To: Article 29 Working Party
From: ICANN's Intellectual Property and Business Constituencies
Date: February 1, 2018
Re: GDPR and WHOIS

Summary

The Intellectual Property Constituency (IPC) and the Business Constituency (BC) of the ICANN community are writing to the Article 29 Working Party regarding the upcoming May 2018 effective date of the General Data Protection Regulation (GDPR). In light of previous correspondence between the Article 29 Working Party and ICANN,[1] and the Article 29 Working Party's invitation to enter into a dialogue to discuss data protection issues affecting the WHOIS database, we wanted the Article 29 Working Party to understand the importance and utility of the WHOIS database and the IPC and BC perspectives when crafting any guidance.

We read with interest the "**Rules for businesses and organisations**" published by the EU on 24 January 2018, but did not observe any guidance regarding business access to WHOIS data.[2] In the hope that the EU will soon publish specific guidance for WHOIS compliance with GDPR, we offer this document with suggestions in connection with this anticipated guidance. In this way, the EU can help ICANN preserve aspects of the current WHOIS system for legitimate consumer protection and cybersecurity purposes by authorized organizations and individuals while also complying with GDPR.

Access to WHOIS is and has been critical for consumer protection, Internet security, law enforcement and other related functions.[3] We note and greatly appreciated the European Commission's 29 January letter to ICANN which provides more direct input regarding GDPR compliance and WHOIS access.[4] As the Commission noted, "the WHOIS system is currently used by a variety of stakeholders for different purposes, including for achieving public policy objectives" such as identification of contact points for network operators and administrators, help in countering intellectual property infringements, and finding the source of cyber-attacks or assistance to law enforcement investigations.[5] Without such access, consumers, the general public and governments will face much higher rates of online and offline crimes, frauds and other abuses. Fake news, financial scams, sales of illegal contraband, and other serious societal harms will be much harder to stop.

---

[1] *See* the Article 29 Working Party's December 11, 2017 letter to ICANN, ICANN's January 15 response, and the January 29, 2018 letter from the European Commission to ICANN.
[2] *See* European Commission, Rules for Businesses and Organizations (Jan. 24, 2018), available at https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations_en.
[3] See the Appendix to this letter for a list of non-exhaustive use cases for WHOIS data.
[4] *See* European Commission, Letter from Dimitris Avramopoulos, Věra Jourová & Sir Julian King to Göran Marby, *available at* https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf (the "January 2018 EC letter").
[5] January 2018 EC letter.

Accordingly, we hope to clarify the balance between the GDPR's privacy requirements and the limited legitimate needs for access to WHOIS data.

The purpose of this communication, therefore, is to: 1) reiterate and explain the types, scale and impact of threats that Internet users face, 2) show examples of the use of WHOIS for legitimate protection purposes in order to mitigate these threats, 3) demonstrate that a robust WHOIS is possible while protecting privacy specified by the GDPR, and 4) provide the Article 29 Working Party, and individual Data Protection Authorities who participate, practical input on how the public interest functions of the WHOIS system can be preserved while ensuring the system complies with the GDPR.

Thank you for taking the time to consider our concerns and suggestions.

Contents of this document:

About the IPC and BC:

The Intellectual Property and Business Constituencies (IPC and BC) are representative bodies charged with addressing the interests of global rights holders and business users, respectively, as they relate to domain name activity. Our constituencies are participants in the bottom-up, multi-stakeholder governance work of ICANN, the technical coordinating body for the global Domain Name System ("DNS").

WHOIS, Internet Security, and Consumer Protection

The WHOIS system is ingrained in the processes of Internet security and consumer protection, which are consequential functional requirements of online business, as well as other non-commercial online activity. Internet economic activity is significant: global business-to-consumer e-commerce sales reached an estimated USD $2.3 trillion in 2017.[6] Consumers making purchases through e-commerce operate under a system of trust: they must trust that they are visiting legitimate websites and that they are purchasing authentic goods and services. In the event that consumers are defrauded, it is important that a system be in place to help identify the bad actors and pursue available remedies.

