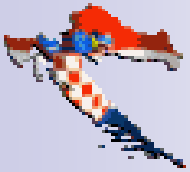


Republic of Croatia
Ministry of the Interior
Police Academy
Police College

# *"Cross-border Access to Digital Evidence at Internet and Cloud"*

*Chief Police advisor, Asossiet Professor* **Krunoslav Antoliš,** Ph.D.

***All statements made in this presentation are solely those of the authors and in no way reflects the official positions or policies of the Republic of Croatia, Croat's Parliament, Croat's Government or Ministry of Interior.***

# Digital (electronic) evidence as the challenge

- The aim is to support decision-makers in taking clear national positions regarding the legal norms in the area of access to the Internet infrastructure.
- Legal consequences and acceptability of certain methods of gathering digital evidence and possible violation of the privacy of legal and private persons!

# Scope of the problem

- Most of **the relevant information** is held by a number of service providers including electronic communications service providers and information society service providers, providers of internet infrastructure services and digital marketplaces.
- Both relevant data and relevant service providers **could potentially be anywhere in the world,** as the relevant services are provided at a distance and are independent of national borders.

# Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021

- Ransomware affiliate programs enable a larger group of criminals to attack big corporations and public institutions by threatening them with multi-layered extortion methods such as DDoS attacks.
- Mobile malware evolves with criminals trying to circumvent additional security measures such as two-factor authentication.
- Online shopping has led to a steep increase in online fraud.
- Explicit self-generated material is an increasing concern and is also distributed for profit.
- Criminals continue to abuse legitimate services such as VPNs, encrypted communication services and cryptocurrencies.

# Size of the problem ? ! .

- **More than half of all investigations include a cross-border request to access e-evidence.**
- **E-evidence in any form is relevant in around 85% of total (criminal) investigations.**
- **In almost two thirds (65%)** of the investigations where e-evidence is relevant, **a request to service providers across borders** (based in another jurisdiction) **is needed**.
- **Germany** (35,271 requests), the **UK** (28,598) and **France** (27,268), **accounted for more than 75% of the total number of requests from the EU** to the five main service providers in the last year.
- **Google and Facebook accumulated more than 70%** of the total number of requests from EU Member States to the five main service providers in the last year.
- **The number of requests** to the above service providers **has increased by 70% in the last 4 years!**

# EU challenges in cross-border access to electronic evidence

- Once a cross-border element is or might be present, **authorities have to rely on one of the three channels existing today to access e-evidence across borders:**
  - **judicial cooperation between public authorities,**
  - **direct cooperation between a public authority and a service provider and**
  - **direct access to electronic evidence by a public authority.**
- These **channels suffer from a number of shortcomings** that can be summarised as follows:
  - **judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources;**
  - **direct cooperation can be unreliable, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability;**
  - **legal fragmentation abounds, increasing costs on all sides; and**
  - **the size of the problem is steadily increasing, creating further delays**

# What are the problem drivers?

| Problem drivers | Specific objectives | General objective |
|---|---|---|
| 1.It takes too long to access e-evidence across borders under existing judicial cooperation procedures, rendering investigations and prosecutions less effective<br>2.Inefficiencies in public-private cooperation between service providers and public authorities hamper effective investigations and prosecutions<br>3.Shortcomings in defining juris-diction can hinder effective cross-border investigation and prosecution | 1.Reduce delays in cross-border access to electronic evidence<br>2.Ensure cross-border access to electronic evidence where it is currently missing<br>3.Improve legal certainty, protection of fundamental rights, transparency and accountability | Ensure effective investigation and prosecution of crimes in the EU by improving cross-border access to electronic evidence through enhanced judicial cooperation in criminal matters and an approximation of rules and procedures |

# Various approaches to the digital (electronic) evidence on the Internet & Cloud

- Cybercrime Convention (Council of Europe)
  - Russia, China, India
- NATO approach
- CLOUD Act
  - Privacy Policy - GDPR vs. CLOUD Act
- Australian "Decryption" Bill

# Russia, China, India

The most controversial provision of the Budapest Convention, such as Article 32, on cross-border access to stored computer data with the consent or if it is publicly available.

The party may, without the consent of the other party:

a. access to publicly available (open source) stored computer data, regardless of where the data are geographically located; or

b. to access or receive, through the computer system on its territory, stored computer data located in the other Party, if the party obtains the lawful and voluntary consent of a person with the statutory authority to disclose information to a party through that computer system.

