U.S. CHAMBER OF COMMERCE

About the ICANN WHOIS Database

ICANN's WHOIS database is an important tool in retrieving information around domain name ownership that has been available to law enforcement, intellectual property owners, security researchers, domain name owners, and other types of Internet users for over two decades. The database plays an indispensable role in ensuring good governance, accountability, and transparency for the Internet. Legitimate public access to the database has proven crucial to effectively identify, prioritize, and allocate resources to the policing of malicious and unlawful activity on the Internet.

The database allows access to critical information that helps identify and address malicious or fraudulent online activity, such as finding and taking down websites that are involved in cyber theft or sell counterfeit goods that could risk the health and safety of consumers. Some examples of the legitimate interests served by keeping WHOIS data public:

- Public Health and Safety (e.g., combatting online sale of dangerous counterfeit medications)
- Child Abuse (e.g., combatting online trafficking of child abuse images)
- Consumer Protection (e.g., combatting online scams)
- Intellectual Property Protection (e.g., combatting online piracy and counterfeiting)
- Cybersecurity (e.g., combatting phishing, malware, ransomware, identity theft)
- Stability and Security of Internet (e.g., combatting distributed denial of service attacks, bot nets, data breaches)

WHOIS Database and the EU General Data Protection Regulation (GDPR)

Oversight of the protection and use of personal data is both prudent and necessary in today's economy. However, the General Data Protection Regulation (GDPR) has created an unintended consequence that poses serious questions around the governance, transparency, and accountability of the Internet.

In particular, GDPR in Article 5 lays out criteria under which this personal data can be collected and processed, and the interpretation by the Article 29 Working Party (WP29) has put the WHOIS database at risk. The WP29's feedback indicated that "ICANN and the registries would also not be able to rely on a legitimate interest for making available all personal data in WHOIS directories to the general public".

ICANN has been working with the WP29 to create solution by May 25 that will allow legitimate access to the database while bringing it into compliance with GDPR. However, it is unlikely that any solution will be finalized in time, and ICANN's Proposed Interim Model does not adequately preserve access to necessary information in the database.

The WP29 has not as of yet granted ICANN's request for a one-year extension on compliance. In the meantime, many registries and registrars are taking preemptive action to limit the information on and access to their WHOIS services.

Industry Concerns

- **The database could "go dark" on May 25.**

  If access to the database is eliminated on May 25 this will have a detrimental impact on public safety, and the security and stability of the Internet. There will be a significant rise in cyberattacks and fraudulent online activity because law enforcement, cyber researchers and professionals, companies, or consumers will be significantly constrained in their ability to respond or remedy. An assurance of forbearance of enforcement or an interim "self-certification" solution, preserving this access to qualified users with appropriate safeguards, is necessary.

- **Access to the database could be limited.**

  The Proposed Interim Model creates an accreditation program for access to non-public WHOIS data. Limiting access to the database will make it impossible for those with a legitimate purpose to use data to do so. For example, it is not clear if a licensed attorney will be able to obtain accurate WHOIS data, which will make it increasingly difficult for an entity seeking to identify a malicious actor.

- **The information on the database could be limited.**

  The Article 29 Working Party has called for limitations around the data held within the database, in particular masking contact information such as an email address. It also appears that many registries and registrars are planning to restrict access.

  If names and contact information for all registrants from the database are removed, this will make it more difficult to research the history and ownership of domain names to pursue legal remedies for cybersquatting, security breaches, or other domain name misuse. Registrants that are legal entities should remain publicly accessible and, consistent with GDPR, should not be treated the same as those that are natural persons.

- **Registries and Registrars could apply GDPR globally.**

  Considering the EU makes up only 10% of global population, over-compliance with the GDPR by applying it to all information in the WHOIS database is not recommended. This would further limit access to WHOIS data and create unnecessary risks to the security and stability of the Internet as well as consumers.

- **Europe could become a haven for cyber criminals.**

  An unintended consequence of GDPR could be an increase in fraudulent domain name sales in Europe. Restricted access makes it more difficult to confirm proper ownership of a domain name. Limited information on the database will make it more difficult to track down malicious and fraudulent actors.