ANNEX TO LETTER:

The Digital Services Act is an Opportunity for the European Commission to Restore Urgently Needed Access to WHOIS Data

BACKGROUND ON WHOIS DATA

The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit organisation which, through its multi-stakeholder community, sets policies and enters into accreditation contracts with domain name registries and registrars with the goal of ensuring the secure and stable operation of the Internet Domain Name System. ICANN's jurisdiction only covers generic top-level domain names ("gTLDs") such as .com, .net, .org, .info and .online. Currently there exist over 1,200 gTLDs[1]. ICANN's policies and contracts do not apply to country-code top level domains ("ccTLDs") such as .be for Belgium and .dk for Denmark. Rather, policies and rules for the operation of ccTLDs are determined by the relevant country and legal entity that exists to operate the ccTLD.

Under ICANN's policies and contracts, domain name registrars and registries sell and administer gTLD domain names. When an individual or an organisation acquires a domain name for a website, that individual or organisation (referred to as the "registrant") must provide contact information, including name, email address, postal address and phone number as part of the domain name registration process. Combined with certain other attributes of a registered domain name, this information is collectively referred to as WHOIS data. For more than 20 years, ICANN has administered the collection and availability of WHOIS data for gTLDs. During that entire period, up until May 2018, WHOIS data was always publicly and immediately accessible via an online lookup portal. Until May 2018, the publicly accessible WHOIS data[2] essentially functioned as the equivalent of a land registry for Internet domains.

THE IMPORTANCE OF WHOIS DATA TO THE PUBLIC INTEREST

Until May 2018, publicly accessible WHOIS data was used for a variety of purposes by both public and private sector organisations, including law enforcement agencies, cybersecurity investigators, network technology professionals, child protection organisations, patient safety organisations, consumer welfare organisations, and anti-counterfeiting and anti-piracy organisations. Government agencies and private sector organisations routinely used WHOIS data as the first step in their work of investigating websites engaged in potential illegal or abusive activity. Consumers concerned about the legitimacy of a website could easily (and routinely did) consult WHOIS data via a WHOIS portal hosted by the registry or registrar, or a centralised look-up operated by ICANN to find out who had registered the domain name of the website and determine whether that information matched or supported what the website was purporting to be. The 170+ member Governmental Advisory Committee ("GAC") to ICANN stated in June 2020 with respect to WHOIS data, *"[A]ccess to this information is essential to allow public*

[1] See this Wikipedia entry for further background information on gTLDs: https://en.wikipedia.org/wiki/Generic_top-level_domain

[2] Before May 2018, WHOIS data had been a public directory since the earliest days of the Internet, beginning in the early 1980s. For a brief history of WHOIS, see: https://whois.icann.org/en/about-whois#field-section-3

authorities and other relevant entities to serve objectives such as law enforcement, cybersecurity, consumer protection or the protection of intellectual property. Such access remains a high priority for the GAC."[3] Note that the European Commission as well as all EU Members States are active members of the GAC. In its recent Communication on the EU Security Union Strategy, the Commission emphasised that *"access to Internet domain name registration information ("WHOIS data") is important for criminal investigations, cybersecurity and consumer protection."*[4] In short, WHOIS data served as the sole, reliable accountability mechanism in an otherwise-anonymous internet.

THE GDPR AND WHOIS DATA

The General Data Protection Regulation ("GDPR") came into effect in May 2018. We agree with the Commission's recent Communication to the European Parliament and the Council that the GDPR *"strengthened data protection safeguards [and] provides individuals with additional and stronger rights."*[5]

