EU POLICING, DATA RETENTION & SECURITY

EuroCOP Position Paper

Current and future security threats to European society are no longer easy to define or combat. An example is the rising trend in criminal organizations turning to the Internet to facilitate their illegal activities. Cybercrime is a fast-growing area of crime that encompasses a wide range of criminal activity (e.g. email scams, identity theft and child pornography) that present real threats to Europe's citizens. In 2014, EUROPOL emphasized that the EU will remain a key target for cybercrime activities because of its relative wealth, high degree of Internet penetration, its advanced Internet infrastructure and increasingly Internet-dependent economies and payment systems. One of the main challenges of cybercrime is that cyber criminals can easily attack a large number of victims without being identified, whereas in the off-line world criminals are typically physically present at the crime scene. Cybercrime is therefore the perfect example of an issue that has forced police agencies to rethink the basic tools and skills they need to do their job. Moreover, parts of the Internet that enable criminals to remain anonymous, known as Darknets, are increasingly hosting hidden services and marketplaces devoted to traditional types of organised crime, such as the drug trade, selling stolen goods, weapons dealing, compromised credit card details, forged documents, fake IDs, and the trafficking of human beings. In order to combat serious crimes and to protect citizens from online criminal activity, police officers rely on the ability to detect and investigate the traces resulting from any electronic communications related to crime. Without this ability it becomes increasingly difficult to uncover criminal activity in online networks.

"We understand the complexities and sensitivities of data retention, and the fine balance between ensuring our security and protecting our freedom. For EuroCOP though it is essential that the police are given the best possible tools and opportunities to do their job".

EuroCOP President
Anna Nellberg Dennis

Total value of transactions € 3.5 trillion

Fraud: € 1.33 billion

Payment card transactions are the most widespread noncash payment method used in the EU. In 2012, the total value of transactions made by debit and credit cards issued within the Single Euro Payments Area (SEPA) amounted to EUR 3.5 trillion. In the same period, criminals acquired EUR 1.33 billion from payment card fraud (PCF). This represents 38 cents lost to fraud for every EUR 1000 worth of transactions.

(Sources: EuroPol The Internet Organised Crime Threat Assessment 2014)

DATA RETENTION & COUNTER TERRORISM

In recent debates on European counter-terrorism measures, the importance of access to data by the police and intelligence agencies is often addressed. In various EU Member States there have been calls from politicians to (re-) introduce data retention laws. Because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of serious crime and terrorism.

EU POLICY FRAMEWORK

Data Retention Directive
Following the terrorist attacks in Madrid in 2004 and London in 2005, several EU Member States adopted legislation providing for the retention of data by service providers and the national provisions varied considerably. To harmonize the EU efforts in the investigation and prosecution of the most serious crimes such as, organized crime and terrorism, the Data Retention Directive (Directive 2006/24/EC) was adopted.

The Directive required operators to retain certain categories of traffic and location data (excluding the content of those communications) for a period between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of preventing, investigating, detecting and prosecuting serious crime and terrorism.

ECJ Case
On 8 April 2014, the EU Court of Justice declared the Data Retention Directive invalid (joined Cases C-293/12 and C-594/12) because the scope of the surveillance it allowed included all individuals, which went beyond the bounds of proportionality. In particular, the Court held that the Directive seriously interfered with the rights to privacy and personal data protection of individuals, guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities. However, the Court also acknowledged that ensuring public security may depend to a great extent on the use of modern investigative technologies. It therefore considered that data retention serves, under clear and precise conditions, a legitimate and general interest, namely the fight against serious crime and the protection of public security.

EUROCOP RECOMMENDATIONS

- European Union Member States need an EU instrument in place to harmonize the efforts in the investigation and prosecution of the most serious crimes. In the context of current and future security threats and to ensure a coherent and coordinated EU approach, EuroCOP calls on the European Commission to review the Data Retention Directive.
- When reviewing the Data Retention Directive or considering a new proposal, EuroCOP calls on the Commission to take into account all interests involved in order to ensure fundamental rights are protected and citizens remain secure. EuroCOP therefore looks forward to participating in a consultation process where stakeholders can cooperate to find solutions that serve these goals.
- For police officers to do their job, it is important to have clear regulations that stipulate under what circumstances stored data information can be requested. In order to enhance cross border police cooperation in the EU, it is also critical to implement an EU approach to data retention in order to avoid different national requirements which create uncertainty and hamper cooperation.

POLICE CASE STUDIES

If police officers were allowed to connect owner data to IP addresses, various serious crimes could be solved (or prevented from occurring). For example in Sweden, the police are increasingly reviving "cold case" investigations to retrieve information about cases of serious crime that happened in the past (more than a year ago). There are various cases where the lack of clear data retention rules has hampered these investigations. This means that the chance of solving cases of serious crime drastically decreases. Moreover, in Germany there have been several cases where child abuse and the spread of child pornography were openly discussed in a chat room. In all cases, the IP addresses of the accused provided the only investigative leads. Due to not being able to access data through the provider, offenders could not be prosecuted. As a result, other acts of abuse could not be prevented. According to EuroPol, in 2014 80% of victims of child sexual exploitation online (CSEO) were younger than 10.

ABOUT EUROCOP

The European Confederation of Police, EuroCOP, is the umbrella organisation for 35 police unions and staff organisations in Europe based in Luxembourg. It represents the interests of almost half a million police officers in 27 European countries, dealing with issues which range from police cooperation across borders to a safer working environment for police officers on the street. EuroCOP was established in November 2002. It is an independent, non-profit and secular organisation and has no affiliation with any government or political party. It is self-financed through contributions of its members. EuroCOP is open to any organisation representing police officers in member countries of the European Union or the Council of Europe.

www.eurocop.org