People focused on network defense are tasked with ongoing risk assessment and mitigation of various online threats. Because domain names are fundamental to the operation of the Internet,

[6] *See* Aaron Orendorff, Global Ecommerce Statistics and 10 International Growth Trends You Need to Know (Sept. 11, 2017), *available at* https://www.shopify.com/enterprise/global-ecommerce-statistics.

they factor into nearly every attack. Security teams must closely analyze domain name registration data to know if an alert represents a credible threat. Applied at scale, risk assessment of domain names using registrant data can identify a signal from noise and bring to the surface otherwise unknown attacks early in their lifecycle. Much of the network security and threat intelligence context for WHOIS data necessitate high volume access to aggregated or centralized data sets, something we encourage the Article 29 Working Party to consider in its advice to ICANN on this critical issue.

Domain names are the navigational fulcrum of the Internet. In investigating difficulties with these pivotal resources, the WHOIS service allows people to find out "who is" the owner of a domain name, plus important details about its registration and history in the DNS. This information allows businesses, consumers, consumer protection agencies, law enforcement, and others to understand not only with whom they are doing business, and receiving information or solicitations, but in instances of unfortunate harm, to identify the party behind abusive behavior and use that information to pursue a variety of remedies.

The barriers to entry for domain name abuse are already quite low. Domain names can be registered in bulk for USD $10 or less, and abusive actors can wreak considerable damage with minimal investment. Contrast this with the fact that disabling or recovering a single infringing domain name can cost thousands of dollars in dispute resolution and legal fees.

The group calling itself the Iranian Cyber Army that has been known for committing espionage, sabotage and political repression had many of its exploits uncovered and disabled through investigations enabled by Whois research.[7]

Accurate and accessible WHOIS data is an indispensable part of any solution to addressing these issues.[8] For example, WHOIS data grants those who are victims of infringement or investigating fraud the ability to reach out to the unauthorized party directly, file a complaint to recover or disable an infringing domain name, report the activity to consumer protection and regulatory agencies, and more.[9] Without appropriate access to WHOIS data, enforcement would become not only more expensive and time-consuming, but in many cases impossible. The cost of cybercrime is already projected to reach USD $6 trillion by 2021.[10] Lack of a reliable, accessible database to identify criminals and bad actors could very well accelerate those costs.

---

[7] Domain Tools, From Cybercrime to Political Repression, Shedding Light on the Iranian Cyber Army (Jan. 9, 2018), *available at* https://blog.domaintools.com/2018/01/from-cybercrime-to-political-repression-shedding-light-on-the-iranian-cyber-army/.
[8] See the Appendix to this letter for a list of non-exhaustive use cases for WHOIS data.
[9] *See, e.g.*, tneogi, Experiments on Fake News detection and prevention (May 7, 2017), *available at* https://medium.com/@tneogi/experiments-on-fake-news-detection-and-prevention-713438356f39.
[10] *See* CSO Online, Top 5 cybersecurity facts, figures and statistics for 2018 (Jan. 23, 2018), *available at* https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html?nsdr=true.

Harmful online activity often occurs on a large scale, affecting numerous Internet users at once. In one well-known example, a hack of Yahoo email accounts affected approximately 500 million users.[11] In this specific example, WHOIS data was used to help identify one of the key participants in the attack and enumerate additional infrastructure that was possibly used in similar attacks against other email services. In these instances, the ability to obtain bulk and historical WHOIS data, and to rapidly analyze it, enables investigators to connect the dots between individual websites or instances of infringement or fraud and tie them to an individual domain name registrant. This facilitates much more rapid and complete takedown of networks of harmful online activities. Further, the more data fields available in WHOIS, the more likely an investigator is able to quickly address a potential or unfolding harm. For example, in a recent case, a network of bad actors who had compromised users' Windows machines were not able to be identified through IP address alone; domain information was required.[12] Criminals and other malicious actors are becoming increasingly sophisticated in their use of constant, global, and mass-scale automation techniques to perpetrate their nefarious schemes; the parties – both in the public sector, and to a massive degree, in the private sector – who prevent, detect, and remediate these harms also require such tools, and WHOIS is a key tool in their toolbox.

