National Crime Agency feedback on ICANN's Proposed Interim Models for Compliance with the EU's General Data Protection Regulation

Summary

- Access to all current WHOIS data is **vital** for law enforcement (LE) investigations.
- Without WHOIS data, LE's ability to protect the UK from serious organised crime will be significantly hampered.

- Access to WHOIS data enables a proportionate and victim-centred investigative strategy.
- A centralised, federated access system would:
    - Ensure a consistency of information is provided
    - Prevent the compromise of law enforcement investigations.
    - Ensure access to information is provided in a consistent and fair manner
    - Allow for a coherent audit trail
- Retention periods for WHOIS data need to be long enough to:
    - Enable a victim to identify they have been a victim (with network intrusions and malware, this can take months)
    - Allow law enforcement to carry out an investigation

Introduction

The UK's National Crime Agency (NCA) welcomes this opportunity to provide feedback on ICANN's proposed models for compliance with the EU's General Data Protection Regulation (GDPR). The NCA is fully supportive of the ICANN Governmental Advisory Committee's (GAC) submission to the consultation and this document should be read as a supplement to that. This separate response aims to provide ICANN with more information about the specific national law enforcement context and to increase awareness of the significant role WHOIS data plays within investigations, particularly those focussed on cyber dependent crime and child sexual exploitation and abuse.

The response will outline each of the key principles the NCA will require from any model implemented by ICANN if it is to investigate cyber crime effectively, and explain the risks attached if a model is chosen which does not address the principle fully.

The NCA hopes that ICANN's commitment to 'ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible' holds firm. Without it, our ability to protect the UK from serious organised crime via investigations into data breaches, malware and DDoS attacks, as well as into child sexual exploitation and abuse, will be significantly hampered.

WHOIS Lookups are central to an effective LE response

Overall, the NCA conducts approximately 80,000 WHOIS look ups each month; with the National Cyber Crime Unit and the Child Exploitation and Online Protection Command being the areas where numbers are highest.

WHOIS lookup information often provides the first lines of enquiry for investigations involving the Internet; particularly for cyber dependent crime (network intrusion, malware, DDoS), where these can often be **an essential line of enquiry** within the critical early stages of cyber crime investigation.

Crucially, WHOIS information enables investigators to understand how criminal infrastructure functions as a whole system. This enables investigators to make more informed decisions about whether domains are criminally-owned or victims of an infection themselves; this in turn enables investigators to decide whether to contact the registrant as a victim and provide clean up advice, or whether to investigate the domain further, and work with registries to implement take down or sink-holing activity.

In summary, WHOIS provides the NCA with information which facilitates the **most proportionate and effective investigative strategy.**

Fields required

The NCA is supportive of the GAC model to combine the fields for the ICANN consultation models 1 and 3. Both thick and thin WHOIS data provide an investigator with the opportunity to begin elementary subject profiling and pattern-matching with other available intelligence. Law enforcement expect the criminal may input false information when registering a domain, but any information, false or otherwise, may enable the investigator to understand some aspect of the criminal individual or group. Since any/all of the information provided by the registrant can be untrue, it is impossible to prioritise the information and suggest that some fields may be more valuable than others. This is why the NCA supports the GAC's model which proposes the inclusion of as much information as possible whilst remaining GDPR compliant.

The need for a 'centralised federated access system'

A 'centralised federated access system' to WHOIS information is **crucial** for effective investigation.

If the release of WHOIS look up information was left to the discretion of each individual registry, at best, there would be inconsistent release and quality of information; at worst, registries providing bullet proof services to criminal infrastructure (knowingly or otherwise) may inform the registrant of the law enforcement interest and compromise the investigation.

An **independent third party would provide access to information in a consistent and fair manner** to all those organisations and individuals accredited for access. It would also **allow for a coherent audit trail**, enabling law enforcement and other accredited bodies to be held to account for their requests.

Retention

The GAC submission states that "60 days is entirely too short to effectively conduct investigations". The NCA agrees with this point; the risks attached to short retention periods (which the NCA would suggest is any period less than three years) are significant. For example, crimes where the victim is unaware of the crime for a period after it has taken place, or not confident to report the incident as a crime, or where the crime has been facilitated by a much earlier cyber crime (eg. fraud which has been enabled by a network intrusion and subsequent data breach) would reduce the investigative window. Even investigations which are opened as a response to a crime in action would still experience difficulties if the criminal infrastructure predated the retention period. Furthermore, almost all cyber crime investigations require multiple International Letters of Request. These each take a minimum of two weeks to process and can take many months. Overall, the shorter the retention period, the fewer victims will be protected.

Access

The NCA succeeds in reducing the impact of cyber crime 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 investigations . 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.

Similarly, the NCA works with academic partners to build knowledge and capability to ensure that it remains credible and effective at protecting the UK public in the 21st century.

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

be unmanageable, it would also remove many organisations' ability to protect themselves from cyber crime, meaning the number of crime victims may rise exponentially.

The need for a simple request rather than a subpoena process

A system requiring bodies to present a subpoena to either individual registries or a centralised body, would dramatically increase the time taken to conduct investigations involving the internet, and thus increase the time taken to arrest child sex offenders and cyber criminals, and protect victims.

The NCA has never investigated a cyber crime where all the domains are hosted in the UK. Approximately 90% of all domains the NCA has investigated are hosted outside of the UK. If a subpoena process is introduced, the NCA would need to submit International Letters of Request for each WHOIS look up. This process would take a minimum of two weeks for each request. There is obviously no average number of domains within each investigation, but given the current NCA cyber crime average of 80,000 WHOIS look ups a month, this process would delay each investigation therefore exponentially increasing the time taken to arrest those criminals responsible and protect victims.