

# Domain names used in connection with criminal activity

## *Response to Revised Draft Recommendations*

This document is a response to the revised draft recommendation<sup>1</sup> by the Nominet Issue Group considering ‘domain names used in connection with criminal activity’ published on 17<sup>th</sup> October 2011.

As a preliminary comment, asking for feedback on a document email at 15:32 on 17<sup>th</sup> October to be returned in readiness for a meeting on 20<sup>th</sup> October does not appear to me to be a reasonable period for consultation. For this reason, I hope you will excuse any typographical errors in this response.

I have already made a detailed submission<sup>2</sup> on what I believe the correct principles should be, I will try to avoid repetition and concentrate on the draft principles as proposed. I made a further submission<sup>3</sup> on September 2011 on the draft principles, and am pleased to see some but not all of my suggestions have been included. I have briefly stated to what degree the revised proposals address my four main criticisms in a summary section.

***“In line with the company’s public purpose mission to promote a safe and trusted internet space, and in order to defend its private interests, Nominet should have a specific and published abuse policy that governs an expedited process by which it addresses the criminal use of domain names in its terms and conditions.”***

1. I welcome the attempt to make more specific the justification for the policy, but I still do not agree that such a policy is *necessary* in order to defend Nominet’s private interests, or to promote a safe and trusted internet space. Requiring a one million pound behaviour bond from each registrant would no doubt also help defend Nominet’s private interests, but that is not suggested because it is harmful to registrants. Couching the argument in terms of Nominet’s needs and public purpose is to miss the point. The first argument that the Issue Group needs but fails to make here is that the need to protect two main sets of stakeholders (consumers and rights holders) outweigh the dangers to registrants in terms of collateral damage and freedom of expression. Obviously, this is a value judgment. The second argument that the Issue Group needs but fails to make is that if such an imbalance exists, it is for Nominet rather than the courts or politicians to address it; as set out in my first response, Nominet is proposing to act here unlike any other public purpose organisation that provides a service, and *prima facie* that requires justification.
2. The issue group still appears to be shying away from the point that it is dealing with alleged criminal activity, and not criminal activity. Few people (if anyone) would object to Nominet suspending domain names in connection with activity that a court had determined to be criminal. There are two reasons why this is significant. Firstly, Nominet should be up front about what it is doing (acting without the authority of a

---

<sup>1</sup> See [http://www.nominet.org.uk/digitalAssets/53051\\_Issue\\_group\\_draft\\_recommendations\\_171011.pdf](http://www.nominet.org.uk/digitalAssets/53051_Issue_group_draft_recommendations_171011.pdf)

<sup>2</sup> Submitted through the Nominet process, but also to be found at <http://blog.alex.org.uk/2010/11/26/domain-names-and-criminals/>

<sup>3</sup> Submitted through the Nominet process, but also to be found at: <http://blog.alex.org.uk/2011/09/01/nominet-and-soca-a-romance-in-three-parts/>

court). Secondly, for Nominet's own protection: if Nominet describes a domain name suspension as being 'under its policy for dealing with criminal activity' (as is suggested under Issue Group recommendation 15), and the activity turns out not to be criminal after all, I suspect the registrant's chances of a successful action in defamation would be higher than had Nominet described it as 'alleged criminal activity'.

***“With a view to providing certainty and clarity for stakeholders, Nominet’s abuse policy should clearly define the circumstances and procedures by which Nominet will suspend a .uk domain name following notification that it is being allegedly used in connection with criminal activity.”***