Marcus Hutchins, once lauded for stopping WannaCry, was revealed as the author of vicious malware and brought to justice via WHOIS research after having victimized millions.[13]

These remedies are necessary because the consequences of misleading and fraudulent activity on the Internet can be quite dire for consumers. For instance, if consumers purchase pharmaceuticals on the Internet that turn out to be counterfeit, the results could be deadly: the medication may not contain the ingredients necessary to address a critical health issue, could contain incorrect dosages, or could contain impurities, even poisons, that could lead to death.[14] The harm, naturally, is not limited to pharmaceuticals:

- Counterfeit automotive parts have malfunctioned, leading to deadly accidents or failing to deploy and protect drivers.
- Counterfeit electronics have exploded and caught fire, putting users at risk.
- Counterfeit furniture (for example, baby cribs) have not met safety requirements, and led to injuries and deaths.
- Counterfeit household products (for example, cleaning products or baby formula), have not met safety requirements, or were formulated incorrectly, or even contained harmful or poisonous impurities.

---

[11] *See* Brian Krebs, Four Men Charged with Hacking 500M Yahoo Accounts (Mar. 15, 2017), *available at* https://krebsonsecurity.com/2017/03/four-men-charged-with-hacking-500m-yahoo-accounts/. The article amply demonstrates the value of WHOIS data in delineating the scope of this criminal activity, and presumably in investigating it in the first place.
[12] *See* Krebs on DomainTools: A closer look at the Terracotta VPN Research (Aug. 15, 2015), *available at* https://blog.domaintools.com/2015/08/krebs-on-domaintools-a-closer-look-at-the-terracotta-vpn-research/
[13] *See* "Who Is Marcus Hutchins?", *available at* https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/
[14] *See* BBC News, Counterfeit drugs: 'People are dying every day' (Sept. 27, 2016), *available at* http://www.bbc.com/news/business-37470667.

- Consumers who believed they were making charitable donations actually were transferring funds to bad actors, including terrorist groups and other large-scale criminal enterprises.
- Illegitimate sites also captured consumers' credit card details and other banking information when making purported sales, which led to wide-scale identity theft. Many scams even target consumers who are seeking romantic connections.[15]

Consumer protection and related regulatory agencies use the WHOIS database to conduct investigations regarding potential bad actors, and stop fraud and deception. Such agencies use WHOIS as a tool in taking down organized networks of fraudsters operating websites selling illicit products or seeking to steal credit card information. The data is also used to identify proper parties for service of legal process in the context of lawsuits or regulatory and administrative actions. Investigative journalists are also users of WHOIS data, which further aids the public's interest in exposing fraud and other harms.[16]

Access to WHOIS is also used to protect individuals' privacy. Since most Internet services use domain names, WHOIS provides the means to identify online data controllers at scale, and enables common tools to proactively block third-party tracking and blacklist domain names involved in abuse. For example, "over 1 in 10 people use browser plugins or built-in browser features which block certain forms of third party tracking." [17]

Access to WHOIS data also allows businesses and intellectual property owners to proactively engage in enforcement against unauthorized third parties, often before extensive harm is caused to consumers. Without the ability to access WHOIS, businesses would be challenged to develop and implement sophisticated enforcement programs. Such programs can prevent, or greatly reduce, the loss of goodwill and harm to finances, health, democracy, and even life itself that can result from bad actors on the Internet. While it is important for individual consumers who have been defrauded to be able to make complaints and seek restitution, it is equally important for the companies whose users are being harmed to be able to address bad actors before their customers fall victim to fraud. But all such efforts depend significantly on access to WHOIS data.

In addition to the examples above, WHOIS data can be used to investigate other online schemes and fraud involving brand names (such as email phishing, where an unauthorized third party uses a brand name in a text, app or email address to convince the recipient to inappropriately share personal or payment information). For example, a recent phishing campaign targeted users of the electronic document signature service DocuSign, and

---

[15] *See* HuffPost, How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts (July 20, 2017), *available at* https://www.huffingtonpost.com/entry/romance-scams-online-fbi-facebook_us_59414c67e4b0d318548666f9.

[16] For examples of reporting that relied at least in part on WHOIS, *see, e.g.*, http://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/index.html and http://money.cnn.com/2017/10/25/media/itl-green-floid-cloudflare-russian-sites/index.html.

