The impact of GDPR on WHOIS: Implications for businesses facing cybercrime

Received (in revised form): 13th July, 2018

Anthony J. Ferrante
is a Senior Managing Director and Global Head of Cybersecurity at FTI Consulting. He is based in Washington, DC in the Global Risk & Investigations Practice (GRIP) of the Forensic & Litigation Consulting segment. Anthony is considered an expert in cyber resilience, response and remediation services. He has more than 15 years' top level cyber security experience, providing incident response and preparedness planning to more than 1,000 private sector and government organisations, including over 175 Fortune 500 companies and 70 Fortune 100 companies. Prior to joining FTI Consulting, Anthony served as Director for Cyber Incident Response at the US National Security Council at the White House, where he coordinated US response to unfolding domestic and international cyber security crises and issues. Building on his extensive cyber security and incident response experience, he led the development and implementation of Presidential Policy Directive 41 — United States Cyber Incident Coordination, the federal government's national policy guiding cyber incident response efforts. Before joining the National Security Council, Anthony was Chief of Staff of the FBI's Cyber Division. He joined the FBI as a special agent in 2005, assigned to the FBI's New York Field Office. In 2006, Anthony was selected as a member of the FBI's Cyber Action Team, a fly-team of experts who deploy globally to respond to the most critical cyber incidents on behalf of the US Government.

Global Risk & Investigations Practice, FTI Consulting, USA
Tel: +1 202 312-9165; E-mail: ajf@fticonsulting.com

Abstract To protect privacy rights, the European Union's General Data Protection Regulation (GDPR) has been effectively blocking access to the personal information of individuals who register Internet domains. Prior to the May 2018 GDPR enforcement deadline, this information was available through WHOIS, the directory service maintained by the ICANN, the organisation that manages the global domain system. By preventing access to this information, GDPR is depriving cyber security professionals of data that is vital for fighting a variety of Internet-based crimes. ICANN and European authorities have been engaged in high-stakes negotiations over who may legally access the data in the future, and how. To address the concerns of security professionals and others, ICANN has proposed creating a tiered system to allow accredited users, including security professionals, to continue accessing personal data. However, how that tiered system would work is unclear, complicated and mired in controversy. Corporate security officials should take note, as it could speed up the already rapidly escalating problem of cybercrime.

KEYWORDS: GDPR, WHOIS, ICANN, Internet Corporation for Assigned Names and Numbers, PID, personal identifiable data, cybercrime, cyber security

INTRODUCTION

Europe's General Data Protection Regulation (GDPR) took effect on 25th May, 2018, following a two-year grace period. GDPR's ambitious goal is to put people in control of their personal data at a time when misuse of private data has become a serious threat. Unlike previous data privacy regulations, GDPR has teeth. It carries stiff penalties including fines of up to €20m or 4 per cent of global revenues of the prior year. This has prompted a flurry of activity as organisations worldwide seek to comply to avoid serious repercussions.

Yet GDPR is depriving security professionals of a key tool in their fight against cybercrime: access to the personal identifiable data (PID) of people who register Internet domains through WHOIS, the directory service maintained by the Internet Corporation for Assigned Names and Numbers (ICANN), the organisation that manages the global domain system. This data is vital for fighting a variety of Internet-based crimes. Even as the enforcement deadline has passed, ICANN and European authorities are engaged in high-stakes negotiations over who may legally access it in the future, and how. Corporate security officials should take note of the issue, as it could speed up the already rapidly escalating problem of cybercrime.

WHAT IS GDPR?

GDPR is the strongest major privacy regulation to date and is intended to control how companies collect, store, analyse and use PID.

In addition to regulating data use, GDPR mandates that significant data breaches are reported within 72 hours. Organisations large and small typically try to keep incidents quiet, but underreporting veils the ubiquitous nature of cybercrime. Without that knowledge, there is less impetus to develop the necessary defences against it.[1]

However, by denying cyber security professionals access to the PID of Internet domain registrants in the WHOIS domain name registry, GDPR could impair their investigative work — including, in many cases, law enforcement agents — while making life easier for cybercriminals, spammers and scammers.

