POST-COVID CHALLENGES IN CRIMINAL JUSTICE

E-EVIDENCE AS THE NEW EVIDENTIARY FRONTIER FOR EU LEGAL PRACTITIONERS

Dublin, 20-21 April 2023

EXCELLENCE IN EUROPEAN LAW

Speakers and chairs

John Berry, Barrister, Bar of Ireland, Dublin

Laviero Buono, Head of Section for European Criminal Law, ERA, Trier

Rainer Franosch, Prosecutor, Deputy Director-General for Criminal Law and Criminal Procedure, Head of Cybercrime Division, Ministry of Justice, German Federal State of Hesse, Wiesbaden

Klaus Hoffmann, Senior Prosecutor Prosecutor's Office, Freiburg

Damir Kahvedžić, Solutions Advisor and Operations Manager, ProSearch, Dublin

Aisling Kelly, Senior Counsel, Law Enforcement & National Security, Microsoft, Dublin

Joachim Meese, Professor, Criminal Law and Procedure, University of Antwerp; Attorney, Bar of Ghent

Sara Phelan SC, Chair of the Council of The Bar of Ireland, Dublin

Chatrine Rudström, Senior Public Prosecutor, National Public Prosecution Department, National Unit against Organised Crime, Stockholm

Stanisław Tosza, Associate Professor of Compliance and Law Enforcement, University of Luxembourg

Victor Voelzow, Trainer for Digital Forensics, State Policy Academy, Hesse

Key topics

- The foundations of electronic evidence
- Collecting, authenticating and evaluating digital data in the framework of legal proceedings
- The challenges posed by encrypted data
- Conducting a criminal investigation across state borders: search orders, search and seizure, destruction of evidence, evidence from other jurisdictions, trial
- Chain of custody (through case studies)

Language
English

Event number
323DT11f

Organisers
ERA (Laviero Buono) in cooperation with the Bar of Ireland

THE BAR OF IRELAND
The Law Library

With the support of the European Union

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Thursday, 20 April 2023

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Sara Phelan SC & Laviero Buono

PART I: TECHNICAL ISSUES AND BASIC UNDERSTANDING OF THE INTERNET ACHITECTURE AND CONCEPTS

Chair: Laviero Buono

09:35 **Internet searches and computer forensics: using open-source intelligence to gather evidence online**
- Internet 1.0/2.0 vs social media 1.0/2.0
- Internet cache: deleting and retrieving
- Hidden features of websites to help you gather unseen evidence: real-life examples from selected websites and social media
- Best practices on how to gather online evidence correctly
- Analysis techniques to investigate evidence effectively
- Demonstration of evidence-gathering tools

Damir Kahvedžić

10:30 Discussion

10:45 **Open-source tools and computer forensics in the "Cloud"**
- Encryption and reverse-image search
- How to review a webpage or site that is offline
- Physical and logical acquisition of data
- Cloud providers and replicated data on websites

Victor Voelzow

11:30 Discussion

11:45 Break

PART II: LEGAL ISSUES RELATED TO THE COLLECTION AND THE PRESENTATION OF E-EVIDENCE IN COURT

Chair: Joachim Meese

12:15 **Online investigations and the challenges of dealing with electronic evidence in criminal proceedings**
- Principles of dealing with electronic evidence
- Common procedures for recognising and handling evidence
- International investigations (search and seizure – obtaining evidence from the Internet, admissibility)

Klaus Hoffmann

13:00 Discussion

13:15 Lunch break

14:15 **The collection of evidence located abroad and the challenges of cross-border access to data**
- Cross-border access to data and cloud computing
- European enforcement challenges in the online context
- Shortcomings and remedies

Stanisław Tosza

15:00 Discussion

15:15 Break

Objective

As a result of online investigations, criminal courts are confronted with the question of whether electronic evidence presented in criminal proceedings is admissible. Rules governing the admissibility of electronic evidence vary in the legal frameworks of different Member States and are continuously challenged by the evolution of digital devices.

This seminar aims to provide advanced knowledge and the exchange of experience and best practices between judges, prosecutors and lawyers in private practice from EU Member States who are dealing with online investigations. This will improve participants' knowledge of the strategies and techniques used in different European countries and will ultimately improve cross-border cooperation among Member States' authorities.

This series of events addresses various challenges that judges, prosecutors and lawyers in private practice working in the field of EU criminal justice will have to face for the years ahead. Some of these challenges will remain the "new normal" well beyond the end of the pandemic.

About the Project

This seminar is part of a large-scale project sponsored by the European Commission entitled "Preparing criminal justice professionals to address new (post-) pandemic challenges as a result of criminals' new *modi operandi*". It consists of seven seminars to take place in Bucharest, Dublin, Lisbon, Cracow, Barcelona, Thessaloniki and Tallinn over the period 2022-2024.

Who should attend?

Judges, prosecutors and lawyers in private practice from eligible EU Member States.

