introducing self-regulatory frameworks.³⁵ Nominet's previous action in suspending domains is further evidence of such an assumption of responsibility, and the

²⁸ <http://torrentfreak.com/how-to-stop-domain-names-being-seized-by-the-us-government-110205/>

²⁹ At the time of writing, 113 members of Nominet were ICANN accredited registrars and it is of note that numerous LEAs, including SOCA, recently made certain due diligence recommendations for ICANN to adopt in accrediting registrars and registries and also proposed amendments to the Registrar Accreditation Agreement (RAA). These latter amendments not only suggested passive obligations (i.e. collection of more information at registration), but also active obligations, involving validation of information, and periodic review. The recommendations were endorsed by ICANN's Governmental Advisory Committee (GAC) in its Brussels Communiqué of 23 June 2010, and were also addressed in detail in the Joint GNSO-ALAC (At Large Advisory Committee) Drafting Team's 'Final Report on Proposals for Improvements to the Registrar Accreditation Agreement', which was published on the 18th October 2010. On validation, the Drafting Team suggested that PCI (payment card industry) compliance was to be prioritised. ICANN has indicated its support for the LEA recommendations, but there remains doubt as to whether certain recommendations should be addressed through a new policy initiative, under the GNSO Council's mandate, or through contract negotiations. See 'ICANN Board-GAC Consultation: Law Enforcement Due Diligence Recommendations – Due Diligence and Registrar Accreditation Agreement.' (Draft, 21st February 2011, available at: <http://www.icann.org/en/topics/new-gtlds/gac-board-law-enforcement-due-diligence-recommendations-21feb11-en.pdf>) The law enforcement proposals are included in their entirety as Annex G to the Drafting Team's Final Report on Proposals for Improvements to the RAA.

³⁰ *Moving Towards Balance: A study into duties of care on the internet* (University of Amsterdam 2010) at 11. Available at: <http://www.juriscom.net/documents/resp20101127.pdf>

³¹ In the study, duties of care were described "primarily about the relationship between the government and Internet service providers and usually take the form of regulations and coregulation." *Ibid.* at 9.

³² OECD, *The Economic and Social Role of Internet Intermediaries* (Paris, 2010); Dommering and Van Eijk, *Convergentie in regulering: Reflecties op elektronische communicatie*, Ministry of Economic Affairs, ('s-Gravenhage, 2010). It is noteworthy that the OECD report did not include domain registries as internet intermediaries within the scope of their report, although registrars were included.

³³ *Moving Towards Balance*, above note 30 at 34

³⁴ *Ibid.* at 39

³⁵ *Ibid.* at 31. On the position of auction and selling platforms under the E-Commerce Directive (2000/31/EC), see opinion of Advocate General Jääskinen in *L'Oréal v. eBay*, (Case C-324/09, opinion of 9th December 2010) at paras. 133-151. Numerous examples of other self-regulatory regimes exist, including Facebook's nudity policy, which generated controversy recently due to Facebook's decision to remove pictures which showed a breast cancer survivor's scars. The suspension of a woman's profile due to her having the same name as Prince William's fiancée, Kate Middleton, also raised concern about the social networking platform's internal checks and policies.

fostering of self-regulation by internet service providers (ISPs³⁶) is one of the stated actions of the European Commission's Digital Agenda for Europe.³⁷

11. However, as outlined above, some argue that Nominet should not assume any such responsibility and do not have need for an abuse policy. For reasons of liability alone, this would appear unwise, and it is the opinion of the present author that an abuse policy is necessary. This is not to deny that action by Nominet, in isolation, may push crime to other TLDs, and that co-ordination across all registries will be a challenging endeavour for the future. Nor is it to deny that registrars and hosts may be better placed to take action and provide information. But these points seem to demand clarification of the circumstances when action by Nominet is required, rather than the exclusion of any action altogether.
12. At the time of writing, Nominet had 3644 registrars, 412 of which were based outside of the UK, and hosting providers in many LEAs and rights-holders' investigations are also often non-UK based. A shared experience of these investigatory bodies is that a response from a registrar or host, if based abroad, is often not forthcoming. Numerous examples exist of pressing situations, such as 'paper ticket' scams, where immediate action has been deemed necessary in order to limit consumer harm. It will undoubtedly be a challenge to delineate the precise circumstances when action by Nominet is appropriate, but it would appear to the present author that if, for example, a registrar or host cannot be contacted, or refuses to assist, then Nominet should be approachable for the purposes of seeking suspension in specified circumstances. Enhancing the due diligence and co-operation obligations of registrars could limit the likelihood of action by the registry being necessitated, but an abuse policy would ensure that when exceptional circumstances exist, Nominet will assume responsibility as a stakeholder in the value chain.
13. Furthermore, an abuse policy and pre-determined arrangement as to when and how suspensions might be requested, would lend assurance to members of the public who are sceptical of the existing suspension process. Current relationships with law enforcement can at best be described as *ad-hoc*, and there is a need for elaboration of a formal procedure, to ensure a consistent and proportionate mechanism is in place to safeguard the rights and interests of all parties. This would also assure many registrars who specifically requested Nominet to take the lead on the suspension issue, having expressed considerable uncertainty as to when action by them was appropriate.

b. Legitimacy of Nominet taking action and 'Fair trial' guarantees

14. Many of the comments received raised concerns that Nominet was unlawfully attempting to enforce criminal law, and was relieving the police of the need to prove criminal allegations against individuals. This characterisation, however, blurs and confuses criminal enforcement and Nominet's action when they suspend for illegal material. Nominet's power to suspend derives from the registrant's contractual commitments, and not any public duty to prevent or enforce criminal law. Its choice to suspend is considered in line with its vision of making the internet a trusted space. In almost all instances where Nominet has taken action, it may be justified on the basis of a breach of contract because incorrect registration details were provided. In the few

³⁶ References to ISPs in this document are intended to cover a broad range of entities in the 'value chain', such as hosting providers, and registrars, although in the 'Moving Towards Balance' report, above note 30, ISPs refer only to internet access providers.