As WHOIS data sometimes contains personal data, such as name, postal address and phone number of a natural person, ICANN adopted a policy called the Temporary Specification in May 2018 intended to comply with the GDPR's personal data protection requirements.[6] Under this policy, most of the WHOIS data—and in particular the contact data of the registrant and the registrant's agents—is redacted from the publicly accessible WHOIS directory. In adopting this policy, ICANN permitted domain registrars and registries to redact the data of legal entities, even though the GDPR only applies to the data of natural persons.[7] But even under ICANN's Temporary Specification policy, registrars and registries must provide "reasonable access" to the redacted WHOIS data to third parties on request, such as law enforcement agencies or anti-counterfeiting organisations, when necessary for the legitimate interests of those third parties, except where such interests are overridden by the interests or rights of the data subject which require protection of personal data. This is the same standard for third party legitimate interest access articulated in Article 6(1)(f) the GDPR. However, registries and registrars have not provided reasonable access to this data, and ICANN has stated that it is unwilling to enforce this policy to require access in any case where a registry or registrar has refused it.

FAILURE TO GRANT ACCESS TO WHOIS DATA FOR LEGITIMATE PURPOSES

Since May 2018, the WHOIS data relevant for law enforcement investigations, cybersecurity investigations and mitigation, consumer safety and welfare, child protection efforts and intellectual property enforcement has gone dark. With respect to access requests to serve legitimate interests, almost all of such access requests are ignored or denied in a system that is now fragmented. In the practical experience of one leading group, Appdetex, only 6.2% of over 1,110 requests for registrant contact data for domains that were involved in phishing and malware attacks resulted in the provision of

[3] See ICANN67 GAC Communique at: https://gac.icann.org/contentMigrated/icann67-gac-communique at p. 7
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN at p. 11
[5] https://ec.europa.eu/info/sites/info/files/1_en_act_part1_v6_1.pdf
[6] The Temporary Specification may be found here: https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf
[7] ICANN received guidance from the European Data Protection Board that contact details of natural persons contained in the WHOIS data of legal persons are within the scope of the GDPR.

registrant contact data.[8] The European Parliament has taken note of this lack of access of WHOIS data for legitimate interests with alarm as evidenced by a Parliamentary Question earlier this year which noted notwithstanding that ICANN's policy *"requires that access is granted to entities with a legitimate purpose for such access . . . approximately 75% of requests for access remain unanswered and almost all requests that receive an answer are denied."*[9]

The subjective judgment of domain name registries and registrars operating under ICANN policy as the controllers of redacted WHOIS data has led to an unpredictable and fragmented system and contributed to this unacceptable situation where legitimate access requests are routinely denied. Even European government agency and law enforcement requests for redacted WHOIS data have been denied. As described in a May 2020 letter from the ICANN President to the European Data Protection Board, requests that have been made by European Data Protection Authorities for access to redacted, non-public WHOIS data to assist in their investigations of potential privacy violations have been denied by domain name registrars and registries.[10] Such registries and registrars are likely to evaluate the privacy of redacted WHOIS data of registrants in absolute terms, without considering other rights and legitimate interests, to avoid possible regulatory sanctions or judgments against them. Far from furthering legitimate privacy interests, the ICANN policy in response to the GDPR and its implementation by domain name registries and registrars have actually undermined the privacy protections of end users of the Internet—and not just by blocking investigations by Data Protection Authorities, but also by other consequences, such as increased phishing attacks as described later in this Annex.

Moreover, ICANN's policy and its implementation has significantly hampered and impeded law enforcement investigations and likely contributed to the substantial increases in illegal and abusive activity online. A survey conducted by the Public Safety Working Group of the GAC of over 50 law enforcement agencies from around the world detailed how the lack of availability of WHOIS data since ICANN's adoption of the policy in an effort to comply with the GDPR has interfered with the work of such government agencies. Prior to the adoption of the ICANN policy in May 2018, only 2% of the law enforcement agencies reported that WHOIS data did not meet investigative needs. Following implementation of the policy, **67% of the agencies reported that WHOIS data did not meet investigative needs.**[11] The Commission noted in comments on ICANN's WHOIS policy that *"we stress that the current situation is affecting EU Member States' authorities to obtain legitimate access to this data."*[12]