WHY WHOIS IS IMPORTANT

Before the GDPR deadline, maintaining and displaying the PID of domain name registrants had been a contractual obligation imposed by ICANN via registrars (such as GoDaddy). This data, on more than 180m registered domains, could then be looked up via the WHOIS directory service. It could also be accessed via third-party tools, which enabled, for example, searches by IP addresses.

PID accessed via WHOIS has helped cybercrime investigators track and identify a wide variety of attackers and attacks. In one case, investigators reportedly used IP addresses and email accounts — the type of information that is no longer reliably available for cyber security professionals in WHOIS under GDPR — to tie a 2015 infiltration of Anthem Health's servers to China's military cyber espionage division.[2] The attack compromised the information of 78.8m individuals and could give a competitive edge to China's biotechnology industry.[3]

Similarly, when Russia's Federal Security Service allegedly hacked into 500m Yahoo accounts in 2014, a 22-year-old Canadian named in the indictment failed to cover his tracks. A reverse WHOIS search uncovered 81 domains registered in his name, including many that appeared to be designed for fraudulent activities.[4,5]

Aside from hampering investigations of such large-scale attacks, the inability to consistently access WHOIS data means average users can expect more spam, phishing and malware. That is because filters against these malicious activities depend on data made available through the WHOIS system. Specifically, filters use WHOIS data to determine whether a domain is linked to previous spam or scams, establishing reputation-based systems to suppress bad actors. As one security professional put it, 'reputation systems are one of the things that keeps the Internet usable'.[6,7]

WHOIS data has other important uses as well. It enables copyright and trademark holders to crack down on websites that use intellectual property without permission. Finally, in ICANN'S words, WHOIS builds 'consumer trust online as it allows Internet users to "look up" who is responsible for a particular domain name'.

HOW GDPR WILL IMPEDE THE WORK OF CYBER SECURITY PROFESSIONALS

Supporters of GDPR have argued that redacting personal information from WHOIS will not have a significant impact. They contend that cybercriminals tend to register domains using fraudulent identities or take advantage of existing services to cloak their personal information.[8,9] However, any information provided — especially information used across multiple domains and cybercrime campaigns — helps to assess unlawful activity and determine attribution. And, for a variety of reasons — laziness, ignorance, or the confidence that local authorities will not prosecute them for cybercrime against American or European targets — criminals often do not hide their information effectively. Even when they do use privacy services, there is frequently sufficient legacy information online to identify them.[10]

GDPR defenders argue that bringing cybercriminals to justice is the job of law enforcement, which, they contend, will be able to get more access than the public.[11] Yet the process for obtaining such access remains to be determined. ICANN has proposed easy access to non-public data for law enforcement and other legitimate users, but some commentators have argued that access should only be provided through legal due process.[12] Months after the 25th May deadline, ICANN is still soliciting legal clarification from European authorities.[13]

GDPR defenders point out that under ICANN's proposed changes, private security professionals *might* be able to request full WHOIS records from registrars by declaring a specific need for the information.[14] Such access is important, as private security researchers often do much of the initial evidence gathering required to convince law enforcement agencies that there is a case worth pursuing. However, it is not yet clear whether European authorities view this as permissible under GDPR. Moreover, replacing instantaneous online searches with manual requests, likely filed by web form, will delay investigations. In a world where the average life cycle of a phishing site is four to eight hours,[15] even a one-day response lag would give criminals a significant edge over investigators.[16]

WHAT IS HAPPENING IN THE SHORT TERM

To enable compliance with GDPR, ICANN is allowing registrars (worldwide) to redact personal information from WHOIS search results.[17] Many registrars are doing this, resulting in the elimination of PID from public WHOIS searches.

To address the concerns of security professionals and others, ICANN has proposed creating a tiered system to allow accredited users, including security professionals, to continue accessing personal data. However, how that tiered system would work is unclear, complicated and mired in controversy. ICANN has indicated that a new system would not be available until late 2018 at the earliest.

In the interim, impeded access to WHOIS data is handicapping security professionals in the fight against cybercrime. It is also leaving businesses, the economy, democracies and individuals more vulnerable.