³⁷ http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

instances where registration details were accurate, but the content of the site was criminal, the action would be lawful for breach of an implied term not to use the domain for unlawful purposes. Moreover, in the absence of a breach of contract, it could be argued that further legality stems from the common law power to use reasonable force in order to prevent the commission of an offence.³⁸

15. In connection with the legitimacy point was a frequently expressed argument that any suspension by Nominet would be contrary to the principle of “innocent until proven guilty”, and would infringe Article 6 of the European Convention on Human Rights since it is tantamount to punishment without trial. The last three words of that sentence are the key to understanding why fair trial rights are not implicated in any decision to suspend. There has been no criminal charge or trial. In fact, in most instances where suspensions have occurred, no prosecution has ensued.³⁹ This is not to downplay the potentially serious repercussions which suspensions can have on an individual’s business and reputation, or the risks to human rights as a result of an overly reactive suspension policy. However, it is important to recognise that suspension of a domain name is not a criminal penalty, but rather a contractual right, enforced by Nominet.
16. Aside from fair trial rights, questions were also asked of a related issue, namely, the fairness of Nominet’s internal decision-making process. These questions queried whether there would be a right to respond, an ability to re-activate in case of wrongful suspension, and an appeals process. Publication of all suspensions was also called for.⁴⁰ Operational issues are outside the scope of this paper, but these concerns will ultimately need to be addressed by Nominet.

c. What types of activity would an abuse policy seek to discourage?

17. This was one of the most commonly cited, and controversial topics from the public’s comments. A large majority expressed great concern over the human rights implications of the suspension process and feared that it would lead to curtailment of free speech, and censorship. This unease is understandable given some recent suspensions of websites by registrars and hosts including: Amazon’s refusal to host Wikileaks⁴¹, Network Solution’s reaction to Geert Wilder’s movie ‘Fitna’⁴², the suspension of ‘Fitwatch’⁴³ following a Metropolitan Police request to the hosting provider and, in Italy, the suspension of the ‘Savona e Ponente’⁴⁴ blog.⁴⁵
18. This appears to be the most challenging issue before the Issue Group, and the primary question is which types of harm or categories of offences, if any, should Nominet take action against? Thus far, Nominet have suspended in relatively clear-cut examples of illegal activity. A similar trend can be discerned from the US, where the ‘Operation In Our Sites’ initiative of the DOJ and

³⁸ *Walters v WH Smith and Son Ltd* [1914] 1 KB 595.

³⁹ Speaking following publication of the Detica cybercrime report, Security Minister Baroness Neville-Jones stated that she does not “believe that the successful combating of this kind of crime is going to lie primarily in prosecutions.” Available at: <http://www.guardian.co.uk/uk/2011/feb/17/cyber-crime-costs-uk-27-billion-a-year> This approach to the problem, focusing on defence and disruption rather than exclusively on prosecution, was supported by all of those involved in the investigation of e-crime with whom I spoke for the purposes of this report. Either for reasons of online anonymity, or jurisdictional problems with offenders being based outside of the UK, prosecution is often not a viable avenue to pursue.

⁴⁰ See, for example, the Google Transparency Report, though this lacks precise details on individual takedowns. Available at: <http://www.google.com/transparencyreport/>

⁴¹ <http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon>

⁴² <http://news.bbc.co.uk/1/hi/7310439.stm>

⁴³ <http://www.guardian.co.uk/world/2010/nov/16/student-anti-police-website-closed>

⁴⁴ <http://www.savonaepONENTE.com/>

⁴⁵ <http://politics.slashdot.org/story/11/02/13/2259214/Italian-Police-Seize-Blog-Over-Kill-Berlusconi-Satire>

ICE have primarily related to counterfeit goods.⁴⁶ The fear, however, is that this practice will lead to a slippery slope and be used to curtail a further range of offences, both civil and criminal. There are already examples of the ICE diversifying and seeking suspensions for other illicit activities, such as sports streaming sites⁴⁷, and child pornography.⁴⁸