Amplified by the COVID-19 crisis and the accelerating rate of dependence on digital services in our daily lives, there has been a well-documented increase of online illegal activity of all kinds, from online child sexual abuse[13] to cybersecurity and phishing attacks. From a public health perspective, there is a rising tide of websites taking criminal advantage of fear and misinformation regarding COVID-19 and seeking to sell falsified medicine and even vaccines.[14] The Commission has observed that *"cyberattacks and cybercrime continue to rise"* and that the COVID-19 pandemic has *"opened the door to an extraordinary*

[8] See: https://blog.appdetex.com/appdetex/dns-phishing-mitigation-slow-and-unwieldy
[9] E-000826/2020: https://www.europarl.europa.eu/doceo/document/E-9-2020-000826_EN.html
[10] See: https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf
[11] https://gac.icann.org/presentations/public/icann63%20pswg.pdf
[12] https://mm.icann.org/pipermail/comments-epdp-recs-04mar19/attachments/20190417/6f0a65b2/CommentsontheTemporarySpecificationforgTLDRegistrationDataPolicyRecommendations-0001.pdf
[13] See e.g., https://www.europol.europa.eu/iocta-report
[14] See e.g., https://themedicinemaker.com/manufacture/the-rise-of-the-covid-19-scammer

increase in malicious attacks." [15] In a recent report by Europol on criminal networks involved in the trafficking and exploitation of underage victims, Europol found that *"the internet and social media increasingly play a role in the recruitment phase."*[16] In the U.S., the FBI's Internet Crime Complaint Center reported that as of June 2020, daily cybersecurity complaints had spiked from 1,000 to 4,000 and that cyberattacks on financial institutions had increased by nearly 240%.[17] During the recently concluded virtual ICANN69 meeting, a European law enforcement member of the GAC Public Safety Working Group noted that reports of ransomware attacks have increased by over 700%.[18] A recent report by Interisle found that during the three-month period of May 1 – July 31, 2020 there were over 120,000 phishing attacks. This dramatic increase in online illegal activity and abuse has also been recognised and acknowledged by domain name registries and registrars themselves. As reported by a leading American domain name registry earlier this year, Neustar, *"we're seeing a dramatic upturn in attacks using virtually every metric that we measure. We have observed an increase in the overall number of attacks as well as in attack severity..."*[19] (emphasis added) Clearly this situation is leading to an erosion of consumer trust online—an issue of key concern to the Commission with respect to the Digital Services Act.

As a result, governments have emphasised the urgent need to resolve the current lack of access to WHOIS data. In October 2018—two years ago—the Council of the European Union endorsed EU lines to take on WHOIS policy that included the following:

"The EU and its Member States stress that the current situation where access to non-public WHOIS data for public policy objectives is left at the discretion of registries and registrars affects the Member States authorities' ability to obtain legitimate access to non-public WHOIS data necessary to enforce the law online, including in relation to the fight against cybercrime. It may also affect the rights of individuals.

The EU and its Member States note the concerns raised by law enforcement authorities, cybersecurity organisations and intellectual property rights holders about the negative impact of limitations of access to WHOIS data on their work. Finding a workable solution for access to non-public WHOIS data should be treated as a matter of priority." (emphasis added)[20]

ICANN'S RESPONSE IS NOT FIT FOR PURPOSE

After more than two years since the adoption of its Temporary Specification in May 2018, the ICANN Expedited Policy Development Process team issued a nearly 200-page Final Report of the Temporary Specification for the gTLD Registration Data dated July 31, 2020 ("Report").[21] The Report contains a