[17] *See* Public comment to ICANN from Reuben Binns, Max Van Kleek, Jun Zhao, Nigel Shadbolt, Tim Berners-Lee, et al (Jan. 29, 2018), *available at* https://www.icann.org/en/system/files/files/gdpr-comments-binns-et-al-icann-proposed-compliance-models-29jan18-en.pdf

aggregated data was used to identify and take down the bad actors.[18] The data is also used to identify proper parties for service of legal process in the context of civil litigation. In a similar vein, the data is used by providers of domain name dispute resolution services (such as the UDRP) to confirm the appropriate domain name registrant was named in a complaint, as well as to notify the registrant of the action. A report by the Digital Citizen's Alliance highlighted the danger to Internet users from websites that use infringing copyrighted material to spread malware, noting that visitors to such sites are 28 times more likely to get malware from a content theft site than from similarly-visited mainstream websites or licensed content providers.[19]

The utility of the WHOIS system is wide-ranging and significant.

One of the world's largest malicious botnets, Siren, was disabled with the help of WHOIS data. This Botnet generated 90k Twitter accounts and created 8.5M posts, driving 30M clicks using pornographic material as bait to sting victims via romance scams - each incident costing victims up to $100K.[20]

WHOIS data has other legitimate, practical business uses as well. Businesses of all sizes, as well as individual consumers, use the WHOIS database to resolve e-commerce issues, including finding an appropriate contact point for an online supplier, distributor, or retailer (if information is not available directly on the website or e-commerce platform). WHOIS serves as an important back-up resource if a consumer-facing website is temporarily down, bringing it back online by alerting the website operator or online service providers, or to identify appropriate customer support. WHOIS serves a key transparency function by providing a means for businesses and consumers to find out who operates a domain or website, as well as the online service providers who are connected to the website (such as the registrar and hosting provider), and provides basic information necessary for Internet users to take steps to protect themselves against malicious and unlawful activity, including to refer complaints to the relevant enforcement authorities.[21] The ability to locate this information and to engage in these activities contributes to the trust necessary to maintain a functioning e-commerce system. WHOIS data is often necessary for individual consumers to file reports with consumer protection agencies, which often rely on tips and reports such as these from consumers to do their work.

---

[18] *See* Hunting the Phish: What We Can Learn from the DocuSign Malspam Campaign (May 19, 2017), *available at* https://blog.domaintools.com/2017/05/hunting-the-phish-what-we-can-learn-from-the-docusign-malspam-campaign/

[19] *See* Digital Citizens Alliance, Digital Bait: How Content Theft Sites and Malware Are Exploited by Cybercriminals to Hack Into Users' Computers and Personal Data (Dec. 2015), *available at* http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/digitalbait.pdf.

[20] *See* ZeroFOX Research, Inside the Massive SIREN Social Network Spam Botnet (July 16, 2017), *available at* https://www.zerofox.com/blog/inside-massive-siren-social-network-spam-botnet/.

[21] Many law enforcement authorities are reluctant to commence an investigation of allegedly abusive or unlawful activity without an indication that they have jurisdiction over the source of that activity, which requires certain basic information, including geographic location of the registrant of the domain.

The Future of WHOIS in Consumer Protection

The Charter of Fundamental Rights of the European Union (the "Charter") recognizes that "Union policies shall ensure a high level of consumer protection." *See* Charter, art. 38. The Charter also recognizes fundamental rights to security, to operate a business, to protect intellectual property, and to access services of general economic interest. *See* Charter, arts. 6, 16, 17, and 36. These rights must be balanced against the right of personal data protection, *see* Charter, art. 8, as well as duly considered in the context of enforcing the GDPR, which is designed to implement the fundamental data protection right.

If registrars and registries were unable to continue to collect and make appropriately available domain name registrant data, the critical functions enabled by the WHOIS service – and thus a reasonable level of consumer protection – would be severely curtailed. This also would run contrary to the GDPR principle of data accuracy, as it would be necessary to collect and disclose certain data in order for entities to file complaints regarding its inaccuracy and request that inaccurate data be rectified. *See* GDPR, art. 5(1)(d). This element is vital to an accountable WHOIS system, and more broadly to an accountable domain name system and online marketplace.

As the European Commission correctly pointed out in its 29 January 2018 letter to ICANN: "the WHOIS system is currently used by a variety of stakeholders … 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."[22] The Commission underlined the importance of these objectives and the corresponding need to preserve WHOIS functionality and access to its information. Importantly, the Commission highlighted that the GDPR is not intended to create additional burdens for business operators (such as registries and registrars), and that these rules are flexible and can be implemented in a manner that accommodates continued WHOIS data access as discussed here.