19. Nominet faces a challenge in developing a framework within which it can operate without risk of legal liability. As developed below in section 2(g), Nominet could be criminally liable as an accessory for all criminal offences which occur via .uk domains, when evidence concerning the offence is brought to its attention. Issues of liability may also arise in cases of wrongful suspension and this is more likely for certain categories of crime such as copyright offences, or obscenity and speech offences. This is because these offences are more challenging for assessments of illegality than are fraud offences or child sexual abuse content, or some of the malware distribution sites with which SOCA deals. The reasons for this are twofold. First, these offences will normally involve a balancing of rights and legal interests, which does not pertain to offences such as fraud. Second, there is a lack of harmonisation of laws relating to speech and copyright offences, and the internet is replete with instances where conduct is lawful in one country, but unlawful in others.⁴⁹ One of the recent ICE domain seizures in the US demonstrates this point, since the 'rojadirecta' seizure occurred despite the legality of the site passing judicial scrutiny in Spain.⁵⁰ Beyond copyright, other examples of extraterritorial effects are numerous, and illustrated by US Treasury Department requests to a registrar for suspension of travel websites, which were aimed at European citizens, on the basis of aiding evasions of US travel restrictions to Cuba.⁵¹ Obscenity and speech offences also differ substantially between many states and have long caused difficulties for service providers, such as Facebook, with its internal policy for removing holocaust denial groups previously heavily criticised.⁵²
20. A related problem for Nominet to consider is how it might justify taking action against counterfeit goods but, for example, not against copyright offences. Both carry civil and criminal penalties in England and Wales. Both can be the subject of injunctive relief if hosting providers are within the EU and do not disable access to the infringing content.⁵³ And both involve rights owners who complain of substantial economic impairment when civil remedies are not enforceable against the infringers due to the location of the host and/or registrar. Therefore, with either unlawful activity, Nominet may be expected to take action if the registrar or host refuse to do so.
21. Without defining the circumstances when suspension could occur, many will continue to fear that Nominet will, or could, act as censors and it is for this reason that some sought the creation of a defined list specifying the particular crimes over which action would be taken. This would be

⁴⁶ <http://www.justice.gov/opa/pr/2010/November/10-ag-1355.html>

⁴⁷ http://www.theregister.co.uk/2011/02/07/federal_domain_seizure_slammed/ If the 'Combating Online Infringement and Counterfeits Act' comes into force, even further tools will be at US LEA's disposal for dealing with criminal use of domains. See <http://www.govtrack.us/congress/bill.xpd?bill=s111-3804&tab=summary>

⁴⁸ http://www.dhs.gov/ynews/releases/pr_1297804574965.shtm

⁴⁹ See e.g. Russian music-download sites, which operate legally in Russia. See Kibby, "'The Legal Bit's in Russian': Making Sense of Downloaded Music' in Hunsinger, Klastrup, Allen (eds) *International Handbook of Internet Research*, (Springer 2010) at 295

⁵⁰ http://www.huffingtonpost.com/2011/02/02/rojadirecta-org-seized_n_817458.html For criticism of the current "Operation In Our Sites" initiative, and suspension being an inappropriate response to copyright infringement, see letter by Senator Ron Wyden, to Attorney General Eric Holder and Immigration and Customs Enforcement Director John Morton (February 2 2011), available at: http://www.cdt.org/files/Wyden_Letter_Domain_Name_Seizure_Feb_2011.pdf

⁵¹ <http://www.nytimes.com/2008/03/04/us/04bar.html>

⁵² http://www.pcworld.com/article/164765/facebook_boots_holocaust_denial_groups.html Considering how different states would deal with 'wikileaks' further demonstrates the diversity of legal approaches to speech crimes.

⁵³ See The Electronic Commerce (EC Directive) Regulations 2002, ss. 19-20.

in contrast to the registry and registrar contracts mentioned in the first section (though illustrative lists of types of abuse are often provided) and LEAs indicated resistance to the creation of a fixed category of offences since it could limit responses to newly developing e-crime. A definitive list might also be cautioned against bearing in mind the potential for accessory liability, which applies to all criminal offences.

22. Should a list of specific offences be decided against, an alternative approach that could provide similar assurance, might be to state more broadly that suspensions will only occur for “serious” crime and/or outlining particular levels of harm which would have to exist in order for action to be taken. A further alternative may be to outline the circumstances where Nominet will not act. For example, Interpol’s constitution states at Article 3 that it does not undertake interventions in cases of a political, military, religious or racial character.⁵⁴ Since potential curtailment of freedom of expression was the predominantly expressed concern for members of the public, a statement that Nominet would not take action against certain forms of speech could be considered useful. However, if speech offences such as incitements to commit terrorism are reported, then for liability reasons Nominet may need to take action.

d. Which country’s criminal law would be applicable?

23. Related to the above sub-section, is the question of whether prohibition of unlawful activity should be restricted to breaches of domestic criminal law, as the issue group brief suggested. This suggestion was subject to criticism in the comments received, particularly from organisations involved in the prevention of illicit pharmaceutical products. They expressly called for the prohibition to extend to breaches of foreign law, since a common strategy for rogue pharmacists is to comply with the laws where they are based and where their website is registered and hosted, but to breach the laws of numerous countries to which they deliver goods. This allows them to operate with relative impunity, since it places them outside of law enforcement’s reach. Limiting breaches to the laws of England and Wales, it was suggested, would run the risk of .uk being seen as a safe haven for these rogue pharmacists.
24. However, were Nominet to suspend domain names for breach of foreign law, when it is not a criminal offence in England and Wales, the process of ascertaining whether a breach of contract has occurred would be more difficult to determine. It would be particularly controversial if Nominet were seen to be capable of suspending websites on the basis of requests from States with laws that are at variance with domestic law on issues such as pornography, obscenity and free speech. This could also prove to be a disincentive for registration of .uk domains, though it is to be noted that none of the registry or registrar contracts mentioned in the introduction limited prohibitions of unlawful activity to domestic law only.
25. Regardless of whether action is limited only to breaches of domestic law, it is important to distinguish Nominet’s position, from judicial enforcement. Cases such as *Waddon*⁵⁵ and *Perrin*⁵⁶, for example, have been criticised for extending obscenity laws to all foreign-hosted websites, thus widening the jurisdiction of courts to cover material which can have little or no nexus with England or Wales. These jurisdictional controversies, however, are distinct from decisions by Nominet to suspend domain names where the registrant is abroad, operating lawfully in the home country. These individuals have chosen to enter into a contract with Nominet, and if Nominet creates an abuse policy which binds the registrant into respecting domestic criminal