Venue

King's Inns (hosted by the Bar of Ireland)
Henrietta Street, Dublin 1

15:30 **Cooperation with EU public authorities: views from the Tech sector**
Aisling Kelly

16:15 Discussion

16:30 End of first day

20:00 Dinner offered by the organisers

Friday, 21 April 2023

PART III: ONLINE INVESTIGATIONS AND HANDLING OF E-EVIDENCE – BEST PRACTICES

Chair: Stanisław Tosza

09:30 **The European Investigation Order (EIO) and its effectiveness in collecting evidence located abroad**
- Legal framework and problems regarding traditional mutual legal assistance (MLA) in the digital age
- The EIO in the online context
- Specificities and challenges of criminal cases where anonymous networks and encrypted files are involved

Joachim Meese

10:00 Discussion

10:15 **Addressing new (post)-Covid pandemic challenges – criminals' new *modi operandi*: cybercrime, ransomware, child sexual abuse and non-cash payment fraud**
Rainer Franosch

10:45 Discussion

11:00 Break

Chair: Rainer Franosch

11:30 **Handling electronic evidence in courts**
- The importance of the chain of custody in handling evidence
- Trial considerations: methods of presentation and admissibility tests

Chatrine Rudström

12:00 Discussion

12:15 **Collecting, authenticating and evaluating digital data in the framework of legal proceedings: best practices**
- Issuing order
- Presentation in court and admissibility of e-evidence
- Case studies

John Berry

12:45 Discussion

13:00 End of seminar and light lunch

For programme updates: **www.era.int.**
Programme may be subject to amendment.

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). Participation in the full programme of this event corresponds to **8 CPD hours**.
A certificate of participation for CPD purposes with indication of the number of training hours completed will be issued on request. CPD certificates must be requested at the latest 14 days after the event.

Your contact persons

Laviero Buono
Head of Section
E-Mail: LBuono@era.int

Susanne Babion
Assistant
Tel.: +49(0)651 9 37 37 422
E-Mail: sbabion@era.int

www.era.int/elearning

This programme has been produced with the financial support of the European Union.

The content of this programme reflects only ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

Application

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Dublin, 20-21 April 2023 / Event number: 323DT11/SBa

Terms and conditions of participation

Selection

1. Participation is only open to judges, prosecutors and lawyers in private practice from eligible EU Member States.

   The number of places available is limited (30 places). Participation will be subject to a selection procedure. Selection will be according to professional eligibility, nationality and then "first come, first served". Spanish applicants who work for the prosecution service must apply for this event through CEJ.

2. Applications should be submitted before **16 February 2023**.

3. A response will be sent to every applicant after this deadline. **We advise you not to book any travel or hotel before you receive our confirmation**.

Registration Fee

4. €130 including documentation, lunches and dinner.

Travel and Accommodation Expenses

5. Participants will receive a fixed contribution towards their travel and accommodation expenses, and are asked to book their own travel and accommodation. The condition for payment of this contribution is to sign all attendance sheets at the event. No supporting documents are needed. The amount of the contribution will be determined by the **EU unit cost calculation guidelines**, which are based on the distance from the participant's place of work to the seminar location and will not take account of the participant's actual travel and accommodation costs.

6. Travel costs from outside Ireland: participants can calculate the contribution to which they will be entitled on the European Commission website (https://era-comm.eu/go/calculator). The distance should be calculated from their place of work to the seminar location.

   For those travelling within Ireland, the contribution for travel is fixed at €36 (for a distance between 50km and 400km). Please note that no contribution will be paid for travel under 50km. For more information, please consult p.10 on https://era-comm.eu/go/unit-cost-decision-travel

7. Accommodation costs: international participants and national participants travelling more than 50km one-way will receive a fixed contribution of €139 per night for up to two nights' accommodation. For more information, please consult p.13 on https://era-comm.eu/go/unit-cost-decision-travel

8. These rules do not apply to representatives of EU Institutions and Agencies who are required to cover their own travel and accommodation.

9. Successful applicants will be sent the relevant claim form and information on how to obtain payment of the contribution to their expenses. Please note that no payment is possible if the registered participant cancels their participation for any reason.

Participation

10. Participation at the whole seminar is required and participants' presence will be recorded.

11. A list of participants including each participant's address will be made available to all participants unless ERA receives written objection from the participant no later than one week prior to the beginning of the event.

12. The participant will be asked to give permission for their address and other relevant information to be stored in ERA's database in order to provide information about future ERA events, publications and/or other developments in the participant's area of interest.

13. A certificate of attendance will be distributed at the end of the conference.

Apply online for "(Post)Covid Challenges in Criminal Justice" online:
www.era.int/?131840&en

Venue
King's Inns
(hosted by the Bar of Ireland)
Henrietta Street
Dublin 1

Language
English

Contact Person
Susanne Babion
Assistant
Tel.: +49(0)651 9 37 37 422
E-Mail: sbabion@era.int

323DT11
TABLE OF CONTENTS

With the support of the Justice Programme of the European Union

This publication has been produced with the financial support of the Justice Programme of the European Union. The content of this publication reflects only the ERA's view and the Commission is not responsible for any use that may be made of the information it contains.

A1-05	Charter of fundamental rights of the European Union *(OJ. C 364/1; 18.12.2000)*
A1-06	Explanations relating to the Charter of Fundamental Rights *(2007/C 303/02)*
A1-07	Convention implementing the Schengen Agreement of 14 June 1985 *(OJ L 239; 22.9.2000, P. 19)*

A2) Court of Justice of the European Union

A2-01	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-02	Consolidated version of the Rules of Procedure of the Court of Justice (25 September 2012)

A3) European Convention on Human Rights (ECHR)

A3-01	Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 together with additional protocols No. 4, 6, 7, 12 and 13, Council of Europe
A3-02	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-03	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-04	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-05	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-06	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-07	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-08	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-09	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015
A3-10	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-11	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-12	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-13	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-02	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-03	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-04	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020

