Department for Science, Innovation & Technology

Powers in Relation to UK-related Domain Name Registries

Government policy response to consultation

February 2024

Contents

Contact details

This document sets out the government's policy response to the public consultation 'Powers in Relation to UK-Related Domain Name Registries'. This follows the summary of responses that was published on 21 November 2023.

Enquiries on the government's policy response can be sent to:

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

Email: ukdomainnames.consultation@dsit.gov.uk

Consultation reference: Powers in Relation to UK-Related Domain Name Registries

Executive summary

On 20 July 2023, the Department for Science, Innovation and Technology (DSIT) published a consultation titled 'Powers in Relation to UK-related Domain Name Registries'. This consultation asked for views on DSIT's proposals for regulations which are to be made following sections 19-21 of the Digital Economy Act 2010 (DEA 2010) coming into force.

These sections set out the Secretary of State's powers of intervention in relation to internet domain name registries and abuse of domain names. Specifically, the consultation asked for views from respondents on the prescribed practices and requirements that the registries in scope of the powers should adhere to. These included a draft list of misuses and unfair uses of domain names in scope and proposed principles which will underpin the prescribed dispute resolution procedure. The full list of the questions asked can be found on pp. 19-20 of this document. On 21 November 2023, DSIT published a summary of responses to the consultation. Following the summary of responses, we are now setting out our policy response to the feedback we received.

The majority of responses to the consultation agreed with the proposed list of misuses and unfair uses. Our proposed approach therefore remains broadly the same as detailed in the consultation document, with some minor clarifications as a result of useful feedback.

We considered a number of additional proposed misuses. These included domains created or used for the sale of illicit or counterfeit pharmaceuticals or domains created to make available content or goods that infringe intellectual property rights. Our assessment, which has been set out in more detail in the response below, is that our regulations would not be the most effective mechanism for addressing these. There are a number of existing policies and regulations in place which we have pointed to in our response. We acknowledge the concerns raised through this consultation and DSIT will keep under review the effectiveness of the policy and the regulatory landscape.

Feedback also demonstrated that it was not always clear what constituted a misuse versus an unfair use. For the purposes of these regulations, our assessment is that misuses of domain names are types of harmful activity which are generally considered to be illegal. Therefore, registries should have in place adequate policies and procedures to mitigate against domain names being registered and deal with instances when they have been notified that domain names are being used, with the purpose of carrying out such misuses. Unfair uses are not necessarily illegal but can still result in harm to end users and therefore the registries are only expected to have in place an adequate dispute resolution procedure to deal with such unfair uses.

We also acknowledge the feedback that our proposed dispute procedure should not conflict with the existing dispute procedures that registries in scope of the regulations are bound by and the need to ensure that the policy does not result in increased costs for the registries nor those purchasing domain names.

It should be noted that we received some feedback which was out of the scope of what can be done in our regulations, for example regarding the formerly publicly available data of

registrants (WHOIS). We have ensured this feedback has gone to the relevant government departments.

We also received interest on the scope of UK-related domains, and what might be considered in scope in the future. The DEA 2010 deems a domain to be "UK-related" if, "in the opinion of the Secretary of State, the last element of its name is likely to cause users of the internet, or a class of such users, to believe that the domain and its sub-domains are connected with the United Kingdom or a part of the United Kingdom". Future UK-related domains would be automatically covered. We therefore determine the existing domains .uk, .scot, .wales/.cymru and .london to fall into scope. Internet registries who are proposing the creation of new domains in the future should consider if they will be in scope of the regulations.

Government policy response outlined per question

Questions on domain name misuse

The first three questions in the consultation related to the proposed list of misuses, their definitions and whether any additional types of domain name misuses should be included. These questions were:

- Do you agree we should include all of 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?
- 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.
- Are there any other types of domain name 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.

Overall, the consultation responses demonstrated broad agreement with the proposed list and associated definitions of domain name misuses, as identified by the Internet Corporation for Assigned Names and Numbers (ICANN)[1]. As a result of the feedback received, we have proposed some changes and additions detailed below, which we have developed through consultation with technical and industry experts.

Policy response

Six respondents proposed aligning the list of misuses and associated definitions more closely to established norms, including the Budapest Convention. The Budapest Convention is a legally binding treaty established in 2001 through the Council of Europe as a framework to facilitate increased international cooperation to protect against cybercrime[2]. The UK ratified the Convention in 2011 and supports international cooperation on tackling cybercrime.
We considered the Convention in the context of the proposed regulations and found that, given the Convention's broad scope for tackling a range of cybercrimes on the internet and computer networks, it would not be directly pertinent for the specific purpose of these regulations.