⁵⁴ <http://www.interpol.int/Public/ICPO/LegalMaterials/constitution/constitutionGenReg/constitution.asp>

⁵⁵ [2000] All ER (D) 502

⁵⁶ [2002] EWCA Crim 747 (22nd March, 2002)

law, then that is a valid term which can be challenged contractually, in case of wrongful suspension. This applies regardless of where the information is hosted, as some comments suggested. The contractual arrangement may have extraterritorial effects, but does not result in the extraterritorial application of English criminal law.⁵⁷

e. Are court orders required?

26. An overwhelming majority of the comments received regarded police requests as insufficient and called, prior to the suspension of a domain, either for judicial warrants or criminal convictions to have already been secured in respect of the specific offence. Furthermore, it was argued that police should not be granted any more powers than they already have and their current 'seizure' powers for physical property were contrasted with the current domain name suspension process, since the former require an order to be made by a court after conviction of an offence.⁵⁸
27. The above comments demonstrated some misunderstanding as to the actual practice in previous suspensions. Police did not compel Nominet to take action against infringing registrants, nor have they been granted any new powers. Rather, they have instructed suspensions, and Nominet have dealt with these requests by considering whether there has been a breach of their terms of service. However, the question as to whether requests for suspension constitute 'seizures' of property does warrant consideration, because despite Nominet's registrant contract stating that a domain name is not 'property', there has been some domestic judicial comment that it does constitute 'intangible property'⁵⁹ and the European Court of Human Rights has also declared that the open-ended right to use or transfer a domain name constitutes a "possession", for the purposes of Article 1 of Protocol No. 1 to the Convention.⁶⁰
28. This means that if a state authority, such as the police, were to legally compel Nominet to suspend a domain name, this act would either constitute a deprivation of the possession within the meaning of the second sentence of the first paragraph of Article 1 of Protocol no. 1, or a control of the use of property within the meaning of the second paragraph of Article 1 of Protocol no. 1. A binding enforcement power such as this would require a court order, since there is currently no legislative provision granting police such authority. However, non-enforceable requests or instructions do not require a court order and the classification of a domain name as a "possession", for Convention purposes, would not prevent Nominet from taking action when it becomes aware of unlawful use. This was implicitly recognised in the Paeffgen GMBH decision, with the court noting the open-ended nature of the contract between the registry and registrant, and the fact that it could be terminated by the registry without notice, for good cause.
29. It is also useful to consider the context of Nominet's previous suspensions. Many ISPs already take action against infringing websites without a court order⁶¹, and Nominet's phishing feed from Netcraft normally results in immediate suspension by the relevant registrar.⁶² Rights-

⁵⁷ Cf the ongoing controversy in the case of *Commonwealth of Kentucky v. 141 Internet Domain Names*:

<http://www.eff.org/cases/commonwealth-kentucky-v-141-internet-domain-names>

⁵⁸ See e.g. s. 143 of the Powers of Criminal Courts (Sentencing) Act 2000

⁵⁹ See e.g. *Douglas v Hello* [2007] UKHL 21 *Per* Lord Hoffman at para 101.

⁶⁰ *Paeffgen GMBH v Germany* (unreported 5th Section ECtHR decision, 18th September 2007) Application nos. 25379/04, 21688/05, 21722/05 and 21770/05.

⁶¹ Google's Transparency Report lists the number of takedowns worldwide following governmental request, with a further breakdown of the number which were court ordered.

⁶² <http://www.nominet.org.uk/registrars/antiabuse/phishingfeed/>

holders' representatives have also developed various mechanisms for dealing with illicit content, and for contacting registrars and/or hosts. The Publishers Association, for example, have a semi-automated process for authorised individuals to send notices directly to ISPs. The system locates the relevant ISP, checks for repeat infringers and automatically serves the notice. Their website also lists the ISPs who have been most and least compliant, the number of notices served, as well as the most recent infringing sites.⁶³ The Federation Against Copyright Theft (FACT), on the other hand, operates a more individualised policy of prevention and disruption whereby they initially attempt contact with the registrant, and if a response is not received, they then approach the ISP. Evidence packs concerning all illicit content, and previous attempted communications, are provided. The Association for UK Interactive Entertainment (UKIE) approach hosts and registrars in a similar manner, but only do so when a decision to prosecute has been made by a law enforcement agency, while the British Recorded Music Industry (BPI) operate a dual process, with a semi-automated procedure like the Publishers Association, and an individualised approach for specific sites, like FACT and UKIE. The Internet Watch Foundation (IWF) also works in collaboration with the internet industry, LEAs and other entities in order to prevent availability of child sexual abuse images, and obscene and race hate material. It employs numerous tactics in order to do so, including a 'notice and takedown' system.