3. If there is to be such a policy, certainty and clarity are to be welcomed.
4. However, in order to achieve certainty and clarity, one key point is that the domain names to which it applies must be understood. I repeat the point I made before about linkage. There appears to be no linkage proposed between the offence, the offender, the registrant and the domain name. The title of the consultation is 'domain names used in connection with criminal activity', but nowhere in the proposals does 'in connection with' get mentioned, nor what type of connection is required. Point 6 suggests the domain must be have an 'association' with criminal activity – a hugely wide test. Point 12(d) requires that the domain name is 'integral' to carrying out the criminal activity, which is far narrower. Points 2 and 8 say 'in connection with' which might be half way between.
5. I repeat the example I gave before, as this is currently one of the most serious gaps in the proposal: *‘Let us suppose that an alleged fraudster has registered his own personal email address john@dishonestjohn.co.uk, and is using that to communicate with other people. If the alleged fraudster is not using the domain name to perpetrate the fraud, but lack of an email address will hinder him, can the domain name be suspended? If he has communicated once with his alleged victim by email? What if the email address is john@johnsemployer.co.uk, and thus has a totally different (and most likely innocent) registrant? What if it is john@demon.co.uk or john@hotmail.co.uk? What level of connection to the alleged criminal activity must the domain name have in order to merit suspension, and what level of connection to the registrant? This, it seems to me, is key, particularly in order to avoid collateral damage. At the very least suspension should be limited to cases where the registrant is either the alleged perpetrator or is complicit with the crime.’*

***“The policy’s operation should be transparent and consistent, to promote the confidence of all stakeholders. It is important that Nominet’s procedures replicate due process as far as possible to protect the rights and freedoms of registrants, and to mitigate the potential for disproportionate outcomes.”***

6. I agree with the first sentence.
7. If what Nominet's policy aims to do is to “replicate due process”, would it not be far simpler to not have a policy at all, and leave the matter to due process?

***“Nominet’s policy must be proportionate in scope, giving recognition to the fair and legitimate interests of registrants.”***

8. Agree. And to be fair it should also seek to recognise the interests of rights holders and internet users, and recognise that their interests may be in conflict.

***“To enable the relatively swift adoption of lightweight procedures, the scope of the policy should apply to a limited subset of criminal activity in the first instance. The policy must explicitly exclude civil disputes and cases where freedom of expression and other fundamental rights of the registrant or third parties are central to the dispute at issue.”***

9. If there is to be a policy, I agree with the first sentence.
10. The second sentence is peculiar in that it suggests that the policy should ‘*explicitly exclude ... cases where ... fundamental rights of ... third parties are central to the dispute at issue*’. This seems to me odd, as the right to life and the right to property are fundamental rights. Are these not precisely the sort of rights that are breached when the targeted criminal activity occurs? For instance, if a domain name is used for credit card fraud, or sale of counterfeit goods, both are issues where the fundamental rights of a third party (the victim) are central to the dispute. Unless the intent is for the policy to not be applicable at all, I would suggest removing the words “third party” or qualifying them so as to refer to users of the domain name or similar.
11. Whilst I welcome the attempt to make more specific the justification for the policy, I still do not agree that such a policy is *necessary* in order to defend Nominet’s private interests, or to promote a safe and trusted internet space. Requiring a one million pound behaviour bond from each registrant would no doubt also help defend Nominet’s private interests, but that is not a policy Nominet has adopted because it is harmful to registrants’ interests. Couching the argument in terms of Nominet’s needs and public purpose is to miss the point. The first argument that the Issue Group needs but fails to make here is that the need to protect the two main sets of stakeholders (consumers and rights holders) driving this discussion outweighs the dangers to registrants in terms of collateral damage and freedom of expression in a significant number of circumstances. Obviously, this is a value judgment. The second argument that the Issue Group needs but fails to make is that if such an imbalance exists, it is for Nominet rather than the courts or politicians to address it; as set out in my first response, Nominet is proposing to act here unlike any other public purpose organisation that provides a service, and prima facie that requires justification. The third argument that the Issue Group needs but fails to make is that this such a policy is the best way to address such an imbalance.
12. Whilst the carve-out for freedom of expression is to be welcomed, I repeat the points I made in the last submission:
  - A. *It will in practice be hard to tell whether, for instance, ‘Wikileaks’ style activity is freedom of expression, or a breach of the Official Secrets Act with commensurate danger to individuals. Moreover, unless Nominet is to be given full details of the alleged crime (this seems unlikely), one might suggest a law enforcement agency is unlikely to put a suspension request in terms of ‘shutting down a site in order to restrict freedom of expression’. How, therefore, is Nominet to know whether freedom of expression is a central aspect of the disputed issue?*
  - B. *I would suggest an explicit carve-out for criminal libel.*
  - C. *I would suggest Nominet determines what it proposes to do concerning alleged exposure of information with a national security impact, prior to implementing the policy.*

