WRITTEN EVIDENCE SUBMITTED BY THE ICANN BUSINESS CONSTITUENCY

For consideration by the Public Bill Committee regarding the Criminal Justice Bill

8 December 2023

About the ICANN Business Constituency

The Business Constituency (BC) is the voice within ICANN (the Internet Corporation for Assigned Names and Numbers – the coordinating body of domain name system (DNS) policy) of worldwide commercial internet users (including those in the United Kingdom). ICANN is a global body with responsibility for certain policies that relate to the DNS. Domain names are the identifiers consumers and businesses rely upon to find websites for legitimate products and services on the Internet and are used for e-mail. From time to time, the BC provides perspective and comment to governmental bodies interested in DNS-related issues.

The BC has an ongoing interest in combating various types of crime and abuse facilitated through the DNS, including the types identified in Schedule 3 of the Criminal Justice Bill. Accordingly, the BC respectfully submits evidence and input herein in support of the furtherance of this portion of the bill.

Thank you for the opportunity to submit our perspectives on this important legislation.

Executive Summary

- Crime and abuse orchestrated through the DNS, including the types identified in the bill, is a serious and growing problem.
- Industry and ICANN have led voluntary efforts to combat such crimes and abuse, but these measures are insufficient to address the wide scale of types of crime and abuse.
- The Parliament's efforts (particularly via domain name takedowns) to address certain types of crime and abuse in the UK are welcomed but may need to be broadened to ensure efficacy over time.
- The Parliament is encouraged to continually monitor trends in the rapidly developing area of online crime and abuse and evaluate the need for additional legislation.

DNS-related crime and abuse is a costly and increasing problem

1. As representatives of business users of the internet (and their customers and end consumers), the BC takes note of the serious and increasing incidences of online crimes and abuse. In addition to the types of crimes specified in the Criminal Justice Bill, these include fraud, intellectual property infringement, distribution of malware, phishing, distribution of child sexual abuse material (CSAM), and distribution of falsified medicines, to name only a few. Such crimes are increasingly perpetrated via abuse of the DNS, including the misuse of well-known brand names or keywords about current events that are maliciously registered as domain names, and act as bait to lure consumers to sites offering illegal content or to trap them into trusting that an e-mail is from a genuine source (such as a bank).

2. The rate of increase in criminal activity is well documented (online misconduct is one of the fastest-growing areas of crime, and costs businesses and their users billions annually). For example, in the area of phishing alone:

   In its August 2023 study[1] on phishing trends, the US-based consultant Interisle Consulting Group found that:

   - The number of phishing attacks worldwide tripled since May 2020 and continues to trend upward;
   - More than one million unique domain names were reported for phishing between May 2022 and April 2023 alone, the most observed by Interisle in any period since May 2020; and
   - Two thirds of domain names reported for phishing were maliciously registered, meaning they were intentionally registered by a criminal with the intent of launching a phishing attack.

Voluntary, industry-based solutions are insufficient

3. While laudable, initiatives led by industry[2] (e.g., registries, registrars and ICANN itself) have fallen short of the measures necessary to effectively combat online crime which, as noted above, continues to expand.

4. ICANN recently negotiated changes to its contracts with registries (the Registry Agreement, or RA) and registrars (the Registrar Accreditation Agreement, or RAA), which resulted in amendments to the contracts that establish an affirmative duty to disrupt or mitigate DNS abuse. However, while an overall positive step, the contracts' definition of what constitutes DNS abuse is severely limited (it lists only pharming, phishing, malware, botnets and spam as a delivery mechanism for the previous four types) and omits other serious types of crime facilitated through the DNS. ICANN shows no indication of an intention of expanding this definition, even as its own Security and Stability Advisory Committee advises that "These categories have been adopted within the ICANN realm in specific contracts, but do not represent all forms of DNS abuse that exist, are reported, and are acted upon by service providers. New types of abuse are commonly created, and their frequency waxes and wanes over time. Thus, no particular list of abuse types will ever be comprehensive."

5. Accordingly, there has been scant effort within industry to meaningfully address online crime as it is experienced by businesses and internet users. As a result, cybercrime continues to grow, expand and become more sophisticated.

The Parliament's crime bill is welcome, but with regard to online crime, may need to go further

6. The BC welcomes the provisions of the Parliament's crime bill which deal with domain name takedowns and other enforcement measures as a response to facilitation of crime via the DNS.

[1] https://interisle.net/PhishingLandscape2023.pdf

[2] For example, the DNS Abuse Institute, the DNS Abuse Framework, ICANN's own board committee on DNS abuse, and other industry-rooted efforts.

7. The BC notes the definitions in Schedule 3 of "crime" and "serious crime" and, in particular, the identification of unlicensed online gambling as a problem; we however encourage Parliament to incorporate DNS abuse-related crime (e.g., CSAM distribution, phishing, imposter domain names, intellectual property infringement, selling falsified and substandard pharmaceuticals or medications in absence of proper examination or oversight from appropriate medical professionals, the five types of abuse defined in ICANN's RA and RAA, etc.) appropriately into its definitions as a means to broaden its mitigation efforts into a more fulsome list of crimes.

8. Specifically, the BC raises the advisability of a requirement to enable access to domain name registration data (known as "WHOIS") that would enable the investigatory capacity of governments and businesses seeking to protect consumers from online crimes.

The Parliament should monitor DNS-related crime in an ongoing fashion

9. The BC strongly encourages Parliament to employ the use of cybersecurity experts to carefully and regularly monitor developments relating to crime via the DNS. As stated above, "DNS crime and abuse" does not adhere to a static definition and threat vectors will change over time.

10. The BC would be encouraged by follow-up changes to this legislation, or the introduction of new legislation, that more extensively addressed the use of domain name suspension as a means for addressing online crime and malicious registrations.

The BC is available to the Committee to discuss the above and to assist as necessary. We again thank the UK Parliament for the opportunity to comment on this matter.

This comment was drafted by Mason Cole, with edits from Tim Smith and Marie Pattullo.

It was approved in accord with the BC Charter.