Applying GDPR to WHOIS

Having established the importance of the WHOIS system, we note that the GDPR, by its language, supports a WHOIS system that can continue to make certain personal data publicly available, with the balance of personal data accessible through a tiered or layered system that offers natural persons the protections required under GDPR while making access available for the legitimate purposes described above.

GDPR recognizes several valid grounds for processing WHOIS data:

[22] *See* January 2018 EC Letter (citing the GAC's 2007 WHOIS Principles, which are available at https://gacweb%2Cicann.org/download/attachments/28278834/WHOIS_principles).

Public Interest

The security and stability of the Internet depends upon the ability of individual Internet users, consumers, and businesses to supplement the important work done by law enforcement and consumer protection agencies, which promotes the public interest. The current WHOIS system handles millions of queries daily. Even under normal circumstances, such as situations not involving legal process or related investigations, registries and registrars would be inundated with requests for the contact information of domain name registrants (regardless of whether they approve the requests). Without a "self-help" mechanism like WHOIS, individuals and organizations would turn to registries and registrars for processing requests – the potential volume of resulting requests not only would fail to scale and meet the global consumer protection and cybersecurity needs, it would clearly drive drastically upward the costs of the most basic of registry and registrar functions and services, and overwhelm the current system. Similarly, any variant of a tiered access system that depends upon obtaining court orders in order to access the actionable information needed to investigate and rectify abusive behavior risks inundating the judicial system, needlessly squandering limited public resources, and would move too slowly to address a majority of abuse.

Article 6(1)(e) GDPR states that data processing is lawful if it is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Article 6(3) requires that this basis be pursuant to Union or Member State law to which the controller is subject. There are existing laws and official policies that establish both that publicly posting WHOIS data is carried out for the public interest or in the exercise of official authority vested in the controller, and that EU or Member State law necessitates publicly posting certain WHOIS data.[23] The EU Member States through the Council 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."[24]

Domain name registration records are akin to land records in this regard: certain personal information, including name and address, must be collected and made publicly available to both effectuate the purchase of real property and record the ownership right. This allows the property owner to defend against challenges to his or her title and serves the broader public interest by simplifying future land transactions and preventing unlawful disposal. Similarly, appropriate access to WHOIS data also protects the registrant's personal identity or personal brand, and reduces confusion over who owns and operates a website (for consumer inquiries, government investigations, etc.). Domain registration has multiple defensive and offensive purposes in the public interest that protect all parties involved, not the least of which is the domain name registrant her/himself.

[23] *See e.g.,* Regulation (EC) No. 733/2002, Rec. 12 and Art. 4(2); .FI (Finland) Domain Name Act (Feb. 28, 2003), *available at* https://www.finlex.fi/en/laki/kaannokset/2003/en20030228.pdf.
[24] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 14435/17 (Nov. 20, 2017).

Legitimate Interests

Article 6(1)(f) GDPR states that data processing is lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data." Data controllers and processors must take into consideration the reasonable expectations of data subjects,[25] who are informed at the time of registration and throughout the term, of the registrant's obligations related to WHOIS. Further, Recital 47 notes that processing of personal data necessary for preventing fraud is one example of a legitimate interest.[26]

We recognize that these legitimate interests must be weighed against the fundamental rights and freedoms of the data subject which require protection of personal data. However, it is in registrants' best interests to have public proof of their ownership of a particular domain, particularly given the speed and frequency with which Internet domains are threatened by hackers, fraudsters, and other hostile third parties. The balancing of legitimate interests to protect a safe, secure and reliable Internet ecosystem with the fundamental rights of certain EU natural persons who are registrants tips the scale towards legitimate interests in this context.

The Governmental Advisory Committee of ICANN (the GAC) cites EU law in their comments that state "EU law recognizes the public's legitimate interest in the security of the Internet and its essential infrastructures such as registry and registrar services… This is also a legitimate interest in public access as cyber security professionals including but not limited to computer emergency response teams (CERTs), rely on publicly available WHOIS data to quickly identify and respond to threats to the DNS."[27] Both the longstanding 2007 GAC WHOIS Principles and the GAC's re-affirmation of them (both representing the consensus views of governments) are valuable indicators of the breadth of legitimate interests that are served by appropriate access to WHOIS data. Excerpts from other input provided to ICANN by governmental agencies and international organizations are included in the Appendix below, further underscoring the public interest and legitimate purposes served by WHOIS.