***“[As a matter of principle, the issue group believes that the association of a domain with criminal activity should bring the domain within the scope of the abuse policy, potentially rendering it liable to suspension, and that with certain limited exceptions as noted above,***

***the nature of the suspected offence is immaterial.] The way in which Nominet might address a wider set of criminal activities within the policy should be examined under the policy process after an assessment and review of the policy's implementation."***

13. The section in square brackets would be a particularly unwelcome expansion of the scope of this policy. Sending email on a mobile telephone whilst driving is a criminal offence associated with a domain name. Not displaying a business' trading details on a web site (even unintentionally for a matter of hours) similarly. Is the Issue Group really suggesting that as a matter of principle, the nature of the offence is immaterial and these matters should fall within the purview of policy purportedly designed to protect individuals against serious harm? This further illustrates the 'mission creep' / 'thin end of the wedge' point.

14. I agree with the second sentence.

***"The policy should apply where: (a) the nature of the alleged criminal activity creates a clear risk of imminent serious harm to individuals. This would include, for example, phishing, the unlicensed sale of medicines, and botnets; or, (b) the domain is directly involved in the distribution of counterfeit goods."***

15. I agree with limb (a), but fail to see how "botnets" fall within the definition of "imminent serious harm to individuals". Botnets are often used to send spam email, which whilst unlawful and profoundly annoying does not cause imminent serious harm to individuals.

16. I disagree with limb (b), at least without further qualification. Counterfeiting of goods is in general an economic crime against the rights holder. Rights holders are in general well resourced and quite capable of getting injunctions. It seems to me they need no special protection in the way consumers do. If the goods are dangerous, then limb (a) would apply. If the goods are not dangerous (perhaps indistinguishable from the real thing), then the real harm is solely to the economic interests of the rights holder; it seems to me counterfeit goods are no different here to pirated music or software.

***"Domain name suspension by reason of its alleged use in connection with criminal activity should only be undertaken following a notification by a senior officer of a UK public law enforcement authority that has criminal law enforcement duties and has established a "trusted relationship" with Nominet under the policy. As such, notifications from private party or foreign law enforcement agencies should be specifically excluded from this policy."***

17. I agree, and welcome this change.

***"Where a foreign law enforcement agency wishes to make a notification to Nominet, this should be made through the usual mutual legal assistance channels and under a principle of double-criminality."***

18. I agree, and welcome this change.

***"Nominet should develop and publish, in cooperation with UK public law enforcement agencies, a defined framework by which UK public law enforcement agencies can meet the "trusted" requirements. In addition to the requirements outlined at 14(b), this framework could include training, agreements to make notifications under the policy subject to audit procedures, and frameworks to establish SPOC-type procedures."***

19. I agree, and welcome this change.
20. I believe a definition of a ‘UK public law enforcement agency’ would be welcome. My understanding is that various UK bodies are capable of bringing prosecutions, including British Waterways, whose powers are being transferred to a private company. Are all of these potentially ‘UK public law enforcement agencies’? Would the Issue Group consider that in practice the definition should include anyone other than UK constabularies and (perhaps, in its customs guise) HMRC?

***“The ability to make a notification under the policy should only be available to those trusted UK public law enforcement agencies under the principle of ‘last resort’. ‘Last resort’ is defined as the exhaustion of available alternatives before seeking a suspension via Nominet. Such alternatives may include approaching the registrant, the registrar, or the host.”***

21. I agree, and welcome this change.

***“An acceptable notification must (a) Clearly identify the requesting law enforcement agency who must be recognised as a trusted law enforcement agency under the policy; (b) Comply with the procedure set out in the policy and any published materials such as templates by Nominet; (c) Include a declaration of an authorised senior officer on behalf of the agency that suspension of the domain is proportionate, necessary, and urgent and meets the standard set out in 7(a) or 7(b), and that the agency has exhausted available alternatives to deal with the domain; (d) Certify that the evidence gathered to support the notification has been to a prosecutorial standard and that it is ‘beyond reasonable doubt’ that the domain is integral to the carrying out of the alleged crime.”***