A4-05	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-06	The Law Society, “Brexit no deal: Criminal Justice Cooperation”, London, September 2019
A4-07	European Commission, Factsheet, „A „No-deal“-Brexit: Police and judicial cooperation”, April 2019
A4-08	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-09	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-10	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-11	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-12	LSE-Blog, Why Britain´s habit of cherry-picking criminal justice policy cannot survive Brexit, Auke Williams, London School of Economics and Political Science, 29 March 2018
A4-13	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-14	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-15	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-16	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017
A4-17	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)
A4-18	Scottish Parliament Information Centre, Briefing, Brexit: Impact on the Justice System in Scotland, Edinburgh, 27 October 2016

B) Mutual legal assistance

B1) Legal framework

B1-01	Council Act of 16 October 2001 establishing in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(2001/C 326/01), (OJ C 326/01; 21.11.2001,P. 1)*
B1-02	Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union *(OJ C 197/1; 12.7.2000, P. 1)*
B1-03	Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure between the Member States of the European Union and Iceland and Norway (OJ L 292, 21.10.2006, p. 2–19)
B1-04	Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 8.XI.2001*)
B1-05	Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 17.III.1978*)
B1-06	European Convention on Mutual Assistance in Criminal Matters *(Strasbourg, 20.IV.195*9)

B1-07	Third Additional Protocol to the European Convention on Extradition (*Strasbourg, 10.XI.2010*)
B1-08	Second Additional Protocol to the European Convention on Extradition *(Strasbourg, 17.III.1978)*
B1-09	Additional Protocol to the European Convention on Extradition (*Strasbourg, 15.X.1975*)
B1-10	European Convention on Extradition (*Strasbourg, 13.XII.1957*)

B2) Mutual recognition: the European Arrest Warrant

B2-01	Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial *(OJ L 81/24; 27.3.2009)*
B2-02	Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States *(OJ L 190/1; 18.7.2002, P. 1)*
B2-03	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-04	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-05	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-06	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-07	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019
B2-08	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-09	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-10	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-11	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-12	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-13	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-14	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-15	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-16	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-17	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-18	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-19	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-20	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-21	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017

B2-22	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-23	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-24	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-25	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-26	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-27	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-28	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-29	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-30	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-31	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-32	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-33	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-34	C-261/09 Mantello, Judgement of 16 November 2010
B2-35	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-36	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-37	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-38	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-02	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-03	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-04	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020
B3-05	Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
B3-06	Commission Delegated Regulation (EU) …/... of 13.2.2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, C(2019) 1326 final
B3-07	Regulation 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing and confiscation orders, L 303/1, Brussels, 14 November 2018
B3-08	Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, L 284/22

B3-09	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), PE/72/2017/REV/1 OJ L 156, p. 43–74, 19 June 2018
B3-10	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
B3-11	Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)
B3-12	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)
B3-13	Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance)
B3-14	Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community
B3-15	Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
B3-16	Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)

B4) Mutual recognition: Convictions

B4-01	Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention *(OJ L 294/20; 11.11.2009)*
B4-02	Council Framework Decision 2008/947/JHA on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions *(OJ L 337/102; 16.12.2008)*
B4-03	Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union *(OJ L 327/27; 5.12.2008)*
B4-04	Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings *(OJ L 220/32; 15.08.2008*)
B4-05	Case C-234/18, Judgment of 20 March 2020
B4-06	Case C-390/16, Dániel Bertold Lada, Opinion of AG Bot, delivered on 06 February 2018
B4-07	Case C-171/16, Trayan Beshkov, Judgement of the Court (Fifth Chamber), 21 September 2017
B4-08	Case C-528/15, Policie ČR,Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie v Salah Al Chodor, Ajlin Al Chodor, Ajvar Al Chodor, Judgement of the Court (Second Chamber), 15 March 2017
B4-09	Case C-554/14, Ognyanov, Judgement of the Court (Grand Chamber), 8 November 2016
B4-10	Case C-439/16 PPU, Milev, Judgement of the Court (Fourth Chamber), 27 October 2016
B4-11	C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B4-12	C-601/15 PPU, J. N. v Staatssecretaris voor Veiligheid en Justitie, Judgement of the Court (Grand Chamber), 15 February 2016
B4-13	C-474/13, Thi Ly Pham v Stadt Schweinfurt, Amt für Meldewesen und Statistik, Judgement of the Court (Grand Chamber), 17 July 2014
B4-14	Joined Cases C-473/13 and C-514/13, Bero and Bouzalmate, Judgement of the Court (Grand Chamber), 17 July 2014
B4-15	C-146/14 PPU, Bashir Mohamed Ali Mahdi, Judgement of the Court (Third Chamber), 5 June 2014
B4-16	Case C-383/13 PPU, M. G., N. R., Judgement of the Court (Second Chamber), 10 September 2013

B5) Mutual recognition in practice: evidence and e-evidence

B5-01	The European Law Blog, „E-Evidence: The way forward. Summary of a Workshop held in Brussels on 25 September 2019, Theodore Christakis, 06 November 2019
B5-02	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-03	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-04	EURCRIM, "The European Commission's Proposal on Cross Border Access to e-Evidence – Overview and Critical Remarks" by Stanislaw Tosza, Issue 4/2018, pp. 212-219
B5-05	Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-06	Annex to the Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 05 February 2019
B5-07	Fair Trials, Policy Brief, „The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters", October 2018
B5-08	ECBA Opinion on European Commission Proposals for: (1) A Regulation on European Production and Preservation Orders for electronic evidence & (2) a Directive for harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Rapporteurs: Stefanie Schott (Germany), Julian Hayes (United Kingdom)
B5-09	Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17 April 2018
B5-10	Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April 2018
B5-11	Non-paper from the Commission services: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward *(8 June 2017)*
B5-12	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-13	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-14	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-15	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-16	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-17	Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents

	and data for use in proceedings in criminal matters *(OJ L, 350/72, 30.12.2008*)
B5-18	Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence *(OJ L 196/45; 2.8.2003*)
B5-19	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce*) (Official Journal L 178/1, 17.7.2000)*
B5-20	Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring security and trust in electronic communication - Towards a European Framework for Digital Signatures and Encryption *(COM (97) 503)*, October 1997

