

Domain names used in connection with criminal activity

Response to Draft Recommendations

This document is a response to the draft recommendation¹ by the Nominet Issue Group considering ‘domain names used in connection with criminal activity’.

As I have already made a detailed submission² on what I believe the correct principles should be, I will try to avoid repetition and concentrate on the draft principles as proposed. I have briefly stated to what degree the proposals address my four main criticisms in a summary section.

“Nominet should have an abuse policy that specifically addresses criminal activity in its terms and conditions.”

1. I see nowhere in the agreed recommendations any explanation as to *why* Nominet should have such a policy; this is the central issue. Apart from a hand-waving comment about Nominet’s public purpose, there is no coherent statement of why Nominet should suspend domain names a law enforcement activity considers criminal. Telecoms operators do not suspend the telephones of alleged criminals without a warrant. Ambulance drivers do not refuse to carry patients alleged to be criminals, nor do medics refuse to treat them. Newspapers do not refuse to print articles the police allege would be criminal to publish without a court order. Why should Nominet be any different? In fact, is there any ‘public purpose’ organisation that does provide a service, but withdraws it on the request of the police?
2. More particularly, what is different about ‘criminal’ activity (or a subset of criminal activity) from any other behaviour that either Nominet, or any other stakeholder alleges has (a) happened, and (b) is unpalatable to some? If there criminal activity is to be treated differently from civil harm for instance, there should be a justification for it, particularly given some ‘criminal harm’ is far less damaging than some ‘civil harm’.
3. It would appear that the response is not in fact seeking to address ‘criminal activity’ (which no one doubts should be acted upon) but ‘alleged criminal activity’. It seems to me there is a high hurdle to jump to avoid the presumption of innocence until proven guilty; I realise that the group is attempting to navigate this hurdle through the definition of harm below, but I am unconvinced that this is an adequate safeguard. Neither Nominet nor the police is a court, and neither should attempt to act as if they are.

“Nominet should be able to act under an expedited process to suspend domain names associated with serious crime when requested by a law enforcement agency.”

4. This leaves open the questions of (a) which law enforcement agencies can validly make such a request, and (b) what processes are followed. Whilst it is understood that

¹ See <http://www.nominet.org.uk/news/latest/?contentId=8617>

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

this is a proposal of principles (as opposed to implementation details), such a principle's acceptability depends substantially on these 'details'.

5. Assuming such a process existed (which I believe it should not), I would suggest as a matter of principle, Nominet should restrict itself to requests from UK law enforcement agencies, as Nominet operates within the UK's jurisdiction. Accepting requests from other jurisdictions is likely to result in Nominet making value judgments as to whether a police force from a foreign jurisdiction should be trusted; should we trust a request from France? From the USA? From Syria? From North Korea? My understanding is that there are already protocols for cooperation between the police forces for various countries, especially within the EU; these should be used for requests from outside the jurisdiction. As far as the question as to which law enforcement bodies, I see no immediate need to extend this beyond the UK's police services.
6. Again assuming such a process existed, I would suggest as a matter of principle, Nominet should restrict itself to requests which a senior officer of the law enforcement agency concerned has certified as complying, to the best of his or her belief, with Nominet's policy. As a registrant whose domain name is suspended incorrectly is unlikely to have any comeback against the law enforcement agency concerned, and no doubt Nominet will also wish to limit its own potential liability, it is important that there are appropriate checks and balances. One such check would be ensuring that a senior officer is satisfied with the seriousness of the case; this is a safeguard used frequently within the PACE³ and associated codes. Another such check would be review of such suspensions after the event – without such certification it would be difficult in hindsight for Nominet to ascertain whether such powers were being misused. Putting this point the other way, it is difficult to see why Nominet should suspend a domain name in the circumstance where no senior officer is prepared to certify that, to the best of his or her belief, the suspension would comply with Nominet's policy.

“An expedited procedure to suspend domain names should only be available where a) it is the last resort in dealing with the domain name, following requests with registrar, ISPs etc in the first instance or b) it is the most viable option to prevent imminent or ongoing serious consumer harm.”

7. It is difficult to see why limb (a) of this test is needed, particularly given the test is expressed disjunctively. If there is no imminent or ongoing serious harm (the term 'consumer' is dealt with below), then what is the necessity for suspension? This implies a law enforcement agency should be able to suspend a domain name where no serious harm is occurring, solely because the registrar or registrant does not wish to cooperate with the police. This is totally inimical. A court is the appropriate venue to decide this issue. If no serious harm is occurring, there is no need for Nominet to get involved.
8. Perhaps the intention here is the test should be conjunctive, i.e. that *both* limbs should apply. I would support this modification. It seems peculiar that Nominet should be asked to act where other action is likely to be more effective.
9. As far as limb (b) is concerned, the words 'consumer harm' here are a very strange choice, in that they are at once too broad and too narrow. A terrorist threat to an oil rig, for instance, is not 'consumer harm', though it might well involve death, bodily harm, and serious economic harm. Burglary of a business is not 'consumer harm'.

