Response to 2019 Nominet consultation

Contents

1. INTRODUCTION

1.1. Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

1.2. ORG has actively engaged with government and other proposals for online regulation since the Internet Safety Strategy in 2017. The following comments have been developed through a long period of reflection, report writing and engagement with different stakeholder groups. Our main reports underpinning this response are:

1.2.1. Internet Regulation, Parts I[1] and II[2]

1.2.2. Blocked: Collateral Damage in the War against Online Harms[3]

1.2.3. DNS Security: Getting It Right[4]

1.2.4. Response to Consultation on the Online Harms White Paper[5]

1.3. We refer the consultation team to our paper on Internet Regulation, Part I in particular, which set out our views on Nominet's domain suspension programme.

1.4. We welcome this opportunity to respond to Nominet's consultation. Our narrative response opts not to address specific questions but rather deals with issues and concerns more holistically. References to parts of the consultation are included in square brackets [x].

1.5. NGOs including ORG have signed onto the Manila Principles for content moderation. These are the nearest analogous set of human rights principles that could be applied to Nominet's domain suspension programme. These state:

1. Intermediaries should be shielded from liability for third-party content
2. Content must not be required to be restricted without an order by a judicial authority
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality
5. Laws and content restriction policies and practices must respect due process
6. Transparency and accountability must be built into laws and content restriction policies and practices

---

[1] Open Rights Group, *UK Internet Regulation Part 1*, December 2018 <https://www.openrightsgroup.org/assets/files/pdfs/reports/Internet_Regulation_Part_I_Internet_Censorship_in_the_UK_today-web.pdf>

[2] Open Rights Group, *UK Internet Regulation Part 2*, June 2019 <https://www.openrightsgroup.org/assets/files/pdfs/reports/ORG_Regulation_Report_II.pdf>

[3] Open Rights Group, *Collateral Damage in the War against Online Harms*, April 2019 <https://www.openrightsgroup.org/assets/files/reports/report_pdfs/top10vpn-and-org-report-collateral-damage-in-the-war-against-online-harms.pdf>

[4] Open Rights Group, *DNS Security: Getting It Right*, June 2019 <https://www.openrightsgroup.org/assets/files/reports/report_pdfs/ORG_DNS_Security_Report_.pdf>

[5] Open Rights Group,*Response to Consultation on the Online Harms White Paper* July 2019 https://www.openrightsgroup.org/about/reports/response-to-consultation-on-the-online-harms-white-paper-july-2019

2. KEY CONCERNS

2.1. Domain suspension is a significant punitive action to take. Suspension may destroy a business or at the very least inflict great damage to it. Suspension can also silence marginal/minority voices and have fundamental rights implications. Decisions to suspend must therefore be rational and procedural safeguards are essential to ensure accountability and fairness.

2.2. As the infringements involved are mostly civil matters - infringement of IP rights - this could prove very concerning should domains be targeted for suspension wrongly.

2.3. In many countries, including the USA, such a suspension typically follows a court order, meaning that there are legal safeguards against error and abuse. However, in the UK, suspensions are made purely on law enforcement request, with volumes running at around 30,000 a year. On the face of it, there is significant possibility of error. Our research showed that law enforcement agencies often lack public documentation, codified policies for suspension requests and formal oversight of their domain suspension work. This risks unaccountable, inconsistent and unjustified decision-making.

2.4. When we asked law enforcement agencies for policy documents in 2018, many agencies were unwilling or unable to provide them. Some stated they did not have policies governing domain suspension requests.

2.5. In particular, the Financial Conduct Authority refused to supply a policy, as did the Medicines and Healthcare Products Regulatory Agency, as did the Counter Terrorism Internet Referral Unit, which gave a 'neither confirm nor deny' response. The Fraud and Linked Crime Online (FALCON) (Metropolitan Police) and the National Fraud Intelligence Bureau (City of London Police) did not have a policy. The National Crime Agency and National Trading Standards are not subject to FoI and did not respond to our request for a policy. Only two agencies - DEFRA Veterinary Medicines Directorate and Police Intellectual Property Crime Unit (City of London Police) supplied any kind of policy document.[6]

2.6. Once suspension pages exist, this position will be far less tenable, as some public explanation of what has taken place will need to be available from the requesting agencies.