B6) Criminal records, Interoperability

B6-01	Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726) (*OJ L135/85, 22.05.2019*)
B6-02	Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (*OJ L 135/85, 22.05.2019*)
B6-03	Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (*OJ L 135/27, 22.05.2019*)
B6-04	Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA, PE-CONS 87/1/18, Strasbourg, 17 April 2019
B6-05	Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States *(OJ L 93/23; 07.4.2009)*
B6-06	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-07	Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record *(OJ L 322/33; 9.12.2005)*

B7) Conflicts of jurisdiction – *Ne bis in idem*

B7-01	Case law by the Court of Justice of the European Union on the principle of ne bis in idem in criminal matters, Eurojust, April 2020
B7-02	Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings *(OJ L 328/42; 15.12.2009, P.42*)
B7-03	European Convention on the Transfer of Proceedings in Criminal Matters (Strasbourg, 15.V.1972)

C) Procedural guarantees in the EU

C-01	Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297/1, 4.11.2016)
C-02	Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132 1; 21.5.2016)
C-03	Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings (11.3.2016; OJ L 65/1)
C-04	Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294/1; 6.11.2013)
C-05	Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (1.6.2012; OJ L 142/1)
C-06	Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings *(OJ L 280/1; 26.10.2010*)
C-07	Case C-659/18, Judgement of the Court of 2 March 2020
C-08	Case C-688/18, Judgement of the Court of 3 February 2020
C-09	Case C-467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-10	Case C-467/18 on directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, EP, Judgement of the court (Third Chamber), 19. September 2019
C-11	Case C-377/18, AH a. o., Judgment of the Court of 05 September 2019
C-12	Case C-646/17 on directive 2012/13/EU on the right to information in criminal proceedings, Gianluca Moro, Judgement of the Court (First Chamber), 13 June 2019
C-13	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-14	Case C-646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-15	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-16	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-17	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-18	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)

C-19	Joined Cases C-124/16, C-188/16 and C-213/16 on Directive 2012/13/EU on the right to information in criminal proceedings Ianos Tranca, Tanja Reiter and Ionel Opria, Judgment of 22 March 2017 (Fifth Chamber)
C-20	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-21	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-22	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-23	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C-543/14
C-24	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-02	Communication from the Commission to the European Parliament, the European Council and the Council, Twentieth Progress Report towards an effective and genuine Security Union, COM(2019) 552 final, Brussels, 30 October 2019
D1-03	Communication from the Commission to the European Parliament, and the Council, Towards better Implementation of the EU's anti-money laundering and countering the financing of terrorism framework, COM(2019) 360 final, Brussels, 24 July 2019
D1-04	Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, L 123/18
D1-05	Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 amending Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries, L 125/4 (Text with EEA relevance)
D1-06	Council Decision (CFSP) 2019/25 of 08 January 2019 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision (CFSP) 2016/1136, Brussels, 08 January 2019
D1-07	Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, Brussels, 12.9.2018, COM(2018) 640 final
D1-08	Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327/20; 9.12.2017)
D1-09	Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework

	Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6)
D1-10	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119/132; 4.5.2016)

D2) Trafficking in Human Beings, Migrant Smuggling and Sexual Exploitation of Children

D2-01	Regulation of the European Parliament and of the Council amending Regulation (EC) No 810/2009 establishing a Community Code on Visas (Visa Code), PE-CONS 29/19, Brussels, 15 May 2019
D2-02	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-03	Report from the European Commission to the European Parliament and the Council, Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2018) 777 final, Brussels, 03 December 2018
D2-04	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-05	Council Conclusions on setting the EU‘s priorities for the fight against organised and serious international crime between 2018 and 2021, Brussels, 9450/17, 19 May 2017
D2-06	Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA

D3) Cybercrime

D3-01	Internet Organised Crime Threat Assement (IOCTA) 2019
D3-02	Special Eurobarometer 480, Report, “Europeans´ Attitudes towards Internet Security”, Brussels, March 2019
D3-03	Directive 2013/40/EU of the European Parliament and of the Council of 12 august 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal L 218/8 of 14.08.2013
D3-04	Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA *(OJ L 335/; 17.12.2011*)
D3-05	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-06	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (*OJ L 13/44; 20.1.2004*)
D3-07	Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28.I.2003)
D3-08	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

D4-01	European Commission, Executive Summary of the Report on strengthening Victims´ Rights: From Compensation to Reparation – For a new EU Victims´ Rights Strategy 2020-2025, Report of the Special Adviser Joëlle Milquet to the President of the European Commission, Brussels, 11 March 2019
D4-02	Regulation (EU) No 606/2013 of the European Parliament and of the Council of 12 June 2013 on mutual recognition of protection measures in civil matters
D4-03	European Commission, DG Justice Guidance Document related to the transposition and implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-04	Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA
D4-05	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-06	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-07	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-08	Victim Support Europe

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, Report on Activities and Management 2017-2018
E1-02	Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (*OJ L 348/130, 24.12.2008, P. 130*)