We also do not think that the definition of child sexual abuse material (CSAM) in the Convention is the most appropriate for our regulations. However, we are planning an amendment to our consultation definition to ensure the use of the most appropriate terminology and definitions. We assess that the most appropriate definitions of CSAM and indecent images

[1] https://www.icann.org/dns-security-threat
[2] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

of children (IIOC) are found within the Protection of Children Act 1978 and Prohibited Images of Children Crown Prosecution Service Guidance.

Two respondents suggested that we should expand our malware definition, in line with ICANN's Security and Stability Advisory Committee report, SAC115[3] so that it refers to installing 'and/or executing' malicious software. We agree that this is a useful clarification and will therefore look to update this definition accordingly.

Three respondents proposed that the definition of 'spam' be widened to cover spam as an abuse category of its own, as well as when it is used as a vehicle for the misuses as listed in the consultation. For example, using the definition of 'bulk unsolicited email'.

We consider there to be existing regulatory frameworks and policies in place to protect against spam of this type. For example, the Consumer Protection from Unfair Trading Regulations (2008) list 31 commercial practices which are considered unfair in all circumstances and are prohibited. This includes the commercial practice of 'Making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media except in circumstances and to the extent justified to enforce a contractual obligation.'

The Privacy and Electronic Communications Regulations (PECR) 2003 also restricts unsolicited marketing by electronic means including by email. The Information Commissioner's Office (ICO), the UK's independent regulator for data protection and privacy, takes enforcement action against unlawful direct marketing communications from identifiable UK senders. From previous assessments, the ICO has identified that approximately 15% of nuisance communications can be generated from outside the UK. Although the ICO cannot directly enforce against this as PECR is restricted to the UK in its territorial extent, the ICO has agreements in place with several overseas bodies to cooperate and exchange information.

12 respondents called for the inclusion of specific examples of malicious activity. We believe these to be sufficiently provided for through the existing list of misuses as they make it easier to distribute or facilitate malware, which is included in the current list. We have set out additional clarity on this below:

1. **Malicious domain generation algorithms (DGA):** DGA generate a large number of random domains which malicious actors may use to make it difficult for control and command malware to be taken down.
2. **Proxy domain name registration:** Proxy domain registration services provide anonymity for domain users by using a third-party to register domain names on the user's behalf and can be used to protect malicious actors when perpetrating harmful activity.
3. **Domain 'hijacking', 'spoofing' and 'shadowing': Domain hijacking** is when a domain is wrongfully taken from the rightful name holder. **Domain 'shadowing'** creates malicious subdomains, without the domain owner's knowledge. **Domain 'spoofing'** is when a malicious actor uses a domain to impersonate a legitimate website or email

[3] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

domain to trick users. In these cases, the purpose is often to carry out harmful activity, such as phishing, in order to retrieve sensitive information or distribute malware.

4. **Traffic site diversion:** Traffic site diversion, which uses the names of well-known brands or companies to divert website traffic, can take a number of forms. The purpose is not always malicious. In cases where the purpose is to lure users to copycat websites to retrieve personal details or install malware, this would be covered through our existing list of misuses.

17 respondents made reference to the inclusion of misuses related to domains which are registered or used to host content on the internet which is illegal or harmful. This includes domains:

- Created or used for the sale of illicit or counterfeit pharmaceuticals and the illegal distribution of opioids.

- Created or used to sell or make available content or goods that infringe intellectual property. This might include for example, a website offering for sale goods that infringe intellectual property rights (such as counterfeit goods) or a website that enables a user to stream or download content that infringes intellectual property rights.

- Created or used for other types of illegal or harmful content including disinformation, including that which leads to hate crime, money laundering, child exploitation (beyond child sexual exploitation and abuse), human trafficking, and incitements to violence.

We recognise that, through their terms and conditions, the registries already have in place policies to prevent the registration of domains to carry out illegal activity. In addition, we understand that in-scope registries who are aware of this type of activity already work with several appropriate agencies to take action. This includes responding to reports from the UK IP Crime Group (IPCG) and Police Intellectual Property Crime Unit (PIPCU) regarding IP-related criminal activity in support of combatting online piracy, working closely with the Medicines and Healthcare products Regulatory Agency (MHRA) in relation to the sale of illegal or illicit pharmaceuticals and working with the Cyber and Fraud Centre Scotland (formerly known as SBRC) which has a very wide remit against all forms of cybercrime.