30. Nevertheless, requiring a court order as a pre-condition for police to request a take-down would bring many benefits. As mentioned, illegality may often be difficult to assess, due either to conflicting state approaches to the issue, or the nature of the offence, and requiring a court order would mean these assessments are made by an experienced and objective entity. Indeed, in the US, the 'Operation In Our Sites' initiative operates through court warrants.⁶⁴ This would lend considerable certainty to the entire process and would provide assurance to registrants and members of the public. Law enforcement would also welcome the creation of a specific power to request a court order for suspension of a domain, since the lack of one has stymied attempts to request suspension of domains in other jurisdictions. It could also be relied upon in cases where a domestic registry/registrar failed to take action following request. However, LEAs resisted the suggestion of a requirement of a court order in every case on the basis that it would be too time-consuming and resource draining. Making Nominet aware of breaches of contract, without recourse to the courts, is seen by them as a flexible and efficient method of tackling consumer protection crimes, particularly in pressing situations. If the process is to be improved, they say, it is through specifying which police entities and units can request suspension and the internal procedures which must be followed by LEAs.

f. Whose authority should Nominet accept, and what would constitute a legitimate request?

31. The internal checks by Nominet and police in the suspension process were a frequently cited source of concern in the views expressed. Many commented on the ambiguity of the phrase "reasonable grounds", and feared action would be taken even where the majority of a site contained legal content and the illicit content was unknown to the registrant. PCeU and SOCA both indicated that certain internal safeguards are in place in order to ensure proportionality is considered. For PCeU, action is only taken when there is a nexus with the UK, "overwhelming criminality" on the site, and a supervisor request for suspension must be approved by either a Detective Inspector, or Chief Detective Inspector. An internal appeals procedure is also in place, where all of the evidence is re-considered upon complaint.

⁶³ <http://www.copyrightinfringementportal.com/>

⁶⁴ <http://www.justice.gov/opa/pr/2010/November/10-ag-1355.html>

32. The adequacy of these internal police safeguards is open to question. PCeU report very few complaints concerning their suspensions⁶⁵, and in March 2011 published a response to a freedom of information request. This document indicated that between December 2009 and November 2010, 1909 domain names were the subject of suspension requests to Nominet, and implied that Nominet had responded by suspending each domain requested.⁶⁶ Nominet reports some differences in figures relating to this level of response, particularly in more recent requests for suspension. Often, action was not taken due to discrepancies in the requests, and it appears that without internal checks by Nominet, police requests could have resulted in wrongful suspensions.
33. This raises concerns as to who should be entitled to request suspensions and the safeguards which need to be in place before a request can be made. Should Nominet respond to requests from all individuals within domestic police forces, private entities such as FACT, BMI and UKIE, or any foreign LEA? Nominet do not seek to act in an investigative capacity and absent judicial authorisation, determining the criminality of certain content may be challenging even for experienced law enforcement officers. Nominet may favour these requests originating from trusted entities since mistakes could result in liability for Nominet, but refusing to react to requests from other entities that have placed Nominet on notice of criminality would carry its own risks. As discussed below, there is an indirect legal pressure to respond to the request, since criminal liability could be incurred for failure to act. Indeed, some LEAs indicated that this has been considered, when a registrar or hosting provider was refusing to remove content.
34. Without legislation determining this, a formalised process between all interested parties which would specify the requirements for a legitimate request, and from whom it can come, appears necessary. To this end, guidance could be sought from the Council of Europe's 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime'⁶⁷, even though Nominet is not a 'service provider' for the purposes of the document.⁶⁸ The guidelines suggest the creation of written procedures for co-operation⁶⁹, which would include appropriate internal checks being taken by law enforcement and defining clearly in their written procedures which personnel can authorise requests.⁷⁰ There is also some guidance as to what such requests should contain, in order to assist verification of the source of requests.⁷¹
35. Some suggest Nominet should only deal with RIPA⁷² single points of contact (SPOCs), since they are the accredited individuals trained to engage with the communications industry. RIPA is a complex statute dealing with a variety of issues such as the interception of communications and undercover surveillance. Part I, Chapter II of the act covers the acquisition and disclosure of communications data, and only certain individuals may authorise access to communications data, and only for specified grounds (which vary according to the relevant public authority in question).

⁶⁵ Between January 2009 and February 14th 2011, PCeU have had 3026 domain names, 1501 emails, and 1984 telephone numbers suspended. Of the 3026 domain names, only 11 sites were reportedly re-activated. One of these involved an administrative error, and was remedied within 12 hours of suspension. In the other cases, sufficient information was present for the suspension, but following appeal, the infringements were seen primarily as civil offences. While they were re-activated, brand owners took action through civil processes.

⁶⁶ http://www.met.police.uk/foi/pdfs/disclosure_2011/february/2010110005000.pdf

⁶⁷ Council of Europe, Project on Cybercrime, (April, 2008), available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567_prov-d-guidelines_provisional2_3April2008_en.pdf

⁶⁸ The guidelines are also intended primarily for 'legally binding' requests.