E2) Eurojust

E2-01	Eurojust quarterly newsletter
E2-02	Eurojust Guidelines on Jurisdiction
E2-03	Eurojust Annual Report 2019
E2-04	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-05	Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA

E3) Europol

E3-01	Europol Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-02	Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

E4) European Public Prosecutor's Office

E4-01	Decision 2019/1798 of the European Parliament and of the Council of 14 October 2019 appointing the European Chief Prosecutor of the European Public Prosecutor's Office (*OJ L 274/1, 28.10.2019*)
E4-02	Opinion on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 883/2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) as regards cooperation with the European Public Prosecutor's Office and the effectiveness of OLAF investigations Committee on Civil Liberties, Justice and Home Affairs, Rapporteur for opinion: Monica Macovei, 11.1.2019
E4-03	German Judges' Association: Opinion on the European Commission's initiative to extend the jurisdiction of the European Public Prosecutor's Office to include cross-border terrorist offences, December 2018 (only available in German)
E4-04	Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM(2018) 641 final
E4-05	Annex to the Communication from the Commission to the European Parliament and the European Council: A Europe that protects: an initiative to extend the competences of the European Public Prosecutor's Office to cross-border terrorist crimes, Brussels, 12.9.2018, COM (2018) 641 final
E4-06	Council Implementing Decision (EU) 2018/1696 of 13 July 2018 on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing Enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
E4-07	Annex to the Proposal for a Council Implementing Decision on the operating rules of the selection panel provided for in Article 14(3) of Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (''the EPPO''), Brussels, 25.5.2018, COM(2018) 318 final)
E4-08	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')

F) Data Protection

F-01	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (4.5.2016; OJ L 119/89)

G) Police Cooperation in the EU

G1) General

G1-01	European Commission, Press Release, „Commission marks ten years of judicial and police cooperation between between Member States of the European Union", 01 December 2019
G1-02	Regulation of the European Parliament and of the Council on establishing a framework of interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726 and (EU) 2018/1862 and (EU) 2019/816 [the ECRIS-TCN Regulation], PE-CONS 31/19, Brussels, 2 May 2019
G1-03	Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU
G1-04	Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/12; 06.08.2008)*
G1-05	Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime *(OJ L 210/1; 06.08.2008)*
G1-06	Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union *(OJ L 386/89; 29.12.2006, P. 89)*
G1-07	Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration of 27. May 2005 *(10900/05; 27.5.2005)*

G2) Joint Investigation Teams (JITs)

G2-01	Eurojust Information on JITs
G2-02	Third JIT Evaluation Report, Eurojust, March 2020
G2-03	Joint Investigation Teams Practical Guide (Brussels, 14 February 2017; 6128/1/17)
G2-04	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017

G2-05	Council Framework Decision of 13 June 2002 on joint investigation teams (*OJ L 162/1; 20.6.2002*)

PROSEARCH

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Internet searches and computer forensics

Damir Kahvedžić, PhD.

Damir.Kahvedzic@prosearch.com

Co-financed by the European Union

1

Presenters

Damir Kahvedžić

Senior Global Data Service Manager, ProSearch

Damir.Kahvedzic@prosearch.com

2

Scope

What are we talking about here?

How has the landscape of the internet **changed** post Covid

Internet vs social media. Web 1.0 v Web 2.0

Best practices on how to gathering online evidence correctly and **avoid** common pitfalls

Examples from select websites and social media

What we won't talk about

Legal stuff. **I am not a lawyer**

Anything **too** technical

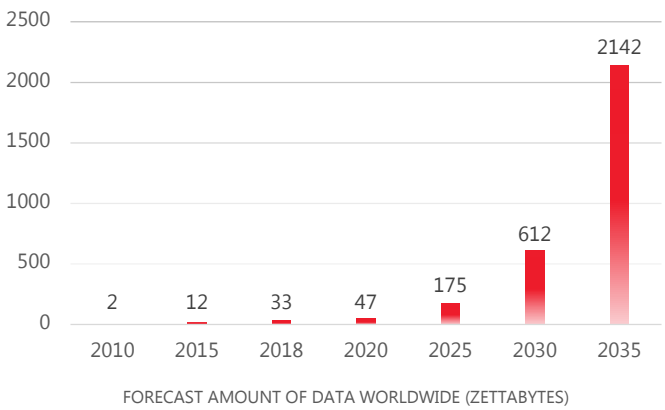
We don't have all the answers

Analysis…

PROSEARCH

3

By the Numbers



FORECAST AMOUNT OF DATA WORLDWIDE (ZETTABYTES)

Slack Daily Active Users 2022

25.7MM

Zoom Minutes in 2020

3.3TN

Teams Daily Active Users 2022

270MM

Emails Sent Per Second

3MM

PROSEARCH

4

By the Numbers

Internet Users	# Websites	Inactive Websites	Social Media Users
7B	1.1Bln	82%	4.26B

PROSEARCH

https://www.forbes.com/advisor/business/software/website-statistics/#:~:text=There%20are%20about%201.13%20billion,are%20actively%20maintained%20and%20visited.

5

PROSEARCH

Post Covid Landscape

Hybrid work drives the digitization of the Workspace

6

"Within the next two or three years, I predict most virtual meetings will move from 2D camera image grids--which I call the Hollywood Squares model, although I know that probably dates me--to the metaverse, a 3D space with digital avatars."