2.7. The .UK domain suspension process also lacks reasonably accessible appeal and review opportunities. While theoretically a decision to request a suspension might be challenged via judicial review, this seems a very onerous process for correcting mistakes. We understand that internal reviews are sometimes requested following errors. However, to be fully confident of a reasonable decision, a domain owner should be able to access an independent appeal. Speed is also a valid consideration for the fairness of appeal processes.

2.8. In our report, we made the following recommendations to Nominet:

1. Adopt Freedom of Information principles

[6] See https://wiki.openrightsgroup.org/wiki/Nominet/Domain_suspension_statistics for links to FOIs showing which agencies had policies or not, or refused to supply details of them.

2. Ask the government for a legal framework for domain seizure based on court injunctions for domain seizures
3. Require notices to be placed after seizures to explain the legal basis and outline any potential dangers to consumers posed by previous sales made via the domain. This could include contact details for anyone wishing to understand any risks to which they may have been exposed
4. Short term: Offer an independent review panel
5. Short term: Require government organisations to publish their policies relating to domain suspension requests
6. Short term: Publish the list of suspended domains, including the agency that made the request and the laws cited
7. Short term: Require government organisations to take legal responsibility for domain suspension requests

This consultation is about the third of those recommendations, creating a requirement for notices to be placed at a landing page for visitors attempting to access the 'suspended' or seized domain.

2.9. In opening a discussion about notification pages, a number of other questions quickly emerge. In particular, as transparency over the process is created, users will want answers to questions such as:

- Why has the domain been suspended?
- Who decided that it should be suspended?
- What should a visitor or owner do if a mistake has been made?

2.10. These questions will need answering. Thus Nominet should be ready to ensure that:

- It has documents that explain the domain suspension process;
- The agency that requested a suspension has a public facing document explaining when they make requests and any independent oversight of their work that might give the public confidence that suspensions are legitimate;
- There is an independent appeals process available to owners, as well as the existing process for an internal review by agencies.

These should be available from the suspension page, as links back to pages on Nominet's own site or the agency as appropriate.

2.11. There is a linked question of liability for the suspension. It is unclear to us that there is a settled view as to whether Nominet or the law enforcement agencies are liable for the suspension. It is important to explain who takes responsibility for it. In our view, the agencies should be regarded as taking legal responsibility, as they made the investigation and asked for the suspension.

2.12. Users will also want information about their own personal risks, should they have purchased dangerous drugs, or goods which may lack safety testing or consumer guarantees. Suspension pages should be used to direct users to information that can help users understand any risks. In some cases, such as the sale of unlicensed drugs, there may be need for more specific advice. Nominet

should facilitate customisation down to individual domains where this may reduce specific risks.

2.13. As domain suspensions are being triggered by law enforcement and have legal effect on owners, notices should be reasonably neutral in tone, attempt to inform rather than scare, and should not be used as marketing or promotional tools, even for public safety purposes.

3. LONG TERM NEEDS

3.1. As noted in our report, we believe that government should create an authorisation process for requests, which are often made in bulk. This need not be slow or onerous, but would provide independence and rationality in decision making.

3.2. Nominet should explore the possibilities for formalising such a process with DCMS. This may require legislation. Such an approach could also positively increase the public accountability of suspensions.

3.3. Nominet are operating as a publicly accountable body when they operate this suspension regime and should be regarded as subject to the Human Rights Act because they are implementing a policy with widespread impacts on rights including speech and the right to run a business. This position is accepted by the IWF in their analogous takedown work, for instance. Nominet also operate as .uk registry subject to DCMS' wish that they continue to do so. For these reasons, Nominet should apply high standards of transparency including responding to information requests as if they were subject to Freedom of Information requirements, and be prepared to share internal documents if asked.

3.4. Nominet should also give thought as to the economics of the criminal purchase of domains. In particular, it should consider whether front loading costs would reduce the purchase of domains for criminal use. For instance, a domain could be bought for a minimum number of years to increase the initial purchase price without adding to the costs of a legitimate customer.

3.5. While it may prove difficult to adjust the .uk market in this way, we believe that it would be useful to at least discuss it, as it seems that it is the low cost of initial purchase is encouraging the large scale purchase of .uk domains for criminal use. DCMS and Nominet should note that law enforcement agencies are bearing the cost of cleaning up a problem which arguably could be reduced by simple changes to pricing structures. At the very least, we should have a clear answer as to why it is not possible to take action in this way.