⁶⁹ Paras 12 and 18

⁷⁰ Para 22

⁷¹ Paras 24-29

⁷² Regulation of Investigatory Powers Act 2000

For police forces, access to communications data requires authorisation by a superintendent or above.⁷³

36. This regime may be a model relevant for the suspension process, though there is a distinction between powers to access communications data, as part of a criminal investigation, and powers to request suspension of a domain, as part of an enforcement action. Furthermore, there are currently over six hundred SPoCs within the UK, and if all could request suspensions, Nominet may need to exercise greater caution prior to suspension, unless the grounds for making a request are highly specified. SOCA are in favour of finding parallels for determining appropriate levels of internal authorisation, and PCeU also seek the creation of standard operating procedures, and a data sharing arrangement between themselves and Nominet. However, requiring the same level of authorisation as under RIPA (i.e. superintendent) for each request was resisted by PCeU since it was deemed to add an unnecessary layer of bureaucracy.

g. Potential Risks and Liabilities

37. There are clear risks attached to the suspension of domain names, and these apply not only to Nominet, but also their registrants. Some registrants claimed they would move their domain to another TLD unless judicial sanctioning was made a pre-condition, because they saw the risk to their business from possible 'false positives' or administrative errors, to be too significant to ignore. Such mistakes could certainly result in damage to customers' reputation and business, and would generate legal and public relations difficulties affecting the reputation of .uk. On the other hand, failures to suspend when informed of criminal use could mean Nominet opens itself to civil or criminal liability. Nominet must effectively engage in a risk management exercise and the choice seems to be between the possibility of incurring criminal sanctions, or suspending and risking civil claims which are indemnified against and for which liability is capped for commercial registrants. Nominet will also need to consider ongoing obligations post-suspension, and whether liability continues to be a risk if it allows re-registration by individuals with identical details, thus facilitating commission of the same, or a similar offence.⁷⁴

1. Liability for non-suspension

38. For many service providers, the question of liability for information made available by third parties is relatively determined due to the E-Commerce Directive.⁷⁵ The relevant provisions of the Directive were implemented in the UK by the Electronic Commerce (EC Directive) Regulations 2002⁷⁶ which provides an additional defence from liability⁷⁷ for mere conduits, and for caching and hosting when the service provider, upon obtaining knowledge or awareness of infringing activity, acts expeditiously to remove access to the unlawful material. These provisions do not apply to Nominet, since licensing use of a domain name would not constitute hosting, caching, or acting as a mere conduit.⁷⁸ The result is that there is arguably more uncertainty as to

⁷³ The Regulation of Investigatory Powers (Communications Data) Order 2010 S.I. 2010/480

⁷⁴ In the context of hosting providers, and the need to implement procedures in order to prevent re-offending, *see* opinion of Advocate General Jääskinen in *L'Oréal v. eBay*, above note 35, at para. 168. A possible model of interest may be Ofcom's 'Consumer Protection Test', which involves listing companies and individuals that have used telephone numbers to cause serious or repeated consumer harm, in order to prevent further allocation of numbers to these individuals. Further information is available at: <http://stakeholders.ofcom.org.uk/telecoms/numbering/applying-activating-tele-no/consumer-protection-test/>

⁷⁵ Directive 2000/31/EC

⁷⁶ S.I. No. 2013 of 2002

⁷⁷ Additional to any defence provided for in the offence itself.

⁷⁸ It could be argued, however, that Nominet is the host for the domain name itself, which can be criminal if, for example, it is causing an advertisement of indecent photographs of children to be published. *See* Section 1(d) of the Protection of

whether, or when, Nominet will be criminally or civilly liable for the activities of registrants. Such liability is likely to arise if Nominet acquires knowledge of criminal use of a domain name, through a request for suspension, but nevertheless refuses to suspend. The following are three examples of how such a refusal could result in criminal liability.⁷⁹

39. First, the knowledge of the criminality, and refusal to respond to it, could render Nominet complicit in the crime and punishable as an accessory under s. 8 of the Accessories and Abettors Act 1861.⁸⁰ The precise meaning of ‘aiding’ and ‘abetting’ has not been conclusively determined, but they “are generally considered to cover, respectively, assistance and encouragement given at the time of the offence.”⁸¹ It could be argued that Nominet’s role here is too remote and did not assist the commission of the offence, given the lack of positive encouragement. Reliance could be placed on the decision in *A-G’s Reference (No. 1 of 1975)*⁸² which required a “meeting of minds” between the secondary party and the principal, in order for liability to arise. Nevertheless, even passive acquiescence can be sufficient to aid an offence, and ‘what matters’ for this type of offence, was neatly described by the Court of Appeal as: “knowledge of the principal offence, the ability to control the action of the offender, and the deliberate decision to refrain from doing so.”⁸³ This case is distinguishable in that it concerned a company, and the acts of its employees, but the position of Nominet is analogous, since it has a right to control the action of registrants, through its terms and conditions and ability to suspend domain names. Further, Nominet would have knowledge of the *specific* offence which is being, or will be committed.⁸⁴ There is, therefore, a distinct possibility that failure to suspend a domain name could render Nominet or its employees criminally liable as accessories to offences committed by registrants through the use of their domain.
40. Second, Nominet could be prosecuted as a principal offender. The inchoate offences of ‘assisting an offence’ under ss. 45-46 of the Serious Crime Act 2007⁸⁵, could be charged in the alternative to acting as an accessory, and other examples of potentially applicable offences are contained in s. 107(1)(d)(iii)⁸⁶, s. 107(2A)⁸⁷ and s. 198(2)⁸⁸ of the Copyright, Designs and Patents Act 1988

Children Act 1978. It is also noteworthy that Nominet would fall within the definition of an “information society service”, the definition of which is paraphrased at Recital 17 of the E-Commerce Directive as covering “any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service...”

⁷⁹ On corporate liability, see Hooper LJ, and Ormerod (eds), *Blackstone’s Criminal Practice* (2010), at A5.17: [A] company can sometimes be guilty of an offence requiring a state of mind under a principle which identifies the acts and state of mind of a senior employee or officer of the company with the company itself.” Individual liability for employees of Nominet could also ensue.