Bill Gates

2021 Year in Review

PROSEARCH

CONFIDENTIAL

7

"52% of employees are open to using digital immersive spaces"

"when compared to an audio-only call, people feel more engaged, more present, and even more comfortable when using an avatar in a meeting"

- Microsoft Worklab

Digitization of the workplace

Merging the **physical** and the **virtual** workplace

- our workplace is **already** digitized

IOT brings the home office to HQ

Digitization of more **nuanced** data

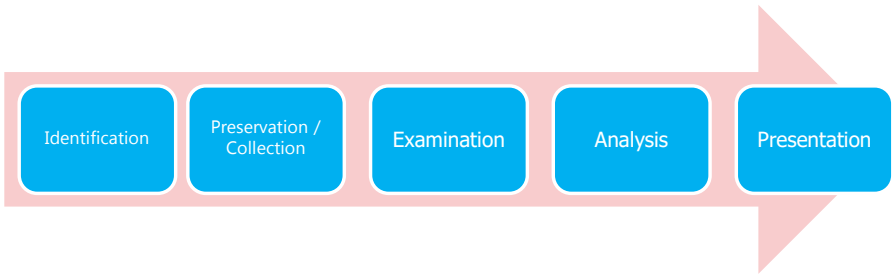
- movement, position and perspective
- sentiment
- intention
- emotion

PROSEARCH

CONFIDENTIAL

8

General Forensic Process



9

Digital Forensic Principles

ACPO Guidelines

Our aim is to preserve the information as accurately as possible. Can we do that?

ACPO Rule 1

That **no action** take is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

ACPO Rule 2

Where a person finds it necessary to access original data held on a digital device that the person must be **competent** to do so and able to explain their actions and the implications of those actions on the digital evidence to a Court.

ACPO Rule 3

That a **trail** or **record** of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third-party forensic expert should be able to examine those processes and reach the same conclusion.

ACPO Rule 4

That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed

10

PROSEARCH

Internet Basics

11

The anatomy of a webpage

At Source (server side)

A webpage can be considered as a collection of **elements**.

HTML is a markup language that tells the browser what elements to put where and how

1. Add some **text**
2. Reserve space for **photos**
3. Reserve space for **adverts**
4. Reserve space for videos stored on **YouTube**

I send my prepared page to an ISP who gives it a webpage name and makes it available to the WWW.

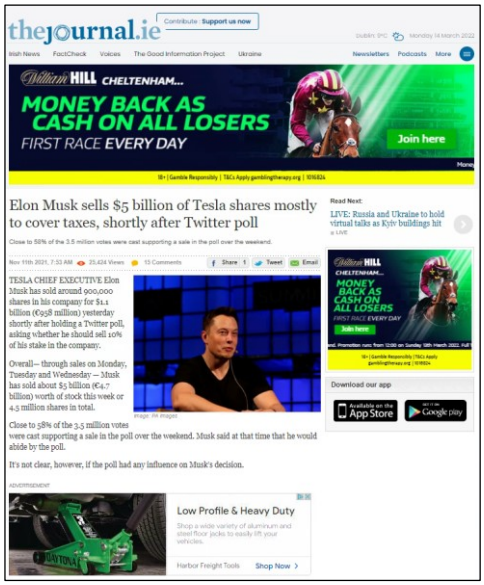
At destination (client side)

Users log into the webpage

The ISP server sends all elements of the webpage.

'Embedded' elements are retrieved from YouTube, Facebook etc.

The exact **final** look of the page may not be known to the creator



The anatomy of a webpage

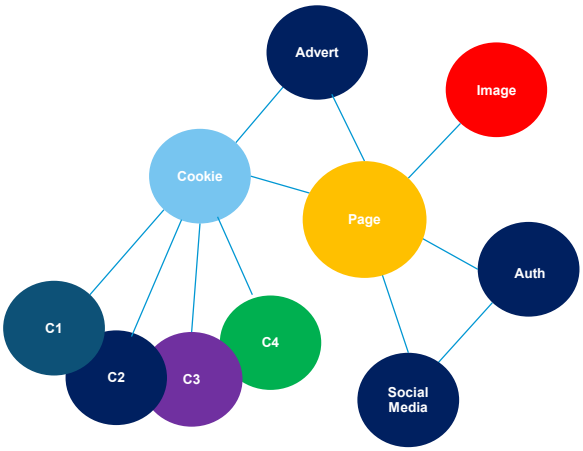
A single page is created using content from **multiple** sources and elements

71
Individual **Files** making the page

12
Distinct **Domains** the site is connecting to

0
Videos Downloaded

10
Adverts Downloaded



PROSEARCH

13

Webpage DNA

HTML is the source code of the page

It's a set of instructions to gather information and show it in the browser.

It also shows much more useful hidden information:

Exact URLs https://www.youtube.com/watch?v=tNRLZLK475A

Meta tag meta name="article:post_date" content=2021-02-10T08:44:03+000">

Comment tag <! – You can't see me 😎 –>

'Hidden' tag <input type="hidden">

PROSEARCH

14

Web 1.0 v Web 2.0 v Web3

Web 1.0

Name given to the **original** World Wide Web

Sites were created for **consumption** of content

Static web pages are created by any user with web creation software

Uses: HTML \ PHP \ CSS

Personal web pages were common but **simple**

The primary use is of **creating, disseminating and consuming** content

Little to no user **participation**

Web 2.0

A new iteration of how the web is used

Instead of a user consuming a web site's content the user is encouraged to **contribute** to make comments, edits and other participation.