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN at p.1 and p.3
[16] See page 19 of report that may be found at this link: https://www.europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims-in-eu
[17] See: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
[18] See page 27 of presentation slide deck available for download here: https://69.schedule.icann.org/meetings/w8wuCYSW5rvL4Yzf3#/?limit=10&sortByFields[0]=isPinned&sortByFields[1]=lastActivityAt&sortByOrders[0]=-1&sortByOrders[1]=-1&uid=a6ijir8iemBHYWRru
[19] https://www.home.neustar/resources/whitepapers/covid-19-online-traffic-and-attack-data-report
[20] See: https://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf
[21] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf

series of weak policy recommendations for the implementation of a so-called System for Standardised Access/Disclosure to non-public registration data (e.g., redacted WHOIS data). Unfortunately, the System leaves WHOIS data disclosure decisions almost entirely to the subjective judgment of gTLD domain registries and registrars, **thereby continuing and endorsing the exact same fragmented situation that the EU identified as unacceptable in the EU Council communication quoted above.** Furthermore, the policy recommendations set service level guidelines allowing several days for registrars and registries to respond to requests for disclosure of WHOIS data. Yet for investigations of cybersecurity threats and other criminal activity, including child sexual abuse, responses are needed in minutes or hours, not days or weeks. As the Europol EC3 Advisory Group on Internet Security explained *"Most cybersecurity investigations . . . rely on WHOIS queries. Such real-time queries provide what is sometimes the only information available to timely identify and protect against advanced persistent threats, cybercrime infrastructure (such as fast-flux botnets), and other DNS abuse."*[22] Indeed, prior to May 2018, the data was immediately accessible supporting real-time queries.

The EU was not alone in its dissatisfaction with the Final Report and the recommended access System. The entire 170+ member GAC (including GAC members from the Commission) filed a Minority Statement to the Report stating that the Final Report and policy recommendations, including the proposed access System *"do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars, and protecting the public from harms associated with bad actors seeking to exploit the domain name system."*[23]

ICANN is not well suited to resolve legal questions concerning how the balance of privacy and public interest and legitimate third-party interest rights set forth in the GDPR should be applied to disclosures of WHOIS data that contain personal data. This is reflected in recent correspondence from the ICANN President to the Chair of the European Data Protection Board wherein the ICANN President stated, *"Following ICANN's implementation of new, heightened standards for access to this previously public directory information [i.e., WHOIS data] to comply with the European Union's General Data protection Regulation (GDPR), entities with legitimate interests in accessing this data face challenges in obtaining it. At least part of this issue appears to be uncertainty surrounding how to perform the legitimate interests assessment contemplated in Article 6(1)f of the GDPR."*[24]

Neither is ICANN well suited to resolve other legal questions that relate to the interpretation of the GDPR, such as the application of the GDPR's concept of controllership. This is reflected in recent correspondence from the ICANN President to the Directors General of DG CONNECT, DG JUST and DG HOME, wherein the ICANN President stated, *"The ICANN community develops policies for gTLDs within the boundaries of the law. The community policy development process cannot, nor should it be able to, define, interpret, or change applicable law."* [25]

---

[22] https://www.icann.org/en/system/files/files/gdpr-statement-ec3-europol-icann-proposed-compliance-models-25jan18-en.pdf

[23] See page 122 at https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf Note that in addition to the GAC's Minority Statement, strong Minority Statements were also filed by the At-Large Advisory Committee, the Security and Stability Advisory Committee, the Business Constituency and the Intellectual Property Constituency. All of these groups—part of ICANN's multi-stakeholder community—found the Final Report and its policy recommendations woefully inadequate and not fit for purpose. Nevertheless, the ICANN GNSO Council approved the Final Report and its policy recommendations in October 2020.

[24] https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf

[25] See https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf

Clearly, government action is required to resolve the current situation that the EU, as well as governments around the world, have determined to be unacceptable and contrary to public interest, safety and welfare. ICANN's multistakeholder community has been unable to establish satisfactory or adequate policies that both comply with the GDPR and appropriately support the legitimate interests described above. As a result, the EU that adopted the GDPR is best suited to provide the appropriate balance and clear regulatory requirements to address this situation.