# Sovereign Internet law

- Russia’s “sovereign internet” law went into effect on Friday , November 1, 2019
- The law tightens Moscow’s control over the country’s internet infrastructure and aims to provide a way for Russia to disconnect its networks from the rest of the world.

# NATO approach

NATO supported "Improved cyber defense policy", based on its cyber defense policy in 2011.

In a statement accompanying the meeting of heads of state, NATO confirmed that "international law, including international humanitarian law and the UN Charter, applies in cyberspace" and clarified that

**"the North Atlantic Council will decide when cyber attack will bring to refer to Article 5 [governing the collective defense] ".**

# Microsoft's email account in Ireland

- One, if not the most prominent instance where the required data is stored on foreign-site servers, is Microsoft Ireland.
- The case began in December 2013, when the US court ordered Microsoft to surrender data belonging to Microsoft's email account in Ireland.
- The service provider disputed a court order based on arguments on jurisdiction and sovereignty, resulting in a legal battle between the Ministry of Justice (DOJ) and Microsoft, which ended before the Supreme Court in 2017.

# CLOUD Act

- However, before the Supreme Court could decide on this issue, in March 2018, the US Congress passed the CLOUD Act, which now allows American LEAs to request data from US service providers even if these data are stored on servers abroad.
- The United States has passed the CLOUD Act, which accelerates access to electronic information held by global ISP providers based in the United States.
- The Law on Clouds allows the United States to conclude executive agreements with other countries that meet certain criteria, such as respect for the rule of law, in solving the problem of conflict of law.
- For investigations of serious criminal offenses, ISPs may qualify for qualified, legitimate electronic data orders issued by another country.

# Privacy Policy – GDPR vs. CLOUD Act

- Privacy concerns created by GDPR on EU territory in the application of CLOUD law are also reflected in the fact that ISP service providers can notify search account owners in accordance with the US court's order under the Law on Preserved Communications unless an independent judge has issued a security order.
- Protective orders pertaining to all provisions of the Act on Preserved Communications (and not just orders in accordance with the CLOUD Act) shall be issued when the Independent Judge finds that there is reason to believe that a notification of a court order may result in adverse outcome

  (1) physical security of an individual;

  (2) escape from persecution;

  (3) Destruction or manipulation of evidence;

  (4) intimidation of potential witnesses; or

  (5) otherwise seriously endangers the investigation or unjustifiably delayed the trial.

# What does Schrems II mean for data privacy?

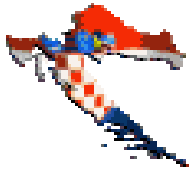
- That rule applies to landmark judgement in Data Protection Commissioner vs. Facebook Ireland Limited, Maximilian Schrems ("Schrems II") from the Court of Justice of the European Union (CJEU).
- Over the past decade, there have been ongoing attempts to validate US companies maintaining an "adequate level of protection" for any EU data. The EU-US Privacy Shield was introduced to specifically address data protection for personal data that is transferred from the European Union to the United States.
- Over 5000 companies soon leveraged the Privacy Shield as their main legal mechanism when transferring personal data from the European Union to the United States.
- The landmark judgement declares the EU-Privacy Shield invalid, throwing the privacy world into disarray. Specifically, throwing into question the legality of transferring EU citizens' data to the United States – and how personal data should be shared across borders.

# Australian "Decryption" Bill

- Australian lawmakers have now decided to ensure that national security and law enforcement agencies have the modern tools they need, with appropriate powers and oversight, to access encrypted conversations of those who want to do harm, by granting the Assistance Act and access only recently 6 December 2018.
- The Australian Law on Telecommunication Access and Assistance allows the government to foster cooperation and capabilities from companies such as social media companies, telecommunications, manufacturers, or even any retail company that provides its customers with WiFi.
- The law will force technology companies to help Australian governments decipher network users' communications - and this could be a big blow to privacy in other parts of the world.
- The law provides for up to $ 7.3m for corporations as well as jail.

# Conclusion

- **Without a common legal framework which will be globally acceptable,** it is not possible to speak of **legitimate access to digital (electronic) evidence**, especially on parts of the Internet infrastructure and the cloud, **which are physically located outside national borders.**
- One of **the biggest challenges for the future** is to explore **what could be a strong enough and acceptable cause** to reach a global consensus on a **legal framework for the Internet.**



# Questions ???

# Comments !!

# Remarks .

*Asossiet Professor* **Krunoslav Antoliš,** *Ph.D.*
***kantolis@fkz.hr***