Another name for Social Media or the Social Web

The pages are developed using advanced technology and usually administered by dedicated platforms

Communications is secured via **user accounts**

Accounts and participation is maintained by the service

Web3

A relatively new concept

Instead of the data of the web being centralised to the big tech companies, the data in Web3 is decentralised and controlled by the user

Based on cryptocurrency and blockchain

It could lead to a more secure and privacy focused web

Out of scope here.

The anatomy of Web 2.0

Templates

Rather than create a website from scratch, most providers make it simple by providing a template.

All you do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

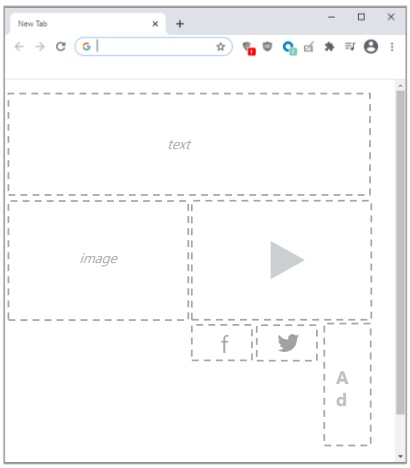
Social Media Sites

All use a template to make the page

The elements are stored in a databases

Once they are accessed the template and the database elements are sent together and assembled.

The final look is **consistent**. The framework of the page is the same with content different.



Social Media Platforms

Templates

Rather than create a website from scratch, most providers make it simple by providing a **template**.

All you do is to fill in the blanks

An explosion of personal content:

- Blogs
- vBlogs
- Personal websites

Social Media Sites

All use a template to make the page

The elements of the pages are stored in a database.

Once they are accessed the template is sent and the database elements

The final look is consistent. The framework of the page is the same with content different.

The data is stored in databases. This is what we are interested in, not the templated page structure.

The Social Web

Social Web

Social web is the term given to the proliferation of social interaction on web sites amongst users and between sites

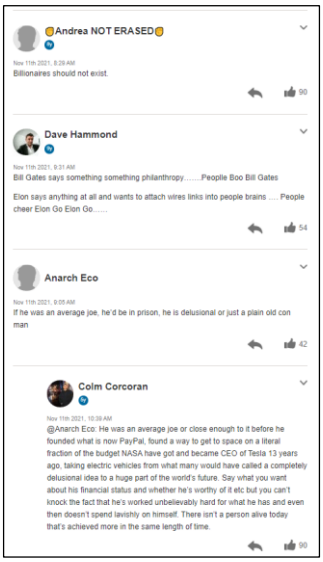
Examples include

- Conversations
- Comments
- Shop Reviews
- Forums
- 'Likes'

There are 4 main forum software providers.

There are 100,000s of **sites** with an indeterminate amount of posts, comments etc.

Provider	# Sites	Market Share
BuddyPress	108,062	59.8%
phpBB	18,169	10.05%
vBulletin	15,016	8.31%
Xenforo	10,159	5.62%



The Social Web

Boards.ie

A traditional forum that allows users to discuss wider arrays of topics

- A Single users can make many threads
- A Single thread can have many posts
- A Single post can have many 'thanks' or 'likes'
- A single thread can be found divided over a number of webpages.

Each object is access via dedicated web page URL. The ID of that element is in the HTML and not visible to the use

Forum software made by vBulletin

PROSEARCH

Internet Collections

Collections

Collection is the acquisition of potentially relevant electronically stored information

ESI and its associated metadata should be collected in a manner that is legally defensible, proportionate, efficient, auditable, and targeted.

The process of collecting ESI will generally provide feedback to the identification function which may impact and expand the scope of the overall electronic discovery process.

What are some of the techniques we have seen used. Which one is the best?

Screenshot

Technique

- Go to each webpage you need
- 'Photograph' static images of the webpages

Problem

- Very easy to fake
- Can't hash to compare and verify data
- Not preserving the background information (metadata)
- Need to manually browse the website which can expose your identity and affect what you see
- You may miss important information
- Slow
- Not recommended in isolation

Screencast

Technique

- Record dynamic images, video or the behaviour
- Ensures that the content is not modified

Problem

- Can't hash to compare and verify data
- Not preserving the background information (metadata)
- Need to manually browse the website which can expose your identity and affect what you see
- Slow

Save Webpage

Technique

- Click Save-As to save a copy of the webpage
- Save a webpage including images, text, and the background code.

Problem

- Dynamic elements of a webpage make verification difficult
- Does not download or save any 3rd party content (YouTube videos)
- Still have to go to every page individually
- Slow

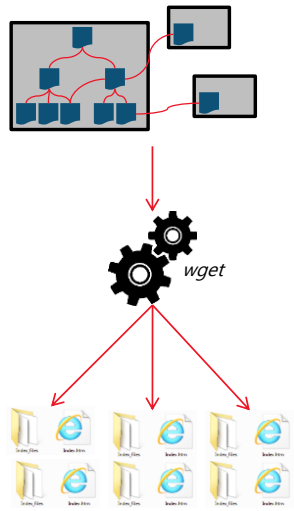
Save Script

Technique

- Download multiple pages all at once
- Can be tailored to follow any third-party links to download
- List the URLs to gather the lot
- Software: **wget, httrack**

Problem

- Fairly technical to set up
- Not suitable all sites (such as social media and HTML5)
- You need to list each URL individually
- May be thousands of pages to visit