THE CURRENT SITUATION IS DANGEROUSLY OUT OF BALANCE

The current situation with respect to WHOIS data is out of balance. It is harming not only public safety and welfare, but also the privacy of Internet end users themselves. For example, an article in PC magazine recently reported a 350% increase in phishing attacks since the beginning of 2020.[26] Phishing attacks involve not just a violation of privacy, but a malicious stealing of personal data in order to profit bad actors at the harm and expense of end users. The current lack of access to WHOIS data not only impedes investigations of phishing, but of cybersecurity threats of all kinds, including malware and botnets. In describing these challenges, an article about cybersecurity professionals and their work explains, *"the Internet is a public resource, so owners of domain names should be required to register them in a way that makes it simple to see who owns what domain."*[27]

In January 2018, the Commission wrote to ICANN concerning the application of the GDPR to WHOIS data and stated:

"The Commission is well aware that the WHOIS system is currently used by a variety of stakeholders for different purposes, including for achieving public policy objectives (e.g. through identification of contact points for network operators and administrators, help in countering intellectual property infringements, finding the source of cyber-attacks or assistance to law enforcement investigations), as already set out in the ICANN Governmental Advisory Committee's 2007 WHOIS Principles. This reflects the broad general interest missions fulfilled by the Domain Name System and by ICANN as the organisation managing this key resource, in the framework of a multistakeholder process which the Commission supports. We would like to underline the importance of these objectives and the corresponding need to preserve WHOIS functionality and access to its information. The EU Member States have also stressed the importance of ensuring swiftly accessible and accurate WHOIS databases of IP addresses and domain names, so that law enforcement capabilities and public interests are safeguarded." [28](emphasis added)

Unfortunately, these important interests and objectives of preserving WHOIS functionality and access cannot be met by ICANN without clear and explicit EU action. Such government action is both warranted and urgently needed to ensure public interests and the privacy interests of Internet end users are appropriately safeguarded.

---

[26] See: https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine
Wikipedia defines phishing attacks as *"fraudulent attempts to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication."*

[27] https://blog.barracuda.com/2019/01/04/cybersecurity-professionals-lament-losing-of-access-to-whois-database/

[28] https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf

DENMARK AS AN EXAMPLE OF ACHIEVING BALANCE

As stated above, ICANN and its policies and contracts only apply to gTLDS--generic top-level domain names. Country code top level domain names--ccTLDs, such as .be and .dk, are administered independently by the relevant country. Each country determines its own policies with respect to its ccTLD. For example, with respect to the .us top level domain, the WHOIS data for registrants of .us domain names remains publicly accessible in accordance with U.S. policy.

In Europe, Denmark has determined that the public interest in accessible WHOIS data for its .dk ccTLD merits that such information be publicly available, even when the registrant is a natural person. Denmark enacted legislation to require that the name, postal address and phone number of all .dk registrants, with narrow exceptions, be publicly accessible.[29] This is consistent with, and allowed, under the GDPR because EU Member States can determine via legislation or regulation when the public interest in personal data outweighs the privacy interest. All of this was clearly explained in recent correspondence between Denmark and ICANN. In fact, Denmark's letter states that in weighing the privacy interests against other interests that *"[t]he purpose of this provision by the Danish legislators was to establish a high-quality domain with as much transparency as possible. Anyone should be able to find out the identity of a registrant, and thus who is the person behind a specific domain name. The provision should, among other things, help to limit illegal websites as well as harassment on websites, etc., since registrants were not, as a rule, anonymous."*[30] (emphasis added)

In a similar vein, the Commission in its August 2020 Study on evaluation of practices for combating speculative and abusive domain name registrations stated the domain name system *"exists to foster a healthy, functional and trustworthy Internet, but it is not immune to abuse."*[31] Thus the Study recommended, with respect to the .eu ccTLD, that registrars be required *"to carry out strict identification of the registrants' identity, possibly through eID authentication, in order to enter correct and accurate registration data [i.e. WHOIS data] in the .eu registry (such as in .dk)."*[32]

All of the above is consistent with and reinforced by the Commission's own observation that *"security and respect for fundamental rights are not conflicting aims, but consistent and complementary."*[33]