⁸⁰ Section 44 of the Magistrates Court Act 1980 contains a similar provision for summary and either way offences. It is of note that under both s. 8 and s. 44, an accessory is liable to be tried as a principal offender.

⁸¹ Blackstones above note 79 at A5.1

⁸² [1975] Q.B. 773 at 779

⁸³ *JF Alford Transport Ltd* [1997] 2 CR App R 326 (CA) at 334

⁸⁴ Glazebrook, ‘*On being required to be a policeman, untrained and unpaid*’, Cambridge Law Journal (2001) 537 at 549

⁸⁵ Section 65(2)(b) states that “failing to take reasonable steps to discharge a duty” constitutes the doing of an act capable of assisting the commission of an offence. The common law duty to assist a constable who calls for assistance in dealing with a breach of the peace could constitute such a duty. Failure to assist is itself an offence. See *Brown* (1841) Car & M 314; *R v Sherlock* (1866) LR 1 CCR 20; *Waugh* (1976) The Times, 1 October 1976). While potentially incredibly broad in scope, this offence is rarely prosecuted.

⁸⁶ “A person commits an offence who, without the licence of the copyright owner ... (d) in the course of a business ... (iii) exhibits in public ... an article which is, and which he knows or has reason to believe is, an infringing copy of a copyright work.”

⁸⁷ “A person who infringes copyright in a work by communicating the work to the public—

(a) in the course of a business, or

(b) otherwise than in the course of a business to such an extent as to affect prejudicially the owner of the copyright, commits an offence if he knows or has reason to believe that, by doing so, he is infringing copyright in that work.”

⁸⁸ “A person commits an offence who causes a recording of a performance made without sufficient consent to be—

(a) shown or played in public, or

(CDPA 1988). A strong argument can be made that these latter copyright offences ought not to apply to Nominet, since Nominet do not directly exhibit or communicate copyrighted material to the public.

41. Nevertheless, it can easily be imagined how a precedent for wider interpretation of such offences could be taken, if a court is faced with the prosecution of a more sensitive offence. The offences contained in s. 1 and 2 of the Terrorism Act 2006 (TA 2006)⁸⁹, are prime examples and apply if a person ‘endorsed’ a particular terrorist-related statement.⁹⁰ Section 3 enumerates how this is to be applied to internet activity involving a statement being “published or caused to be published in the course of, or in connection with, the provision or use of a service provided electronically...”⁹¹ A statement has the endorsement of a person, if a constable has provided notice in accordance with s. 3(3) and the relevant person has failed, without reasonable excuse, to comply with the notice. Like the copyright offences mentioned above, if Nominet was faced with a prosecution under s. 1 or s.2 of the TA 2006, it would contend that it had not itself published or caused the statement to be published. However, a judge may tend to look more critically at a failure by Nominet to suspend a domain name, upon receipt of a s. 3(3) notice, even if Nominet was not directly responsible for the publication. This could create a wider precedent for Nominet’s responsibility for other offences, such as the aforementioned copyright offences, when a copyright owner or representative makes Nominet aware of the infringement.
42. Finally, an offence may be committed short of failing to suspend a domain. If Nominet acquires knowledge of certain criminal activity, but fails to inform the police of that activity, this could result in liability.⁹² Modern legislation has created a number of offences for failure to report criminal activities, such as ss. 19 and 38B of the Terrorism Act 2000 (TA 2000), which respectively criminalise failure to report suspicions of certain terrorist offences having been committed when the information is acquired in a professional capacity, and failure to disclose information which would be of material assistance in the prevention of an act of terrorism. Section 328(1) of the Proceeds of Crime Act 2002 (POCA 2002) also creates an offence when a person “enters into or becomes concerned” in a money laundering arrangement, unless an authorised disclosure is made under s. 338.⁹³ This broad offence not only covers deliberate or dishonest offenders, but also those who become concerned in an arrangement which they suspect involves a money laundering offence. If Nominet suspect that a website is being used to commit such an offence, then their contract with the registrant, which licenses use of the domain name, could be seen as an arrangement facilitating the offence. Suspension of the domain name would be required, as suspension of a bank account was required in *Squirrel Ltd v National Westminster Bank*⁹⁴, in order to avoid criminal liability under s. 328(1).
43. In terms of potential civil liability, the law would appear to be more certain, or at least more certain than the question as to whether Nominet could be prosecuted for the criminal offences mentioned above under the CDPA 1988. Liability for secondary participation in copyright offences was recently reviewed by the decision of Kitchin J. in *Twentieth Century Fox Film and*

(b) communicated to the public, thereby infringing any of the rights conferred by [this Chapter], if he knows or has reason to believe that those rights are thereby infringed.”

⁸⁹ These relate to the encouragement of terrorism and dissemination of terrorist publications respectively.

⁹⁰ s. 1(6) and s. 2(9)

⁹¹ s. 3(1), emphasis added.

⁹² Even if criminal liability is not a risk for failure to report a particular offence, Nominet may still wish to consider reporting incidents over which action was taken, since failures to report crime, when put on notice, could engender reputational harm.

