International Regulation and Trade team
Department for Science, Innovation and Technology
5th Floor
100 Parliament Street
London
SW1A 2BQ

31st August 2023

Response of the DNS Research Federation to the consultation on proposed UK-Related Domain Name Powers

The DNS Research Federation thanks the UK Department for Science, Innovation and Technology (DSIT) for the opportunity to submit comments on DSIT's consultation, Digital Economy Act 2010: Powers in Relation to UK-related Domain Name registries

Introductory comments:

This response focuses on DSIT's proposed updates to sections 19-21 of the DEA 2010, which give the Secretary of State powers of intervention in relation to certain internet domain name registries.

To ensure that current procedures remain in place to deal with both misuse and unfair uses of domain names, the current consultation encourages proposals for the design of regulations in relation to UK-related domain name registries.

The proposals list practices that are considered to be 'misuse' and 'unfair use' of an internet domain name. The draft regulations also contain requirements for registries to have arrangements for handling complaints in connection with the domain names in scope.

Before addressing the questions set out by DSIT, the DNS Research Federation makes the following overarching comments:

There is a lack of agreed definitions and ways of measuring DNS Abuse. The DEA Act has defined 'misuse' to reflect the approach adopted by ICANN. This is in line with DSIT's stated objective of ensuring that these powers 'do not interfere with ICANN's responsibility for the policies in gTLDs… nor the registry agreements that ICANN has with each of the gTLD registries.' However, it should be noted that there is a lack of standardised definitions that are acceptable to all interest groups, such as cybersecurity, public safety and brand communities. A broader definition of domain name abuse was adopted in the 2022 report for the European Commission, ie, that DNS abuse is 'any activity that makes use of domain names or the DNS protocols to carry out harmful or illegal activity'.

Rather than picking sides in these polarised debates, a recent blog by the DNS Research Federation highlights the consequences of choosing one definition, or measurement methodology over another. In short, the definitions and methods of measuring domain misuse or unfair use will lead to different coverage for the proposed measures.

Domain names play an important role in the 'lure' that persuades people to click on malicious links. Outcomes of consumer focus groups conducted for the DNS Research Federation (forthcoming) found that people of all age groups, social and educational backgrounds have fallen victim to scams and online fraud. In link-based scams and fraud, the focus group responses indicate that victims do assess the apparent legitimacy and credibility of the domain name that forms the link, as part of their selective scrutiny in the split-second decision whether or not to click on a link. Further, all focus group participants reported that scams and online fraud had a strong to very strong emotional impact on them, shaking their confidence, and adversely impacting their trust in the online environment at least temporarily.

In recent research, the DNS Research Federation has maintained a focus on the impact of scams and other domain name-related cybercrime on Internet users. While definitions and measurement approaches favoured by the DNS industry (adopted in the proposals) tend to narrow the scope of what is covered, and can suggest a downward trend in abuse, consumer research conducted by the DNS Research Federation indicates that 92% of Internet users in the UK, Germany and France report having received scams, and 57% believe that the volume is increasing. The growing rate of online scams is supported by data from Europol's IOCTA report 2023 and the UK's Office for National Statistics. While not all responsibility for addressing domain name misuse falls to the DNS community, the scale of the impact on consumers requires each stakeholder to play their part in reducing harms.

The UK should consider the extra-territorial effects of NIS2 and impact of accurate registration data. It is surprising to see no mention of WHOIS in the current UK proposals. Since the coming into force of the EU General Data Protection Regulation, there has been a reduction in the public availability of personal data from the WHOIS. This has adversely impacted stakeholders who need rapid access to that data for the prevention and detection of crime, and to combat public safety and cybersecurity threats. The European Union's Directive on the Security of Network Information Systems (NIS2) provides a legislative basis for registries and registrars to collect and **maintain accurate registration data and to put in place verification procedures that reflect best practices in the industry.**

NIS2 has extraterritorial effect - so the UK domain name industry will need to be in compliance with NIS2 if they offer services within the EU. To reduce compliance costs for the UK DNS industry, and to avoid complexity and fragmentation risks through inconsistent national approaches, **UK legislation should maintain consistency with the NIS2 Directive's approach** where there is overlap.

We encourage the continued adoption of best practices. Our report, 'Habits of Excellence: why are European ccTLD abuse rates so low?', shows that the EU ccTLDs have low levels of domain names associated with spam, phishing and malware. The study concludes that a combination of measures - such as automated data syntax validation and ad hoc measures - may explain the EU ccTLDs strong performance as a group. The study also notes that good practice is not confined to the EU and that the **.uk comes third in the world - outperforming all of its EU counterparts in abuse mitigation**.

Importance of data sharing for evidence-based policy making. The DNS Research Federation strongly believes in the importance of data sharing to ensure effective, evidence-based policy research. **The facilitation of data sharing and access to data is crucial for mitigating domain misuse or unfair use.** With different methodologies for defining and measuring domain abuse, it is vital that there is **transparency around registry good practices** and the removal of real and perceived legal barriers to the sharing of non-personal data relating to mitigation of domain name misuse.

The UK proposals need to be future proof, and close current and evolving governance gaps. Our recent article, 'Use of Subdomain Providers Gains Popularity as a Mechanism to Launch Phishing Attacks.' highlights the growing use of subdomains (outside the sphere of control for domain registries) in scams, and of IP addresses in the distribution of malware. Careful consideration should be given to who is responsible for enacting enforcement and understanding the role of different actors.