22. I agree, and welcome this change.

***“Nominet should take responsibility for notifying the registrant of the suspension unless compelled otherwise by law.”***

23. I agree, and welcome this change.

***“Nominet must provide for appeals mechanisms that enable registrants to swiftly challenge suspensions, to seek remedy through the reversal of the suspension, and potential redress through the contract should Nominet fail to apply the policy correctly. In this connection, the issue group recommends that the Board make available the following range of appeals mechanisms for registrants: (a) A transparent and independent appeals mechanism. (b) The policy should enable recourse directly to the law enforcement agency that has originated the request. (c) Registrants must also have the option of recourse to the judicial system. (d) The policy should define under what circumstances the suspension of the domain might be reversed following remedy by the registrant.”***

24. I agree, and welcome this change.

***“Nominet should publish data related to suspensions on a regular basis. At a minimum, this data should include: (a) The name of the domain (b) The date of the suspension (c) The name of the public law enforcement agency generating the notification (d) A statement of the nature of the alleged offence”***

25. I agree, and welcome this change.

***“Nominet should publish an annual statistical summary of the (a) suspensions (b) appeals (c) categories of alleged offences (d) requesting law enforcement agencies that have been subject to the policy.”***

26. I agree, and welcome this change.

***“There should be no implied obligation to act by Nominet and Nominet should not be restricted by the policy from acting under its existing procedures for breach of contract by a registrant.”***

27. I agree, and welcome this change.

***“When the policy is operational, the Nominet Board should establish an independent panel to report on how the policy is working. It should also provide an assessment of the relative adherence to the policy by Nominet and UK law enforcement agencies.”***

28. The word “relative” should be removed; it is not a competition between Nominet and law enforcement agencies to see who adheres least badly. Save for that, I agree, and welcome this change.

***“Nominet should hold further discussions under the policy process to review the acceptability and handling of third party requests for suspension.”***

29. There is nothing wrong with dialogue, but an extension of the process to third parties would be unwelcome. The Issue Group should be clear on whether it is supporting such an extension, or merely suggesting it should not be included within this report. If the former, it is outside the Issue Group’s remit to recommend other policy areas to discuss, let alone give views on them. If the latter, all that is necessary is to say the matter is outside the scope of the Issue Group.

***“Nominet should communicate the outcome of its policy development to Government to inform its own deliberations in this field.”***

30. I agree.

### ***Summary***

31. In my original submission<sup>4</sup>, I mentioned four key reasons why Nominet should not suspend domain names allegedly associated with criminal activity. I reviewed how Nominet’s draft proposals stood up to these in my last submission<sup>5</sup>, and do so again below.

32. Firstly, that there are already more effective ways of dealing with this, such as going to registrars and use of the ‘investigation lock’. These principles still do not set out why existing mechanisms are inadequate; they now make explicit that the proposed procedure should be used as a last resort, but give no examples of when and why other routes would fail.

33. Secondly, collateral damage. The proposals appear not to address this point at all. As per my points 4 and 5, there is still no clarity as to the required linkage between registrant, alleged criminal and domain name.

---

<sup>4</sup> <http://blog.alex.org.uk/2010/11/26/domain-names-and-criminals/>

<sup>5</sup> <http://blog.alex.org.uk/2011/09/01/nominet-and-soca-a-romance-in-three-parts/>

34. Thirdly, civil liberties and due process. It is accepted that civil liberties need to be balanced against protection of the public from serious crime. The revised proposals in some areas (for instance in terms of due process, reporting mechanisms, appeal processes, and transparency) are a very substantial improvement over the previous draft. However, the Issue Group still seems unclear as to what crimes it seeks to protect the public from, and for the sake of which to sacrifice civil liberties. The policy on the one hand attempts to restrict the alleged crimes to those that create '*a clear risk of imminent serious harm to individuals*' (a restriction to be welcomed), but then finds it necessary to include those sales of counterfeit goods that do not fall within that limb, and goes on to suggest under point 6 that in fact any crime should apply.
35. Fourthly, mission creep. The proposals do not address this. Indeed, disappointingly, the mission creep has already started, with an issue group tasked to look at criminal activity already recommending to the board that it look at 'civil and third party' complaints too.

Alex Bligh  
17 October 2011