THE BEST SOLUTION: ENFORCEMENT RELIEF AND A LONG-TERM BALANCE BETWEEN PRIVACY AND SECURITY

As the May deadline approached, ICANN repeatedly sought relief from GDPR, without success. In March 2018, ICANN requested a stay of enforcement to give it time to devise and implement a GDPR-compliant system that would provide accredited users access to WHOIS data. Europe rejected it. The Article 29 Working Party (known as WP29), an official European privacy advisory board with jurisdiction over GDPR, responded that it 'expects ICANN

to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data'.[18] (Note that the statement refers to 'law enforcement personnel' but not to other legitimate security professionals.)

Then, on 10th May, ICANN asked WP29 for forbearance from GDPR enforcement — and the large fines authorities could impose — in recognition of efforts it has made toward compliance.[19] The European Data Protection Board (EDPB — which replaced WP29 upon the 25th May deadline, and is charged with ensuring consistent application of GDPR) confirmed that the law does not allow for enforcement moratoriums, but that authorities may consider 'measures which have already been taken or which are underway when determining the appropriate regulatory response upon receiving such complaints'.[20]

Immediately after the regulation came into effect, ICANN sought an injunction in the German court to force a registrar to collect data that the registrar deemed prohibited by GDPR. The German courts have denied the injunction, but noted that ICANN could continue pursuing its claim. Meanwhile, continued collection of critical WHOIS data by registrars is not guaranteed.[21]

In the longer term, ICANN has proposed solutions to balance GDPR compliance with legitimate access to WHOIS data. These would include tiered WHOIS access, along with an accreditation programme for access to full WHOIS data for data protection authorities and contracted parties, with full transparency for the ICANN community.

Most recently, on 20th August, 2018 ICANN released for discussion a revised framework for tiered access.[22] Many details need to be worked out and it remains unclear (at time of writing) whether European authorities' interpretation of GDPR would allow for timely and sufficient access by security professionals. Previous objections suggest that, at a minimum, additional delays can be expected before European authorities and ICANN can agree on a solution, prolonging the period during which responsible parties will face uncertain access to critical data.

It should be stressed that the longer WHOIS remains dark, the harder it will be to bring transparency back to the Internet. Publishing personal registrant information costs money, and it promotes competition (by making customer details available to all registrars). The registration business operates on thin margins. Without a contractual obligation to ICANN, registrars have little incentive to make their data available.

OPTIONS FOR BUSINESSES AND SECURITY PROFESSIONALS

If, as expected, WHOIS access disappears, there is no alternative source for the information that allows security professionals to help businesses and individuals resist or recover from cybercrime.

This development comes at an unfortunate moment. Cybercrime is at an all-time high. According to the Kroll Annual Global Fraud & Risk Report, 86 per cent of companies experienced at least one malicious incident in 2017.[23] With 5G and later-generation networks coming online, and the Internet of Things (IoT) growing, the frequency and intensity of attacks are primed to increase.

As I testified to Congress earlier this year,

> 'The scope of vulnerabilities and threats posed by these expanding networks has generally exceeded the ability and willingness of businesses to respond to them. The fact is that the combination of automation, machine learning, artificial intelligence, digitized supply chain management and communication

technologies creates massive vulnerabilities for all businesses.'[24]

Juniper Research expects that by 2019 data breaches will cost companies US$2.1tn globally, nearly four times the estimated cost in 2015.[25]

More than ever, it is a business imperative to stay on top of cyber security. While WHOIS is a vital tool for investigations, the best way to handle cybercrime is to have strong defences that prevent it happening in the first place.

Meanwhile, cyber security professionals should follow the ICANN deliberations with European authorities over who may be granted access to WHOIS data, and how they can do so. These deliberations will likely take weeks, if not months. If a solution is reached enabling security professionals to register for access, they should apply for it promptly. Should ICANN be forced to limit access to law enforcement officials, the only options available to private professionals will be either to involve law enforcement in their investigations or to seek access through the courts, which would be slow, expensive, and have no guarantee of success.