THE URGENT NEED FOR AN EU SOLUTION AND RECOMMENDATIONS

ICANN's policy, which has resulted in the over-redaction and lack of access to gTLD WHOIS data for both governments and legitimate third-party interests, flows directly from its uncertainty while attempting to discern the correction application of the GDPR. Therefore, it is up to the EU to undertake specific and definitive action to correct the situation and right the balance. Even though the gTLD domain name

[29] See Section 18 of the Danish Domain Names Act

[30] See: https://www.icann.org/en/system/files/correspondence/vignal-schjoth-to-plexida-28may20-en.pdf

[31] https://ec.europa.eu/digital-single-market/en/news/study-evaluation-practices-combating-speculative-and-abusive-eu-domain-name-registrations at page 10

[32] Ibid., at page7

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN at p.2

system is global, the ICANN policies that have led to a current situation found to be unacceptable by governments around the world—including the EU Member States and the Commission—and unacceptable to all of the undersigned organisations are a result of ICANN's attempt to conform gTLD policies to the GDPR.

We therefore strongly urge the EU in a forthcoming Directive or Regulation, preferably the Digital Services Act, to do the following:

1. **Adopt a provision similar to that of Section 18 of the Danish Domain Names Act[34] that explicitly recognises the public interest in publicly accessible unredacted WHOIS data for gTLDs (generic top-level domain names) as well as all EU and EU Member State ccTLDs.** From the experience of the undersigned entities, which we understand is shared by law enforcement agencies as well, the three most important elements of WHOIS data that should be made publicly accessible, whether the registrant is a natural or legal person, are (in order of priority): a. the verified email address of the registrant; b. the name of the registrant; and c. the postal address of the registrant. ICANN has maintained a centralised portal for searches of gTLD WHOIS data held by registrars and registries for many years and still does so for the currently non-redacted WHOIS data.[35] Therefore, ICANN as a single, not-for-profit entity can readily assume the public interest responsibility for such a registration directory service for gTLD WHOIS data.[36] The EU has established the public interest in publicly accessible multinational directories before, including the EU trade marks Register. Article 111 of Regulation 2017/1001 on the European Union trade mark establishes the Register of EU trade marks and sets forth in subparagraph (9) that *"All the data, including personal data, concerning the entries in paragraphs 2 and 3 shall be considered to be of public interest and may be accessed by any third party."*[37] We believe the public interest in the elements of WHOIS data identified above are of equal, and perhaps greater importance to public welfare and safety, and therefore public interest, as the data in the EU trade marks Register. Therefore, we strongly urge the Commission to make a similar declaration of the public interest in WHOIS data, as permitted under the GDPR, so that this important data may be accessed by any third party.

2. **In accordance with Article 5(1)(d) of the GDPR, the Commission's Study with respect to the .eu Registry, and "Know Your Business Customer" principles, require that verification and identification be undertaken when WHOIS data for gTLDs and EU and EU Member State ccTLDs is collected in order to ensure its accuracy**.[38] As the GAC recently noted with respect to

[34] See explanation of Section 18 in correspondence between Denmark and ICANN: https://www.icann.org/en/system/files/correspondence/vignal-schjoth-to-plexida-28may20-en.pdf
[35] See: https://lookup.icann.org/
[36] The Commission has previously acknowledged that ICANN acts in the public interest. See: https://mm.icann.org/pipermail/comments-epdp-recs-04mar19/attachments/20190417/6f0a65b2/CommentsontheTemporarySpecificationforgTLDRegistrationDataPolicyRecommendations-0001.pdf
[37] See Article 111(9) at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1001&from=en
[38] See in particular page 7 and pages 39-41 of the Study at: https://ec.europa.eu/digital-single-market/en/news/study-evaluation-practices-combating-speculative-and-abusive-eu-domain-name-registrations Note also that EU Member State ccTLDs, such as .dk, also currently undertake rigorous WHOIS data verification procedures in order to both ensure accuracy and reduce abuse and illegal activity. As noted by the Study "Registrants with bad intentions likely use inaccurate data to hide their identity. Accurate registration data can

data accuracy and the failure of the Final Report to address accuracy with respect to gTLD WHOIS data and the proposed (inadequate) access system, *"failing to provide recommendations aimed at ensuring the accuracy of gTLD registration data, including for the purpose for which it is processed in an SSAD, in light of the systemic inaccuracies highlighted by the RDS-WHOIS2 Review, risks fundamentally undermining the compliance of the system with data protection law."*[39] Therefore, it is important for the EU to ensure that accuracy requirements apply to WHOIS data, as ICANN has not done so in its policy recommendations.