Several existing government policies and regulations also exist to help combat this type of activity online. Some examples of this include:

- Schedule 1 of the Consumer Protection from Unfair Trading Regulations (which is being restated in the Digital Markets, Competition and Consumer Bill). This prohibits unscrupulous traders from misleading consumers by appearing to be, or be linked to, to a different business. Trading Standards and other consumer law enforcers can bring criminal or civil proceedings against those engaging in a banned practice such as this, working to ensure consumers are not ripped off by traders pretending to be someone they are not.

- There are available additional remedies for brand owners, such as pharmaceutical companies, to use via the civil courts, namely "blocking orders"[4] which require online service providers to disable or remove access to infringing content.

- Under the Online Safety Act 2023 (OSA) all companies in scope will need to take action to tackle illegal activity, including fraud, where it is facilitated through user-generated content or via search results. They must take preventative measures to prevent fraudulent content, such as selling counterfeit goods, appearing on their platforms and swiftly remove it if it does. Additionally, there will be a duty on the largest platforms and search engines, requiring them to tackle fraudulent adverts on their services. Similarly, the OSA requires services to take steps to effectively mitigate the risk their services are used to facilitate or commit priority offences. Priority offences are the most serious and prevalent illegal content and activities. Priority offence categories include hate crime, incitement to and threats of violence and to kill, human trafficking and money laundering. Under the OSA, companies will also be forced to act against illegal misinformation and disinformation, removing in-scope content if they become aware of it on their services.

- Through the Criminal Justice Bill[5], the government is proposing to create a new power for UK law enforcement agencies to suspend IP addresses and domain names that are being used in serious crime, including fraud and unauthorised access to systems and data. Under the Bill, UK law enforcement authorities, such as the police and the National Crime Agency, will be able to apply for a court order requiring the organisation responsible for providing the IP address or domain name to prevent access. This power will apply to domestic and international domain name and IP address providers, however in the UK we expect the existing voluntary arrangements to be used as the first port of call.

- More broadly, a review of UK product safety law aims to tackle the sale of unsafe and non-compliant products sold online. The existing law is clear that all consumer products, including goods sold online, must be safe before they can be placed on the UK market. Despite this, it is too easy for consumers to buy unsafe products online. The recently published Product Safety Review consultation contained proposals to modernise responsibilities for online marketplaces so that products bought online are as safe as those bought on the high street. Responses to the consultation are currently being considered and a government response will be published in due course.

Taking into account the existing policies and regulations detailed above and recognising the role of the registry operators as being as technical providers of naming and addressing identifiers on the internet, we do not deem our regulations, which only include UK-related

[4] Injunctions ("blocking orders") are available before the courts with respect to online service providers under Section 37(1) of the Senior Court Acts and Section 97A of the Copyright, Designs and Patents Act 1988 with respect to the infringement of IPR. In *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch), the court held that blocking orders are available for infringement of all IPR.
[5] The Criminal Justice Bill was introduced in the House of Commons on 14 November 2023 and is currently being considered by Parliament.

domain names in scope, to be the most effective vehicle to combat the misuses proposed above. However, we do also acknowledge the concerns raised through this consultation and DSIT will keep under review the effectiveness of the current landscape.

Our list of misuses will therefore look as below:

Registries should have in place adequate policies and procedures to mitigate against domain names being registered, and deal with instances when they have been notified that domain names are being used, with the purpose of carrying out the below misuses. We deem misuses to include these five broad categories of harmful activity as identified by ICANN.[6]

- ***Malware:*** *installing and/or executing malicious software on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software.*
- ***Botnets:*** *collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator.*
- ***Pharming:*** *redirection of unknowing users to fraudulent sites or services, typically through the Domain Name System (DNS) hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to the attacker's site instead of the one initially requested. DNS poisoning causes a DNS server, or resolver, to respond with a false IP address bearing malicious code.*
- ***Phishing:*** *when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.*
- ***Spam emails:*** *when used as a vehicle for at least one of the preceding 'misuses'.*

Registries should also have in place adequate policies and procedures to combat the use of domain names administered by those registries which are registered to promote or display ***Child Sexual Abuse Material****. This refers to indecent images of children (photographic/video or pseudo images) as outlined in the Protection of Children Act 1978 and the Indecent and Prohibited Images of Children Crown Prosecution Service Guidance, which includes computer-generated images (CGI's), cartoons, manga images and drawings, that have been produced solely or principally for the purpose of sexual arousal.*

[6] https://www.icann.org/dns-security-threat

Questions on domain name unfair use

Questions four, five and six related to the proposed list of unfair uses, their definitions and whether any additional types of domain name unfair uses should be included. These questions were:

- 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?
- 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.
- 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.