Currently, the proposal does not define 'Domain Name,' and with the evolution of technology there has been an increase in the registrations of **alt-root domain names**. A recent paper from the DNS Research Federation on Web3 disruption and the domain name system examines this trend, considers potential abuses and highlights governance gaps. Therefore, the scope of definitions should be carefully considered to future proof evolving areas of domain abuse.

In summary the definitions of domain name misuse / abuse are contested, and multiple other stakeholder groups believe the definitions should be drawn more broadly. Regulation in a rapidly evolving environment needs to be sufficiently flexible to avoid becoming outdated. Whatever approach is taken by the UK, policy makers need to be mindful to close governance gaps, such as hosting, subdomains and the emergence of new technologies and alternative namespaces which would fall out of scope of these regulations. UK policy makers should mirror relevant provisions in NIS2 to fulfil the stated legislative aim of conforming with international best practice. It is essential to ensure that data is made available to researchers and policy makers, and to learn from effective good practices.

Answers to the consultation questions:

1. **Do you agree we should include *all* the types of misuses of domain names set out under the 'Domain Name Misuse' heading, in our 'prescribed practices'? If not, which ones should be omitted and why?**

As discussed in our introductory comments, it is important to recognise that there are many different approaches to the definition and measurement of domain name abuse that reflect the interests of different stakeholders. The debates have become polarised. Therefore, the UK should be mindful of those debates and differing interests when adopting the definitions contained within the updated DEA. The legislation should avoid creating governance gaps by adopting overly narrow definitions without balancing requirements for other suppliers within the value chain such as sub-domain providers, hosting and proxy providers.

2. **Are the descriptions of the types of domain name misuses set out under the 'Domain Name Misuse' heading fair and appropriate for the purposes of including them in our 'prescribed practices'? If not, please explain why not and propose alternative descriptions.**

Please see our response to question 1 on the definitions, and note that the UK adopts definitions consistent with ICANN's approach.

Are there any other types of domain misuse that should be included in the 'prescribed practices'? If so, please describe them and provide reasons as to why you think they should be included.

If the UK chooses to define the relevant terms, the resulting legislation needs to be robust enough to address evolving or future domain abuse. The scope of what should be prescribed should consider the potential and emerging trends due to emerging technologies. Criminals are continually looking to exploit domains using emerging technologies. Thought should be given to whether the definition is adequately future-proof.

3. **Do you agree with the proposal to include 'cybersquatting' (including 'typosquatting') in the list of unfair uses of domain names in our 'prescribed practices'? If not, why?**

Domain name dispute resolution mechanisms such as the UDRP and UK DRS have been in place for nearly 25 years. Both UDRP and DRS acknowledge the sometimes fuzzy boundaries between domain name registration and content, for example by considering how a domain name is being used.

The inclusion of 'typosquatting' in the UK proposals is in line with both UDRP and DRS, which require a complainant to demonstrate that the domain name is 'identical or [confusingly] similar' to the complainant's trademarks.

The DNS Research research on the Impact of Cyber Scams in 2022 show that there is a link between 'typosquatting' and online scams with 92% of our respondents in our research ever having received an online scam in an email or text message with a link including a brand email. Results from consumer focus groups conducted on behalf of the DNS Research Federation (forthcoming) highlight the role that the domain name plays in the 'lure' persuading victims to click on fraudulent links. When people see a link that has a domain name similar to the brand or function they were expecting, it helps to persuade them to click on the link.

4. **Is the description of 'cybersquatting' fair and appropriate for the purposes of including it in our prescribed practices'? If not, please explain why not and propose an alternative description.**

See above

5. **Are there any other examples of unfair use of domain names that should be included in the 'prescribed practices'? If so, please describe them and provide reasons as to why you think they should be included.**

See above

6. **What would you consider to be too burdensome in the content of resolving disputes under our prescribed dispute resolution procedure?**

No answer

7. **What does 'expeditiously' mean to you in the context of resolving disputes under our prescribed dispute resolution procedure?**

No answer

8. **What do you consider to be 'low cost' in the context of resolving disputes under our prescribed dispute procedure?**

No answer

9. **What would you consider a 'fair' and 'equitable' dispute resolution design to be?**

No answer

10. **Do you have any further comments on best practice or about the overall design of our dispute resolution procedure?**

No answer

11. **To what extent do you agree or disagree with our assessment under the 'Summary of Business Impact' section? Please provide details for your answer**

No answer

12. **Are there potential positive impacts (including costs or financial implications) that the proposals outlined in this consultation may have on business, consumers or the public sector? Please provide any evidence or comments on what you think these positive impacts would be.**

No answer

13. **Are there potential negative impacts (including costs or financial implications) that the proposed outlined in this consultation may have on business, consumers or the public sector? Please provide any evidence or comments on what you think these negative impacts would be.**

No answer

14. **Please provide any other comments or evidence that relates to or is about the analysis under the 'Summary of Business Impact' section.**

No answer

15. **Do you have any comments about the potential positive and/or negative impacts that the options on the broad purposes of the commencement of the DEA 2010 powers outlined in this consultation may have on individuals with a protected characteristic under the Equality Act 2010? If so, please explain what you think these impacts (both positive and/negative) would be.**

No answer

16. **If you believe there may be negative impacts, what do you think could be done to mitigate them?**

No answer

About the DNS Research Federation
Based in Oxford, The DNS Research Federation is a not-for-profit organisation that sits at the intersection of policy and technology. With a mission to advance the understanding of the Domain Name System's impact on cybersecurity, policy and technical standards, the Federation funds research globally, engages in technical standards, and brings technical tools and objective data relating to the Internet's unique identifier systems - especially the DNS - to researchers, public safety and industry stakeholders.