3. **Limit the use of privacy and proxy services to "mask" the identity of domain registrants**. Such services should not be permitted to be used with respect to WHOIS data for any domain name associated with an operational website that either: (i) collects, maintains or stores personal data on the users of or visitors of the website, or on whose behalf such information is collected, maintained or stored, or (ii) engages in commercial activity, which includes offering or directing users to goods or services of commercial value, irrespective of whether such goods or services are of a legal or illegal nature. The Public Safety Working Group of the GAC has found during the COVID-19 pandemic that *"the majority of domains involved in pandemic-related fraud, phishing, or malware have employed Privacy/Proxy Services to hide the identity of the registrant."*[40] According to one Public Safety Working Group member government investigator, 65% of domains referred for investigation for likely abuse used a privacy/proxy service, typically one affiliated with the registrar of the domain name.[41] Privacy/proxy services should not be available to hide the identity of any domain name registrant where the domain name is associated with an operational website engaged in the collection of personal data, commercial activity (legal or illegal), or online abuse.

In recommending this legislative action, we urge the Commission to act upon its judgment about the need for *"hardening of core internet infrastructures and resources, notably the Domain Name System."*[42] (emphasis added) The Commission explicitly acknowledged in its Communication on the EU Security Strategy that access to WHOIS data is *"becoming more difficult"* and that *"legislation may be necessary."*[43] Given the wholly inadequate recent policy recommendations from ICANN concerning WHOIS data access, legislation now clearly is necessary.

Furthermore, by taking the above recommended actions, the EU will strike the appropriate balance between the privacy interests of domain name registrants and the public interest. Indeed, by taking these steps the EU will help to improve the security of the Domain Name System and the Internet, reduce illegal and abusive behaviour and thereby protect not only the safety of end users, but also help protect their personal data as well—a fundamental goal of the GDPR. Moreover, the actions recommended above are simple and straightforward; they provide clear and uniform solutions to a myriad of complicated questions that arise with respect to how the GDPR applies to WHOIS data and the need for access to such data. A number of these complex questions—including those concerning

help law enforcement authorities to identify the domain holders responsible for illegal activities . . . ." (See page 41 of Study)

[39] See: https://gac.icann.org/contentMigrated/next-steps-on-key-policy-issues-not-addressed-in-epdp-phase-2

[40] See: https://gac.icann.org/presentations/icann68-session-8-dns-abuse-slides.pdf and in particular page 14

[41] See page 8 of transcript available at: https://68.schedule.icann.org/meetings/qXuruznZZieKZ52yn#/?limit=10&sortByFields[0]=isPinned&sortByFields[1]=lastActivityAt&sortByOrders[0]=-1&sortByOrders[1]=-1&uid=iAz4vQpCkwvHcRSjc

[42] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN at p.7

[43] Ibid at p.12

controllership, transfers and liability—were recently posed to the Commission in the October 2, 2020 letter from the ICANN President referenced earlier.[44] Undertaking the three legislative actions set forth above would obviate the need for the Commission to respond to those questions and would provide a clear solution in line with the GDPR. The alternative would perpetuate the complexity and uncertainty that is hampering law enforcement and legitimate interests of organisations such as ours, and undermining security online and public safety.