Overall, there was broad agreement with the proposed list of unfair uses and associated definitions.

Policy response

Four respondents wanted us to use the definition of IP infringements in relation to cybersquatting contained in Article 10 of the Budapest Convention on Cybercrime[7]. Article 10 sets out offences related to infringements of copyright and related rights, which is a more detailed definition, focusing on copyright abuse, without mentioning cybersquatting, compared with our definition (pasted below), which focuses on cybersquatting specifically.

As detailed in the section above, we do not find the Budapest Convention to be directly pertinent in the context of these regulations and given a large portion respondents agreed that we should include cybersquatting under the list of unfair uses of domain names, we recognise the importance of maintaining this within our definition.

Two respondents who disagreed on question five wanted to see ICANN/Nominet's definitions used instead. We have considered these definitions, as well as other respondent's proposals to widen and clarify our definition of unfair uses to capture other types of cybersquatting. This includes including 'service marks' and 'domain name speculation', clarifying 'bad faith' and removing 'pre-emptive' in our definition.

From our research, there appears to be multiple pre-existing definitions of cybersquatting, from ICANN, Nominet, World Intellectual Property Organisation (WIPO), those found in dictionaries and others. Many of these include reference to 'bad faith' in the same way we have done in our definition, and do not specifically mention 'domain name speculation' or 'service marks'. We consulted on the use of the definition set by WIPO, which refers to the 'pre-emptive', bad faith

7 See pp.9-10 of this document: https://assets.publishing.service.gov.uk/media/5a7c929ded915d6969f45d32/8309.pdf

registration of trade marks, with the addition of ‘typosquatting’ and the majority of respondents were in favour of this.

We analysed ‘domain name speculation’ and understand this to mean the practice of identifying and registering or acquiring internet domain names (typically by third parties who do not possess rights in such names) as an investment with the intent of selling them later for a profit. As it is frequently carried out without malicious intent, we do not believe it is appropriate to include in our list, given we want to avoid capturing the non-bad faith registration of domain names in our regulations.

We will therefore continue to set out the below cybersquatting definition in our regulations:

Registries should have in place an adequate dispute resolution procedure to deal with instances when they have been notified that domain names have been registered with the purpose of carrying out unfair practices which constitute ‘cybersquatting’.

Cybersquatting refers to the pre-emptive, bad faith registration of trade marks as domain names by third parties who do not possess rights in such names. This includes ‘typosquatting’, when an end user takes advantage of common misspellings made by Internet users who are looking for a particular site or a particular provider of goods or services, in order to obtain some benefit.

Questions on proposed principles for the prescribed dispute resolution procedure

Questions seven to 11 related to the proposed principles which will underpin the prescribed dispute resolution procedure (DRP). Respondents were invited to comment on key principles and overall feedback on the best practice for designing the DRP. These questions were:

- What would you consider to be too burdensome in the context of resolving disputes under our prescribed dispute resolution procedure?
- What does 'expeditiously' mean to you in the context of resolving disputes under our prescribed dispute resolution procedure?
- What do you consider to be 'low cost' in the context of resolving disputes under our prescribed dispute resolution procedure?
- What would you consider a 'fair' and 'equitable' dispute resolution procedure design to be?
- Do you have any further comments on best practice or about the overall design of our dispute resolution procedure?

Policy response

Two respondents noted that the DRP should include an appeals mechanism and not having one may detrimentally affect freedom of speech. In addition, three respondents said that the resolution procedure should be conducted by an independent third party.

The generic top-level domains (gTLDs) in scope must follow ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP), as per their contracts with ICANN. The UDRP does not include an appeals mechanism, therefore, if we stipulated the need for an appeals mechanism in our regulations, this could cause the gTLDs in scope to be in conflict with their contract with ICANN.

We received feedback that our regulations should not conflict with the existing dispute procedures that registries in scope of the regulations are bound by, notably ICANN's UDRP and Nominet's Dispute Resolution Service (DRS). We have taken on board this feedback and recognise that these are effective dispute resolution procedures. We recognise that both dispute procedures appoint independent experts to review and adjudicate their dispute systems.

We have also understood the need for our DRP not to be burdensome and to be as fair as possible with proportionate costs according to the specific case that is being addressed. We therefore do not propose to specify that an appeals mechanism must be in place or that an independent third party must conduct the dispute resolution procedure.

With the above in mind, we do not propose stipulating exact costs, times or processes for resolving disputes, but rather an outline of what a qualifying dispute resolution procedure should look like.