Performance of Contracts

Article 6(b) of the GDPR states data processing is lawful if it is "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract." The WHOIS-related provisions of contracts for the

[25] *See* GDPR, Recital 47.
[26] Many other examples of recognized legitimate interests are cited in the Appendix, and the Article 29 Working Party has itself affirmed a number of such interests in the past. *See, e.g.*, Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC (WP 217) at 29 (Apr. 9, 2014) (recognizing as one such legitimate interest pursued by a third party combatting "illegal file sharing online"), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[27] *See* GAC Feedback on Proposed Interim Models for Compliance (Jan. 29, 2018), *available at* https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf.

registration of domain names are necessary for the performance of the contract, in order to have a safe, secure, and reliable Internet ecosystem.

It has been well established since ICANN's formation in the 1990s that publicly available domain registrant data is essential for the proper functioning of the Internet ecosystem and its various transactions.[28] ICANN's oversight over the domain name system is dependent on a series of contracts that enables the various parties (registries, registrars, and registrants) to register domain names. This self-regulatory framework, which was contemplated from the very inception of the domain name system, requires these parties to participate in a WHOIS system to ensure accountability and transparency of the system, and ensure the contactability of registrants and administrative and technical support for each registration in order to resolve issues such as those identified above related to the domain name. In adopting GDPR, the EU regulators surely did not intend to dismantle the consumer protection and related benefits of the WHOIS system, and adversely affect the self-regulatory system that has enabled the Internet to flourish globally.

Consent

ICANN requires registrants to consent to the usage of their personal data in WHOIS. Article 6(1)(a) GDPR recognizes consent as a valid ground for data processing, if it is freely given, specific, informed and unambiguous, and can be freely withdrawn. Consent could be provided whereby EU natural persons could allow their personal data to be publicly available, even if there is a layered approach to accessing personal data generally. With regard to WHOIS, registrants have the ability to freely consent to the publication of their data, or in the alternative, can chose to register through a privacy or proxy service which enables the registrant to mask their personally identifiable information and replace it with the information of the privacy or proxy service (a legal entity which supplies non-personally identifiable contact information). This is consistent with GDPR (Recitals 28-29, Article 6(4)(e)) which recognizes that pseudonymisation can reduce the risks to the data subjects concerned, and help controllers and processors to meet their data-protection obligations).

[28] *See, e.g.*, US Department of Commerce, Improvement of Technical Management of Internet Names and Addresses; Proposed Rule, pg. 8829 (Feb. 20, 1998), *available at* https://www.ntia.doc.gov/federal-register-notice/1998/improvement-technical-management-internet-names-and-addresses-proposed-. This foundational document for the creation of ICANN addressed the need for a public domain registry as it related to trademark disputes, stating "the job of policing trademarks could be considerably easier if domain name databases were readily searchable through a common interface to determine what names are registered, who holds those domain names, and how to contact a domain name holder."

APPENDIX

The Consumer Protection and Internet Security Utility of WHOIS

The WHOIS database is vital in its utility, to support to support a safe, secure and reliable Internet ecosystem. Following is a non-exhaustive recital of use cases from WHOIS users to demonstrate the broad applicability of the database:

Purpose	***WHOIS Data Use***
Investigate trademark/brand infringement and enforce trademark rights	• Enable contact with relevant parties • Identify fraudulent use • Collect registration history • Send cease and desist letters • Contact registrant/providers whose services are being used to infringe IP • Determine whether similar domains are owned by the same entity • Detect anonymization services
UDRP Resolution	• Verify allegations in UDRP filings • Verify contact information
Consumer protection	• Contact service providers whose services are being used to infringe IP • Contact registrant for resolution • Determine patterns of abuse by same entity • Source contact data for online retailers and others
Evaluation of claim merits	• Investigate likely effectiveness of administrative and legal actions • Determine dates of a mark's first use • Determine dates of a mark's abandonment
Civil litigation	• Identify and confirm other domains used in connection with defendant(s) alleged IP infringement
Digital crimes investigation	• Disrupt cybercrime • Combat piracy • Verify identity of advertisers • Protect against inauthentic news and information
Abuse investigation and prevention	• Investigate fraudulent activity • Investigate malware incidences • Customer vetting • Map bad actors/search for known or prospective inappropriate users • Whitelist email delivery services

