

# Domain names used in connection with criminal activity

## *Response to Draft Recommendations dated 10 November 2011*

This document is a response to the draft recommendation<sup>1</sup> by the Nominet Issue Group considering ‘domain names used in connection with criminal activity’ published on 11<sup>th</sup> November 2011.

I have already made a detailed submission<sup>2</sup> on what I believe the correct principles should be. I made a further submission<sup>3</sup> on September 2011 on the draft principles, and commented<sup>4</sup> on the revised draft recommendation of 17<sup>th</sup> October 2011; I 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.

As the document circulated by the issue group is very similar to the 17<sup>th</sup> October 2011, my reply is very similar. I have highlighted changes appropriately.

***“In line with the company’s public purpose mission to promote a safe and trusted internet space, and in order to protect 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/54345\\_Issue\\_group\\_draft\\_recommendations\\_101111.pdf](http://www.nominet.org.uk/digitalAssets/54345_Issue_group_draft_recommendations_101111.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/>

<sup>4</sup> Submitted through the Nominet process, but also to be found at: <http://blog.alex.org.uk/2011/10/17/nominet-soca-scores-again/>

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, the issue group strongly recommends that Nominet’s abuse policy 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 substitution of 'in association with [criminal activity]' by 'in connection with [criminal activity]' is to a welcome clarification. However, whilst point 12(e)(ii) in my view correctly limits this connection to domain names which are 'integral to the commissioning of the alleged crime' it would be preferably for this restriction to be echoed in the principles section, rather than the process (i.e. in the first sentence of point 7), else it is in theory possible to have a situation to which the policy applies (a domain used in connection with a crime but where it is not integral to its commissioning) which is only safeguarded by the fact that no acceptable notification can be given.
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@johnemployer.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 incorporate procedural fairness mechanisms 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 and users.”***

8. Agree. I welcome the introduction of ‘users’ into this point. To be fair it should also seek to recognise the interests of rights holders, 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 only to a limited subset of criminal activity in the first instance. The policy must explicitly exclude civil disputes and criminal cases where freedom of expression and other fundamental rights are central to the complaint, particularly where prosecution would require authorisation of the Director of Public Prosecutions or the Attorney General, such as cases involving obscenity or hate speech.”***

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 ... are central to the dispute at issue*’. The omission of qualification ‘*of third parties*’ is to be welcome, as is the clarify added by ‘*particularly where prosecution would require authorisation of the Director of Public Prosecutions or the Attorney General, such as cases involving obscenity or hate speech.*’
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 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 (this could be added to the last phrase of the last sentence).*
  - 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.*

**Deleted clause partly incorporated into recommendation 22: “[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 deletion of this clause (and the incorporation of some of its wording into point 22) is to be welcomed – see also my comment number 35.

**“The policy should apply as a principle of last resort where urgent suspension is necessary to reduce harm to individuals. “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.”**

14. The inclusion of ‘urgency’ as a criterion is to be welcomed.

**The scope of these recommendations relates to offences where suspension is deemed to be the most appropriate way in which to effectively minimise the harm caused by the alleged crime. An acceptable notification should meet the following criteria: (a) The nature of the alleged criminal activity creates a clear risk of “imminent serious harm” to an individual or individuals. “Imminent serious harm” is defined as urgent or on-going harm. This would include, but is not limited to, the following examples: phishing, fraud, the unlicensed sale of medicines or other regulated goods and services, and botnets; or, (b) The domain is directly involved in the criminal distribution of counterfeit goods.**

15. The restriction of the recommendations to situations where suspension is ‘the most appropriate way in which to effectively minimise the harm caused by the alleged crime’ is to be welcomed. This would, however, be an ideal place to explicitly set out that the potential of harm to innocent third parties (e.g. those innocently using the domain name in the *demon.co.uk* example given above) should be considered in weighing up the appropriateness of suspension.

16. The new definition of ‘imminent serious harm’ appears to make no sense, for two reasons: firstly, it is not the harm that is urgent, but its resolution, and secondly the definition omits ‘serious’. I suggest simply using the phrase ‘imminent or on-going serious harm’.

17. 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.
18. 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 notification of its alleged use in connection with criminal activity should only be undertaken following formal receipt of a notification authorised 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.”***

19. ***‘Formal receipt of a notification’ should presumably read ‘receipt of a formal notification’.***

***“Nominet should publish a list of law enforcement agencies with whom it has a trusted relationship. Notifications from private party or foreign law enforcement agencies should be specifically excluded from this policy.”***

20. 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.”***

21. 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 15(b), this framework could include training, agreements to make notifications under the policy subject to audit procedures, and frameworks to establish ‘Single Point of Contact’-type procedures, similar to those established under the Regulation of Investigatory Powers Act 2000.”***

22. I agree, and welcome this change.

23. 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?

***“An acceptable notification must: (a) Specify the alleged offence and indicate whether it is within the scope of 7a or 7b, or both; (b) Identify the requesting trusted law enforcement agency; (c) Comply with the procedure set out in the policy and any published materials such as templates by Nominet; (d) Include a declaration of the authorising senior officer on behalf of the agency that suspension of the domain is proportionate, necessary, and urgent, and that the agency is seeking suspension under the principle of last resort; (e) Include a certification that the authorised senior officer is satisfied that: (i) The evidence gathered to support the notification has been to a prosecutorial standard (i.e. a reasonable prospect of conviction); (ii) the domain name is integral to the commissioning of the alleged crime; (f) Where Nominet accepts that very urgent action needs to be taken, Nominet may accept verbal notification from a trusted law enforcement agency, provided written notification in compliance with the policy is provided within [12] hours.”***

24. The substantive change here is to add section (f). This is unwelcome, particularly as there is no way to verify a ‘verbal notification’, and no evidence of it. The information the law enforcement agency is asked to provide could be provided on a single side of A4, and could be sent to Nominet by facsimile or email if necessary, with originals to be supplied within 24 hours. Aside from the evidentiary problems of

acting on a verbal instruction, Nominet should protect its own private interests by requiring the notification to be in writing, if only in electronic form. It is hard to think of a situation where the 5 minutes to complete and sign a form would be that important.