At the present time, when the Commission has noted that *"online dependency has opened the door to a wave of cybercrime"* [45] taking action has become even more urgent. The Europol EC3 Advisory Group on Internet Security was prescient when it stated in January 2018 that removing access to WHOIS data *"will thwart existing cybersecurity mitigation techniques and further empower the ability of cyber attackers to scale their infrastructure with more persistent campaigns."*[46] Earlier this year, the European Parliament asked of the Commission *"will it confirm the need for access to WHOIS as necessary for the public interest?"*[47] We agree with the Parliament that this urgent question must be answered affirmatively and that the Commission should come forward with specific legislative proposals, such as those recommended above, to address adequately the current situation that poses threats to public safety and the privacy of all EU citizens who use the Internet.

This urgent issue is one with respect to which the views of many governments are aligned. We would like to bring to the Commission's attention statements of other governments that reflect the concerns expressed by the European Parliament and other EU institutions. For example, the United States House of Representatives introduced a Resolution earlier this year *"expressing the sense of the House of Representatives that domain name registration information, referred to as "WHOIS" information, is critical to the protection of the United States national and economic security, intellectual property rights enforcement, cybersecurity, as well as the health, safety, and privacy of its citizens, and should remain readily accessible."*[48] Similarly, the G-7 High Tech Crime Subgroup wrote to ICANN in 2019 stating that *"it is of critical importance for the security of the citizens to find a solution which will ensure access to non-public Whois information in order to preserve the investigative capabilities of the G7 members. Supporting investigations related to phishing, malware, ransomware, counterfeit products, child sexual abuse material and terrorism, among other offenses, as well as to facilitate the identification of victims and offenders, goes to the essence of providing domestic security for the citizens of the G7 members. <u>As such, Whois constitutes a key element of online accountability</u>."*[49](emphasis added)

Further, the views of governments and the private sector on the need for a solution are aligned. The Cybersecurity Tech Accord, whose mission is to promote a safer online world by fostering collaboration among global technology companies committed to protecting their customers and users and helping them defend against malicious threats, has a membership that consists of over 100 leading technology companies. In a recent post, the Cybersecurity Tech Accord stated with respect to the lack of access to WHOIS data *"that cybersecurity professionals, in the private sector and the law enforcement community have started wondering whether they will ever be able to rely on this tool again . . . and finds the rising*

[44] https://www.icann.org/en/system/files/correspondence/marby-to-viola-et-al-02oct20-en.pdf
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN at p.3
[46] https://www.icann.org/en/system/files/files/gdpr-statement-ec3-europol-icann-proposed-compliance-models-25jan18-en.pdf
[47] See: https://www.europarl.europa.eu/doceo/document/E-9-2020-000826_EN.html
[48] See H.Res. 875 at: https://www.congress.gov/bill/116th-congress/house-resolution/875
[49] See: https://www.icann.org/en/system/files/correspondence/green-to-chalaby-21jun19-en.pdf

number of domain and DNS threats to be a systemic problem that needs broader oversight."[50] We very much agree and therefore strongly urge the Commission to take action.

In conclusion and to emphasise the importance of these issues, we offer the following intervention from a Swedish police officer made during a public forum at the ICANN63 meeting held in October 2018:

"Good afternoon. My name is Per-Ake Wecksell. I work for Swedish National Police. I'm dealing with online sexual child abuse. I have used the WHOIS since I started this topic in 2006. It's an important tool -- has been an important tool for me to find children and also perpetrators on the Internet. We have gathered some information from WHOIS to find these kids who actually today are being raped. So we have a timeline to cross. We have to find those kids, find those perpetrators. Because of the GDPR, the WHOIS went dark and it takes more time now to send out requests to the registrars and hopefully get some information back. And we really need timely access to WHOIS. . . . Because every day and as we are sitting here, children are being raped."[51]

We hope Officer Wecksell's grave words will remind the Commission that these issues have real life consequences that warrant attention and action.

[50] https://cybertechaccord.org/whois-the-process-grinds-forward-sort-of-no-relief-for-cybersecurity-pros-is-in-sight

[51] See: https://static.ptbl.co/static/attachments/191802/1540245466.pdf?1540245466
Pages 9-10