Our draft proposed dispute resolution procedure is below:

Registries should have in place an adequate dispute resolution procedure for dealing with complaints in connection with domain names. There is not one prescribed procedure that registries must follow or one provider that must be used, however, their chosen procedure must:

- *Not involve a disproportionate cost for the complainant/registrant. The cost should be proportionate to the cost incurred by the registry for either their internal processes or for the mandated provider of the dispute resolution procedure when the registry uses a third-party provider. There should not be a profit made from the procedure.*
- *Resolve the dispute in a timely manner. The time taken should be proportionate to the complexity of the complaint and should always be dealt with in the least amount of time possible.*
- *Be designed in a fair, open, transparent and equitable way. The procedure should be written in plain language with clear definitions so that it is easily available for complainants to understand and engage with.*
- *Not preclude resort to judicial proceedings.*

Questions on business impacts of the proposals at the consultation stage

Questions 12 to 15 related to the potential impact that the proposals outlined in this consultation may have on businesses, consumers or the public sector. These questions were:

- To what extent do you agree or disagree with our assessment under the 'Summary of Business Impact' section? Please provide details for your answer.
- Are there potential positive impacts (including costs or financial implications) that the proposals outlined in this consultation may have on businesses, consumers or the public sector? Please provide any evidence or comments on what you think these positive impacts would be.
- Are there potential negative impacts (including costs or financial implications) that the proposals outlined in this consultation may have on businesses, consumers or the public sector? Please provide any evidence or comments on what you think these negative impacts would be.
- Please provide any other comments or evidence that relates to or is about the analysis under the 'Summary of Business Impact' section.

Policy Response

We have considered the feedback received on the business impact of our proposals. As referenced above, we recognise the need to avoid gTLDs having to build a parallel dispute resolution procedure to reduce business impact.

The majority of respondents did not answer questions 12 to 15. However, the responses that were received demonstrated broad agreement with the government's assessment in that the preferred approach focuses on continuing existing practices and is unlikely to materially affect the actions/steps businesses currently take.

Three respondents that felt that the commencement of the DEA 2010 provisions could make the UK internet domain name industry unattractive. However, the responses also highlighted the positive impacts of the proposals, including increasing trust in UK top level domains and resulting in a cost-effective and efficient means for combating DNS harms and for resolving disputes. We agree that this is important and reaffirm that our policy objective is to ensure that there continue to be procedures in place to deal with the misuse and unfair use of these domains for the users of UK-related domain names that are in scope of the powers.

We will continue to assess the business impact as our policy is finalised and work with the registries in scope of the regulations to ensure that the policy does not result in increased costs for them and therefore increased costs for those purchasing domain names, as per feedback from the consultation. We are also committed to ensuring that the commencement of the DEA 2010 powers does not have a negative effect on the perception/appeal of the UK market.

Questions on impact on individuals with protected characteristics of the proposals at the consultation stage

Questions 16 and 17 related to the potential impact that the proposals outlined in this consultation may have on individuals with protected characteristics. These questions were:

- 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/or negative) would be.
- If you believe there may be negative impacts, what do you think could be done to mitigate them?

Policy Response

We received feedback from one respondent on ensuring our DRP is accessible for all audiences. We will take this into account when drafting our regulations and will continue to ensure that our policies will not adversely affect people who are protected under the Equality Act 2010.

Next Steps

DSIT remains committed to bringing sections 19-21 of the DEA 2010 into force in the coming months. It is essential that there continue to be procedures in place to deal with the misuse and unfair use of these domains for the users of UK-related domain names that are in scope of the powers. Commencing these powers will provide further certainty that these procedures exist and are upheld to the highest standards.

DSIT will follow the policy approach outlined above when drafting the regulations and making the secondary legislation.

Consultation Questions

1. Do you agree we should include all of 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?

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.

3. Are there any other types of domain name 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.

4. 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?

5. 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.

6. 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.

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

8. What does ‘expeditiously’ mean to you in the context of resolving disputes under our prescribed dispute resolution procedure?

9. What do you consider to be ‘low cost’ in the context of resolving disputes under our prescribed dispute resolution procedure?

10. What would you consider a ‘fair’ and ‘equitable’ dispute resolution procedure design to be?

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

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

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

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

15. Please provide any other comments or evidence that relates to or is about the analysis under the ‘Summary of Business Impact’ section.

16. 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/or negative) would be.

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

This consultation is available from: www.gov.uk/government/consultations/powers-in-relation-to-uk-related-domain-name-registries

If you need a version of this document in a more accessible format, please email alt.formats@dsit.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.