References

1. Ferrante, A. (2018), 'Testimony to The U.S.-China Economic and Security Review Commission', available at https://www.uscc.gov/sites/default/files/Anthony%20Ferrante_Written%20Testimony_FINAL.pdf (accessed 3rd September, 2018).
2. Koerner, B. (2016), 'Inside the Cyberattack That Shocked the US Government', Wired, available at https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (accessed 3rd September, 2018).
3. *Ibid.*, note 1.
4. Krebs on Security (2017), 'A DomainTools.com Reverse WHOIS Search Result on Karim Baratov', available at https://krebsonsecurity.com/wp-content/uploads/2017/03/KarimBaratovDomains.txt (accessed 3rd September, 2018).
5. Krebs on Security (2017), 'Four Men Charged With Hacking 500M Yahoo Accounts', available at https://krebsonsecurity.com/2017/03/four-men-charged-with-hacking-500m-yahoo-accounts/ (accessed 3rd September, 2018).
6. Malcom, J. (October 2017), 'Reputation systems are not just nice to have', available at http://mm.icann.org/pipermail/gnso-rds-pdp-wg/2017-October/004480.html (accessed 3rd September, 2018).
7. ICANNWiki (n.d.), 'Greg Aaron', available at https://icannwiki.org/Greg_Aaron (accessed 3rd September, 2018).
8. Badi, F., Dammak, R. and Ferdeline, A. (April 2018), WHOIS afraid of the dark? Truth or illusion, let's know the difference when it comes to WHOIS, Internet Governance Project, Georgia Tech, available at https://www.internetgovernance.org/2018/04/25/whois-afraid-dark-truth-illusion-lets-know-difference-comes-whois/ (accessed 3rd September, 2018).
9. *Ibid.*, note 6.
10. Krebs on Security (April 2018), 'Security Trade-offs in the New EU Privacy Law', available at https://krebsonsecurity.com/2018/04/security-trade-offs-in-the-new-eu-privacy-law/ (accessed 3rd September, 2018).
11. *Ibid.*, note 8.
12. ICANN (March 2018), 'Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation (Working Draft)', Section 5.6, available at https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf (accessed 3rd September, 2018).
13. Marby, G. (May 2018), 'Follow-up to WP29 23 April Meeting, Letter to Andrea Jelinek', Points 9 and 10, available at https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-10may18-en.pdf (accessed 3rd September, 2018).
14. *Ibid.*, note 8.
15. Webroot (2017), 'Quarterly Threat Trends: Phishing Attacks Grow in Scale and Sophistication', available at https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf (accessed 3rd September, 2018).
16. *Ibid.*, note 10.
17. ICANN (2018), 'ICANN Board Approves Temporary Specification for gTLD Registration Data', available at https://www.icann.org/news/announcement-2018-05-17-en (accessed 3rd September, 2018).
18. McCarthy, K. (April 2018), Europe fires back at ICANN's delusional plan to overhaul Whois for GDPR by next year, available at (accessed 3rd September, 2018).
19. ICANN (April 2018), 'Data Protection/Privacy Update: Seeking Additional Clarity from Article 29', The Register, available at https://www.theregister.co.uk/2018/04/27/europe_icann_whois_gdpr/?page=2 (accessed 3rd September, 2018).
20. 'The European Data Protection Board endorsed the statement of the WP29 on ICANN/WHOIS' (May 2018), ICANN, available at https://www.icann.org/en/system/files/files/statement-edpb-whois-27may18-en.pdf (accessed 3rd September, 2018).
21. ICANN (3rd August, 2018), 'German Appellate Court Rules on ICANN Request to Preserve

WHOIS Data', available at https://www.icann.org/news/announcement-2-2018-08-03-en (accessed 5th October, 2018).
22. Marby, G. (June 2018), 'ICANN Data Protection/Privacy Update: Seeking Community Feedback on Proposed Unified Access Model', available at https://www.icann.org/news/blog/data-protection-privacy-update-seeking-community-feedback-on-proposed-unified-access-model (accessed 3rd September, 2018).
23. Cision PR Newswire (January 2018), 'Businesses Report All Time High Levels of Fraud, Cyber, and Security Incidents During 2017', available at https://www.prnewswire.com/news-releases/businesses-report-all-time-high-levels-of-fraud-cyber-and-security-incidents-during-2017-300585657.html (accessed 3rd September, 2018).
24. *Ibid.*, note 1.
25. Smith, S. (2018), 'Cybercrime Will Cost Businesses Over $2 Trillion by 2019', Juniper Research, available at https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion (accessed 3rd September, 2018).