³ Police and Criminal Evidence Act 1984

Serious fraud on businesses are in general not ‘consumer harm’. Producing substandard (but not criminally so) or even overpriced goods might be considered serious consumer harm; surely one threshold should be that the behaviour complained of should be criminal? The section marked ‘summary of discussion’ mentions counterfeiting as an example of a serious crime; whilst it may be serious in some instances, and whilst it is accepted that some counterfeit goods are dangerous, in general counterfeiting does not cause harm primarily to the consumer, but rather causes economic harm to the manufacturer whose goods are counterfeited. Selling fake Rolex watches does not, in general, cause consumer harm, particularly if the consumer is aware they are fake. Selling genuine but unauthorised goods (for instance grey imports) in general do the consumer no harm at all, but cause businesses substantial damage⁴. If the intent is to address such economic crimes, the language used should be appropriate.

10. It is in any case difficult to see why ‘harm’ should be evaluated in terms of whether it is related to purchases of goods by the general public. I would suggest rather that the policy should restrict itself to (i) serious or continuing harm to third parties (including legal persons) which is (ii) caused by the alleged commission of a criminal offence at or beyond a particular threshold of severity, and (iii) where such harm would be substantially reduced by the suspension of the domain name. The threshold severity might, for instance, be an offence that could only be tried in a Crown Court (as opposed to a Magistrate’s court).
11. Most seriously, 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. 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 should exclude suspension where issues of freedom of expression are central aspects of the disputed issue.”

12. This is a good principle, but 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?
13. I would suggest an explicit carve-out for criminal libel.

⁴ If this argument is thought fanciful, see the number of Nominet DRS cases involving Seiko watches.

14. 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.

“Nominet should consider establishing a registrant appeal mechanism.”

15. I support this. However, what redress would a registrant have if his domain name was suspended for many months whilst such an appeal took place? And against whom?
16. The proposals do not address whether prior notice is to be given to the registrant. I suggest prior notice is given where possible, though for operational reasons I accept this may not always be possible or desirable. However, it would help avoid collateral damage.
17. It is likely that in some cases, Nominet may, either in response to suspension, or in response to such notice, receive immediate protestations of innocence from the party concerned, and (quite possibly) threats from his or her solicitors. Quite apart from a lengthy appeal procedure, Nominet should consider what it might do in the event it makes a mistake⁵. It would be desirable for Nominet to be able to reinstate any such site quickly.

“When the policy is operational, Nominet should set up an independent panel to review how the policy is working.”

18. I support this. However, in order to ascertain the effectiveness of the policy, it would be necessary (i) for any suspension request to come with data as to why the suspension is being requested, and (ii) for the panel to be able to follow up to determine whether the suspension had the desired effect, and whether a criminal activity was in fact taking place. I foresee a danger that law enforcement might request a large number of sites to be suspended, but only be able to provide any data about a small number of them at a later date; this would, of course, suggest the process was being abused.

“Nominet should exclude civil or third party requests from this policy (which is focused on criminality), but these merit further discussion under the policy process.”

19. I do not believe the question of whether civil or third-party requests merit further discussion comes within the ambit of this issue group’s activity. This should not have formed part of the issue group’s recommendations.

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

20. I support this, whatever the outcome.

Summary

21. In my original submission⁶, I mentioned four key reasons why Nominet should not suspend domain names allegedly associated with criminal activity.

⁵ See, for instance <http://www.affiliates4u.com/forums/affiliate-marketing-lounge/134862-affiliate-sites-law.html>

⁶ <http://blog.alex.org.uk/2010/11/26/domain-names-and-criminals/>

22. 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 do not set out why existing mechanisms are inadequate. There is some attempt at limiting the ambit of the proposals to situations where other routes have been exhausted, but bizarrely this is only proposed (per my point 8 above) where *no* serious harm is being caused (i.e. it is only relevant where limb (b) does not apply).
23. Secondly, collateral damage. The proposals appear not to address this point at all. As per my point 10, there is no proposed linkage between registrant, alleged criminal and domain name.
24. Thirdly, civil liberties and due process. It is accepted that civil liberties need to be balanced against protection of the public from serious crime. Some attempt has been made to address this balance. However, protection 'of the public' from counterfeit Ugg Boots (for instance) does not seem to me a particularly significant altar on which to sacrifice civil liberties. The policy should concentrate on crimes more serious than these. The proposals for review and appeal are to be welcomed.
25. 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
1 September 2011