See <http://www.smh.com.au/technology/facebook-failed-to-tell-police-about-paedophile-porn-ring-20100826-13ual.html>

⁹³ S. 328(2)

⁹⁴ [2006] 1 WLR 637

others v. Newzbin.⁹⁵ Three forms of secondary liability were discussed: authorising acts of infringement by its members, procuring and participation in a common design, and communicating copyrighted works to the public, which is also a tort under s. 20 of the CDPA 1988. Unlike the criminal law relating to accessory liability, the first two forms of liability are narrower and would not extend to Nominet, even if it deliberately did not suspend an infringing website.⁹⁶ It is also unlikely that Nominet could be said to have communicated the material to the public. Passive services, which did not directly make the material available, were implicitly found not to ‘communicate’ for the purposes of s. 20.⁹⁷ This interpretation of s. 20 may also be informative in the determination as to whether criminal liability should be imposed under the CDPA 1988, for communication to the public.

2. Liability for wrongful suspension.

44. The converse to the risk of liability arising due to a failure to suspend is the risk that suspension itself will be wrongful, either because the registrant was not engaged in illegality, or due to a mistaken suspension. Any registrant who believes this occurs would have recourse to the English courts for a breach of contract. This could be combined with other private remedies, such as an action for negligence seeking to recover any losses caused as a result of the suspension, or defamation, for potential damage to reputation having been associated with criminality, or an unreliable website. Furthermore, if the suspension occurred due to a request by police, this request could be challenged if there was a breach of Convention rights.⁹⁸ Nominet’s position under the HRA 1998 was also mentioned in the comments, and there can be confusion as to Nominet’s legal status and from where it derives its legal authority. However, as a private entity, Nominet is not directly liable under the HRA 1998, and current case-law would suggest it is not a hybrid authority.

⁹⁵ [2010] EWHC 608 (Ch)

⁹⁶ On authorisation of acts of infringement, Kitchin J. stated that the term “‘authorise” means the grant or purported grant of the right to do the act complained of. It does not extend to mere enablement, assistance or even encouragement.” *Ibid.* at para 90. On entering into a common design, he held that “mere (or even knowing) assistance or facilitation of the primary infringement is not enough. The joint tortfeasor must have so involved himself in the tort as to make it his own. This will be the case if he has induced, incited or persuaded the primary infringer to engage in the infringing act or if there is a common design or concerted action or agreement on a common action to secure the doing of the infringing act.” *Ibid.* at para 108.

⁹⁷ *Ibid.* at para. 125

⁹⁸ As a ‘core’ public authority, every police action, whatever its nature, is subject to the ECHR under s. 6(1) of the Human Rights Act 1998. See *YL v. Birmingham City Council*, [2007] UKHL 27; [2008] 1 AC 95 at para. 119.

Section 3: Questions for Consideration

1. Should Nominet have an abuse policy and would creation of one be in line with its vision of making the internet a trusted space? [section 1, and section 2(a)]
2. Should the issue of criminal conduct by domain name holders only be dealt with through registrars and hosts, and/or strengthening the 'due diligence' obligations of Nominet's registrars? Would there be benefits in sharing information with registrars as is currently done with the phishing feed? [section 2(a)]
3. Which types of activity would an abuse policy seek to discourage? [section 2(c)]
4. In what circumstances would suspension of a website be proportionate? [section 2(a) para. 8 & 13, section 2(f) para. 31] Would there need to be an ascertained level of harm or criminality? [section 2(c), paras. 21-22,]
5. How can Nominet avoid the risk of legal liability, when asked to take action against offences which are challenging for assessments of criminality, such as certain alleged speech offences? [section 2 (c), para. 19]
6. Should a list of offences, over which Nominet will take action, be created? [section 2(c), paras. 21-22]
7. Would suspensions be limited to breaches of domestic criminal law, or apply to all countries or those where the registrant expects his activities to have effect? [section 2(d)]
8. What standard of evidence might be required, and who would assess it (e.g. SPoC and/or Nominet)? [section 2(f), para. 31-32]
9. Would a formal relationship be necessary to accept instruction? Who would be able to request suspensions? [section 2(f), para. 33]
10. What principles should govern the form of an acceptable request? Should a formalised standard operating procedure and data sharing arrangement be created between Nominet and law enforcement? [section 2(f), para. 34-36]
11. If suspension does occur, is there a post-suspension continuing obligation to prevent criminal conduct when the registrant uses the same registration details? [section 2(g) para. 37]
12. Would there need to be any form of appeals process? [section 2(b) para. 16]
13. Are there other regulatory or self-regulatory frameworks that would provide useful background or experiences? [see e.g. footnotes 35 & 40 & 74]

Author's Biography

- I. Micheál O'Flóinn is a Ph.D. candidate from Queen Mary, University of London, where he is undertaking research concerning the role of internet service providers in the resolution of jurisdictional problems generated by cybercrime. He was awarded a Graduate Teaching Scholarship in order to pursue his research. Micheál graduated from Trinity College Dublin with an LL.B. degree and was subsequently awarded an LL.M. in Public International Law (Distinction) by the London School of Economics and Political Sciences. He is also an Irish qualified Barrister and was recently called to the Bar for England and Wales (Inner Temple) following successful completion of the Bar Transfer Test.

- II. Micheál has previously taught the law of evidence at Queen Mary, and has delivered conference papers on certain legal implications arising from online surveillance. His recent paper, 'Using Social Networking Evidence Sites in Criminal Investigations', written alongside David Ormerod, is due to be published this year. Prior to teaching at Queen Mary, Micheál worked at the International Criminal Court and the European Commission.