msk

MITCHELL SILBERBERG & KNUPP LLP
A LAW PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

J. Matthew Williams
Partner
(202) 355-7904 Phone
(202) 355-7984 Fax
mxw@msk.com

April 6, 2023

VIA E-MAIL ONLY (CMAREVIEW@HOMEOFFICE.GOV.UK)

Rt Hon Tom Tugendhat MBE VR MP
Minister of State for Security
c/o Cyber Policy Unit
Homeland Security Group
Home Office
5th Floor, Peel Building
2 Marsham Street
London
SW1P 4DF

Re: Review of the Computer Misuse Act 1990: consultation and response to call for information

Dear Minister Tugendhat,

I write as Executive Director and Legal Counsel to the Coalition for Online Accountability (COA).[1] We are pleased to submit these comments concerning the above-referenced review. COA is a longstanding group of companies, trade associations, and copyright member organizations dedicated to enhancing and strengthening online transparency and accountability by working to ensure that domain name and IP address WHOIS databases remain publicly accessible, accurate, and reliable, as key tools against online infringement of copyrights, as well as to combat trademark infringement, cybersquatting, phishing, and other illegal acts. There is no doubt that the motion picture, music and videogame industries have long suffered from widespread online piracy and other abuses. In countless ways, COA members are seeing deceitful use of their company logos, brands, and copyrighted works. Increasing the legal and regulatory tools that should help to thwart such conduct is of great importance to COA's members. In these brief comments, we focus on the issues of most relevance and significance to our coalition and industries, and do not respond to every question in the open consultation announcement. Thank you for the opportunity to reply to the call for information on this important review.

We are very appreciative that the domain name system (DNS) is a subject of your call for information. Bad actors too often maliciously use domain names to commit a growing number of crimes. It is crucial that those with legitimate interests – including not only law enforcement,

[1] COA comprises Broadcast Music, Inc. (BMI), Entertainment Software Association (ESA), Motion Picture Association, Inc. (MPA), NBCUniversal, Recording Industry Association of America, Inc. (RIAA), The Walt Disney Co., and Warner Bros. Discovery.

but both public and private sector authorities – have the necessary tools to prevent, to investigate, and to mitigate online harms.

Accordingly, we focus here on the importance of access to accurate, verified domain name registration data (known historically as "WHOIS" data), which is a central element of healthy DNS functionality.

The important role of domain name registration data

While domain names are an appropriate focus of this consultation, contending with abuse via the DNS necessarily must also include consideration of domain name registration data. Not only must security experts and law enforcement authorities have the ability to prevent threats from arising and to mitigate threats through remediation, but also the ability to thoroughly investigate the person(s) responsible for offending, registered domain names. This requires access to complete and accurate domain name registration data.[2] Such records can identify domain name registrants. This enables traceability of often opaque, bad-actor activity and prevents further harm.

Unfortunately, domain name registrars and registries caused the global elimination of publicly available WHOIS data following the adoption of European Union's General Data Protection Regulation (GDPR). This action impaired investigatory efforts related to online harms in the United Kingdom and elsewhere. While the European Union's Directive on the Security of Network Information Systems (NIS2) includes new requirements for the collection by domain name registries and registrars of a complete and accurate WHOIS database, it remains to be seen whether it will impact domain names outside of the jurisdiction of the European Union. As a result, it serves the public interest in the United Kingdom to include WHOIS requirements in the Computer Misuse Act of 1990.

WHOIS and investigatory capability

Mindful of privacy law obligations, restored publication of WHOIS data pertaining to legal persons would tremendously assist investigations by law enforcement, cybersecurity authorities, intellectual property rights holders, and others. In addition, the WHOIS data pertaining to natural persons must be available ***on request*** to those with legitimate interests in uncovering registration data for nefariously used domain names. Often, quick and timely access to this data can help uncover the source of online crimes and offenses, even without employing the blunt instrument of domain name takedowns.

[2] Importantly, this must include the collection (by registrars) and maintenance (by both registries and registrars) of "thick" WHOIS data – that is, a complete set of data about the domain name registrant (rather than "thin" data, which contains only information about the sponsoring registrar and registration dates). At present, not all registries maintain thick data. Were they so mandated, registries as well as registrars could effectively respond to investigatory queries, contributing more actively to mitigate DNS abuse.

These investigations must be able to access the final, underlying documentation of the registrant(s), even if a registrar or registry employs privacy and proxy services to further mask the identities of registrants. While privacy and proxy services may provide utility to the customer, they must not prevent or impede investigators of cybercrimes and other illegal activities from accessing the customer-specific data underlying any masking service.

NIS2 and clarification of WHOIS-related policy

The EU's publication of the NIS2 in January recognized the unique role of WHOIS in investigating, preventing and mitigating cybercrime. Article 28, and associated recitals, of the directive impose new requirements on registries, registrars, and others involved in the life cycle of a domain name. Specifically, these parties must:

- collect and maintain a complete and accurate database of registration data;
- verify and ensure the accuracy of WHOIS data;
- make publicly available all WHOIS data that is not personal data, including the data of legal persons;
- respond without delay to WHOIS data access requests and provide access upon lawful requests; and
- provide legitimate access to WHOIS data free of charge.

The NIS2 WHOIS policy example is helpful and should be followed in the UK

WHOIS data, while critical to impeding online crime, is not directly a focus of this consultation. However, we encourage the Cyber Policy Unit to include WHOIS access policy as a key area of its forward-looking, policymaking considerations, with an eye toward ensuring timely data access for those with legitimate interests.

Thank you again for the opportunity to respond to this consultation.

Respectfully,

/s/ J. Matthew Williams, Executive Director and Legal Counsel to COA
Partner of
MITCHELL SILBERBERG & KNUPP LLP

JMW/psb