Purpose	***WHOIS Data Use***
SSL certificate administration	• Validate domain name ownership for SSL certs
Security operations analysis/research	• Research unusual registration behavior • Reverse queries to determine infrastructure of abusive campaigns • Document evasive or unusual registration behavior • Look for signs of known threat actors • Provide scalable and unified interface for customer queries
Contractual compliance	• Access registration data for assisting ICANN's enforcement of contractual obligations
Registry/registrar functions	• Facilitate registrations, transfers, renewals, deletions • Facilitate domain portfolio management
Facilitate/respond to third party inquiries	• Make WHOIS data available
Conduct business due diligence for merger, spinoff or audit	• Conduct due diligence to verify domain names and status • Perform internal audits for domain portfolios
Domain name offers	• Evaluate acquisition options and identify current registrant(s)
Borrower credit / lender due diligence	• Conduct due diligence to verify domains registered and status
Hijacking prevention	• Interact with registrars to prevent hijacking
Reputation management	• Value and score data related to domain names
Technical issue resolution	• Find appropriate contact information for addressing technical issues
Business and product identification	• Determine name availability for registration • Domain name brokering and acquisition • Asset verification
Fake news	• Identify trustworthiness of the news source based on the identity of the registrant

Selected Excerpts from European-Based Governmental and International Organizations' Submissions to ICANN

Several European-based governmental and international organizations have submitted comments to ICANN expressing the importance of continued access to WHOIS data:

Commenter	***Comment Excerpts***
ICANN Governmental Advisory Committee (GAC)	Public access to (limited) WHOIS data (including Registrant name and address) should be maintained to the extent possible and only complemented by layered access where required, and; Other EU mandated public registries demonstrate that the EU has considered it a public interest to keep a public record of the owners of EU trademarks, company registers, and domains in EU ccTLDs and hence "implicitly stated that such interests overrides the interests or fundamental rights and freedoms" of the individual. ICANN should implement GAC advice, including "to maintain a WHOIS system that keeps "WHOIS quickly accessible to the public (including businesses and other organizations) for the legitimate purposes, including to combat fraud and deceptive conduct, to combat infringement and misuse of intellectual property, and to engage in due diligence for online transactions and communications." This includes the needs of UDRP and URS providers who should be considered as having a legitimate interest in access to any non-public WHOIS elements necessary to ensure due process. "
National Crime Agency (UK)	The NCA succeeds in reducing the impact of cybercrime by effective collaboration with a range of partners, including industry. The NCA receives a significant proportion of cyber intelligence from industry partners; many of whom use WHOIS data to inform their own internal cyber security investigation. They are legitimate users of WHOIS data who through Section 7 of the 2013 Crime and Courts Act, greatly enhance the NCA's threat picture and enable the NCA to focus its resources on reducing the harm to individuals and businesses in the UK- a proportionate and risk-assessed approach. In addition, law enforcement makes use of industry produced tools, which enable sophisticated interrogation of the WHOIS data. Without these tools, the investigators would find WHOIS datasets difficult to query and bulk queries would be very time consuming. Both industry and academic partners are legitimate users of WHOIS lookup data. In restricting the data to law enforcement access only, the power to protect internet users falls only to law enforcement agencies. Not only would the volume OFFICIAL be unmanageable, it would also remove many organisations' ability to protect themselves from cybercrime, meaning the number of crime victims may rise exponentially.
European Cybercrime Centre (EC3) Advisory	The international Whois protocol plays a critical role in identifying malicious infrastructure and thus defending against or preventing attacks. Accessing Whois registrant information is an essential element of the

Commenter	*Comment Excerpts*
Group on Internet Security – Europol	cybersecurity community's efforts to maintain the overall security and stability of the global Internet, and any loss of access would seriously degrade these efforts. Most cybersecurity investigations, or technical processes determining the safety of domain names, rely upon 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.
Council of Europe Cybercrime Convention Committee	An ICANN WHOIS policy should state clearly that WHOIS serves "important reasons of public interest". These include, inter alia, public safety and the investigation of crime. This public interest in open access to WHOIS data may override data protection rights of individuals.
Council of Europe Bureau of the Committee of Convention 108	The limited publication of WHOIS data can serve the legitimate interests of the controller and it should be added that it could also serve important public interests. The publication however has to serve a specific and predefined purpose and has to be necessary and proportionate to the fulfilment of this purpose.