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

25. I agree, and welcome this change.

*“In the cases of suspension notifications that fall exclusively within the scope of 7b, Nominet should notify the registrant prior to suspension, giving the registrant reasonable opportunity to object, and informing them of the procedures and timeframes by which they may do so”*

26. I agree, and cautiously welcome this change, though in my view (as set out above), 7(b) notifications should not be permitted in any case. However, the recommendations do not appear to cover the proposed procedures and time frames. Whether, for instance, the time limit is an hour, a day, a week, a month or a year makes a substantial difference. The fact of the matter is that a more appropriate remedy in a counterfeit case is the court system, as the facts are likely to be complex and the charge likely to be disputed. You have only to look at DRS cases to illustrate this point (e.g. the Seiko case).

*“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.”*

*“Nominet must provide for appeals mechanisms that enable registrants to swiftly challenge notifications or 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: (a) A transparent, independent, and fee-free appeals mechanism to enable a registrant who objects to the suspension to seek an assessment and decision on Nominet’s correct administration of the policy. The mechanism should provide swift and defined timeframes, and should be subject to a published review. Outcomes of appeals should be published. It may be helpful to look to Nominet’s existing Dispute Resolution Service as an example of good practice. (b) The policy should enable recourse directly to the law enforcement agency that has originated the request. It is recognised that registrants may wish to resolve the basis of a notification directly with the respective LEA. (i) Only LEAs that undertake to operate a system of redress to respond to the registrant complaints within a swift and defined timeframe should be accepted as having a trusted relationship under the policy. Where an LEA does not respond to a complaint within the defined timeframe, Nominet should reverse the suspension. (ii) Nominet should cooperate with law enforcement agencies to agree what level of detail of information should be provided to registrants to facilitate direct recourse, but it is suggested that at a minimum the law enforcement agency and contact details of the requesting officer of the notification should be provided. (c) Registrants must also have the option of recourse to the judicial*

*system. Registrants must be able to substantively challenge a suspension as part of a transparent and fair process. The policy should provide for a procedure where: On the provision of a review and assessment of a registrant statement by an independent expert, Nominet can require a court order from the respective law enforcement agency within a defined period of time in order to carry out or to continue a suspension. The independent expert should provide a deterministic opinion to Nominet, on the basis of a statement or other evidence provided by the registrant, as to the validity and seriousness of the registrant's objection. Registrants must provide a verifiable legal address for service in the UK to the independent expert in order to submit to this procedure."*

27. I welcome the clarifications in this clause.

28. Restricting the address for service to the UK precludes nearly every bona-fide non-UK based registrant from using this policy. This would appear to be seriously unfair to (for instance) a registrant in France, and rather out of tune with an electronic age. Similarly, the requirement for 'a verifiable legal address for service' is a little peculiar: either it is an address for service, or it is not. I suggest requiring that the registrant provides an email address and a physical address for service, and if that address is outside the UK, including a presumption that any notice has been served if a message is sent to the email address provided.

*"The policy should define under what circumstances the suspension of the domain might be reversed following remedy by the registrant. At the very minimum, this must provide for defined timescales by which Nominet will reverse suspensions."*

29. 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; (e) The outcome of any related appeal"*

30. I agree, and welcome this change. I suggest Nominet should also publish whether an appeal has been lodged.

*"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."*

31. I agree, and welcome this change.

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

32. I agree, and welcome this change.

*"If the Board accepts these principles recommendations and the policy becomes operational, the Nominet Board should establish an independent review to report on how the policy and its operational bodies including the appeals mechanisms are working. It should also provide an assessment of the adherence to the policy by Nominet and UK public law enforcement agencies."*

33. The removal of the word 'relative' before 'adherence' is to be welcomed.

34. The first phrase of the first sentence has an orthographical error: either “principles” or “recommendations” but not both.

***“Any broadening of the scope of the policy to address a wider set of criminal activities or the acceptability of handling of third-party requests for suspension must be examined under the .uk Policy Process after an assessment and review of the policy’s implementation.”***

35. I agree, and welcome this change.

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

36. I agree.

### **Summary**

37. In my original submission<sup>5</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>6</sup>, and do so again below.
38. 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.
39. Secondly, collateral damage. The proposals appear not to address this point at all. As per my points 4 and 5, there is still little clarity as to the required linkage between registrant, alleged criminal and domain name.
40. 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. **The removal of the old point 6, suggesting in fact that any crime should apply is an improvement.**
41. Fourthly, mission creep. **Whilst this remains a concern, the proposals now do not specifically endorse recommending to the board that it look at ‘civil and third party’ complaints too, which is an improvement.**

Alex Bligh  
13 November 2011

---

<sup>5</sup> <http://blog.alex.org.uk/2010/11/26/domain-names-and-criminals/>

<sup>6</sup> <http://blog.alex.org.uk/2011/09/01/nominet-and-soca-a-romance-in-three-parts/>