EJCN statement

On 25 May 2018 the General Data Protection Regulation (GDPR) of the European Union enters into force. This occasion also marks the end of publicly accessible WHOIS directories and services, in which information can be found regarding the person(s) holding the registration for a specific Internet domain. Access to this system has proven indispensable for effective and efficient criminal investigations and prosecutions of cybercrime and cyber-enabled crime. The Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for IP address space allocation and domain registration, has chosen to take the publicly accessible WHOIS system offline in order to make access to the personally identifiable information therein compliant with the GDPR. ICANN has proposed an interim model for layered access to WHOIS directories and services on the basis of an accreditation scheme. However, this model will not be ready for implementation on 25 May 2018.

The European Judicial Cybercrime Network, which brings together public prosecutors and investigative judges specialised in cybercrime, cyber-enabled crime and investigations in cyberspace, from the EU Member States, Norway and Switzerland, is concerned with the slow progress in ensuring lawful access to WHOIS records for the purpose of criminal investigations and prosecutions, and urges ICANN, Member States and the Commission to increase the efforts to ensure continued access to the WHOIS system for law enforcement and judicial authorities after 25 May 2018.

If continued access cannot be ensured, the EJCN fears that criminal investigations will be seriously impeded or possibly even discontinued, with detrimental effects to safety and security online in general and to the rights of victims in particular.

Fundamental rights

The EJCN recognises the Internet as a vital element of modern life. Because of its relevance for many aspects of our society and lives, it is relevant that the rule of law is recognised and upheld also in cyberspace. This means that fundamental rights need to be protected. Regulated access and processing of personally identifiable information is imperative to protect the privacy of citizens and to ensure that they can exercise their fundamental rights, including the right to free expression, political freedoms and the freedom of religion.

At the same time, upholding the rule of law in cyberspace means that criminal activity is investigated and where applicable or prescribed, perpetrators are brought to justice. Criminal investigations and prosecutions actively contribute to the exercise of fundamental rights, by protecting the rights and interests of victims of cybercrime and cyber-enabled crime.

If that criminality originated from an Internet domain, WHOIS records are regularly the first steps to identify persons associated with that domain (such as a technical contact) or the lower level providers handling the associated IP addresses, domain names or services. This starting information is vital, and because electronic evidence is volatile in nature, it is important to have it available without delay.

Administrative burden

Although information stored in WHOIS directories and services will not become entirely unavailable for law enforcement and judicial authorities after 25 May 2018, acquiring this information will require a much larger effort and take much more time than is currently the case. Without direct access to the system, authorities will need to initiate formal legal process and mutual legal assistance to obtain relevant information. This will come with a substantial administrative burden as well as long delays.

Currently, many law enforcement and judicial authorities in the EU Member States can access WHOIS directories and services without specific authorisation from a prosecutor or a judge. This is because the current WHOIS system is considered an open source. After 25 May 2018 authorities require formal legal process (e.g. a subpoena or court order) to obtain WHOIS data they require for their criminal investigations. Given the many instances in which WHOIS data is relevant for criminal investigations, a substantial increase in administrative burden can be expected for authorities, but also for registries, registrars and lower-level providers confronted with a large amount of subpoenas or court orders.

On top of this, formal legal process can only be initiated against registries, registrars and lower-level providers within the jurisdiction of the requesting authorities. If WHOIS data is required from a registry, registrar or lower-level provider in another country, authorities need to request the authorities of that other country. For this purpose, within the EU authorities have to send a European Investigation Order. Outside of the EU, traditional mutual legal assistance is required. These processes typically take a number of months.

Given the current workload of law enforcement and judicial authorities, it can be expected that the increased administrative burden involved with formal legal process and mutual legal assistance will result in long delays before information is received from registries and registrars - compared to the immediate access that currently exists - putting investigations on hold and negatively impacting the effectiveness and efficiency of criminal investigations.

Data retention

This time delay comes with an extra risk in view of the jurisprudence of the European Court of Justice (CJEU) on the topic of data retention. Following the rulings of the CJEU in the cases Digital Rights Ireland (2014), Tele2 Sverige and Watson et al (both 2016), the Data Protection Directive of the European Union was invalidated and in a number of Member States domestic legislation was suspended. Currently, there are great differences in legal obligations and/or periods for retaining (non-content) data pertaining to electronic communications. The delays involved in obtaining WHOIS data from registries, registrars and lower-level providers through formal legal process that are expected after 25 May 2018 may be (much) longer than the period for which the data in question is being retained. By the time formal procedures are concluded, the data may therefore no longer exist.

Proposed interim model

The interim model proposed by ICANN provides for layered access on the basis of accreditation. Although many details of this model need to be worked out still, the EJCN is concerned that given the fact that it concerns non-public information, domestic legislation in a number of Member States require formal legal procedures be followed before the system can be queried. Given the fact that domestic legal procedures cannot have a cross-border effect, this means that authorities are prohibited from accessing information held by registries, registrars and lower-level providers outside of their jurisdiction - even if on a technical level they would be able to. For this reason, the EJCN is of the opinion that the proposed interim model is not a valid substitute, nor does it compensate for the discontinuation of the current public access to WHOIS directories and services.

Summary

Considering the above detailed problems, the European Judicial Cybercrime Network is concerned with the slow progress in ensuring lawful access to WHOIS records for the purpose of criminal investigations and prosecutions, and urges ICANN, Member States and the Commission to increase the efforts to ensure continued access to the WHOIS system for law enforcement and judicial authorities after 25 May 2018.

If continued access cannot be ensured, the EJCN fears that criminal investigations will be seriously impeded or possibly even discontinued, with detrimental effects to safety and security online in general and to the rights of victims in particular.