PROSEARCH

CONFIDENTIAL

25

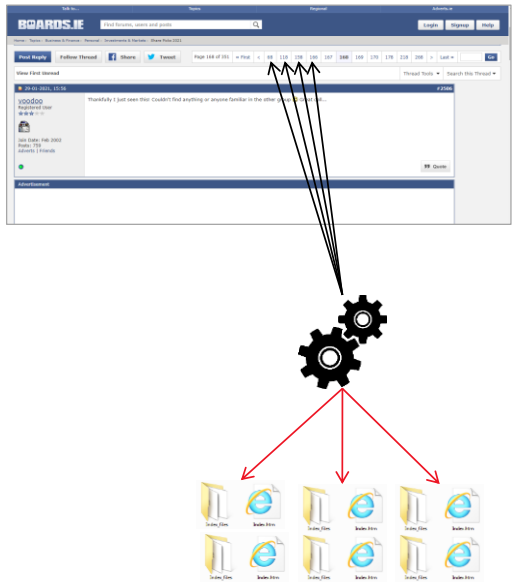
Screen Scraping

Technique

- Screen scraping is a technique where a tool is made to follow links just like a human would do on a page.
- Download all posts a user made as well as all of the responses for context
- Very easy analysis as well as preservation of how data looked originally

Problem

- Software needs to be created for every type of forum **vendor**
- **No known software that does it all.**



PROSEARCH

CONFIDENTIAL

26

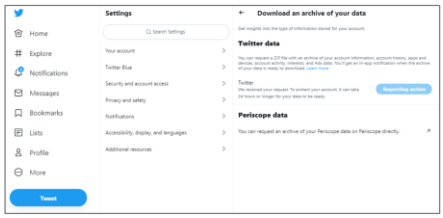
Data Export

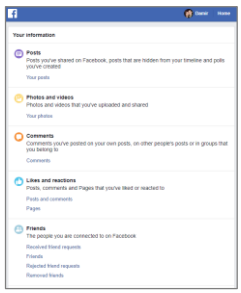
Technique

- Some social media platforms have a capability to export all your media out.
- Usually very simple to do and you should get your data in a nice readable form
- Available for: LinkedIn, Facebook, Twitter

Problem

- You need the credentials of the user to do this
- You are trusting the social network to extract a complete history
- Not available for most social web sites (Reddit, Boards.ie etc)
- The Data Source dictates HOW the data is exported. Some sources export their data in a series of PDFs which are difficult to review.
- Facebook export a mini website which is difficult to search





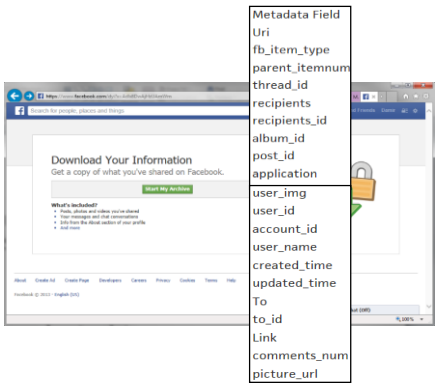
APIs

Technique

- Most Social Media platforms publish APIs and support protocols to allow software to connect and read data
- Collects much more than can be seen
- Can be automated easily
- Commercial professional tools exist

Problem

- Not all vendors support these functions
- APIs can be changed at any time without notice



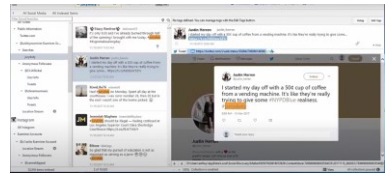
Collection Platforms

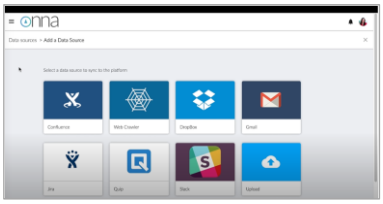
Page Freezer

X1 Discovery
- Supports: Twitter, Instagram, Facebook, Tumblr, YouTube and Online mail
- Downloads all components, hashes the files and maintains an audit trail

Magnet AXIOM
- Full fledged forensics software
- Support collections from Facebook only

Onna
- Supports Teams, Slack, Twitter, Confluence, Jira, Box, OneDrive, Sharepoint
- Download all accessible information and presents it in a usable fashion





Summary

Technique	Prove Authenticity	Scalable?	Easy to Use?	Easy to Review?	Applicability
Screenshot	No	No	Yes	Maybe	All sources
Screencast	Yes	No	Yes	No	All sources
Save Webpage	Yes	No	Yes	Yes	All sources
Save Script	Yes	Yes	No	Yes	All sources
Data Export	Yes	Yes	Yes	Maybe	Only the main sources
API	Yes	Yes	Yes	Yes	Only the main sources
Platforms	Yes	Yes	Yes	Yes	Only supported sources

Takeaways

Key Points

Online data is presenting a number of challenges. Social media is varied, dynamic, and may or may not be supported by the current tools.

Collections are difficult because of this variety. There is no perfect answer on which to use.

The main aim is to balance:

- preserving the **authenticity** of information so that it can be proven that it was not altered
- **readability** and **reviewability** of the result
- **reliability** and **scalability** of the technique

Relying on screenshots only is problematic. The data can be changed easily. The process is slow. The process is not scalable

If you need to collect data from social media. Understand how it operates, the tools available and their limitations. If relying on manual collection, use a tool that can record videos, screenshot, keep an audit trail, hash documents etc. If in doubt consult a specialist for advice.

PROSEARCH

31

PROSEARCH

Damir Kahvedžić | ProSearch | Solutions Advisor

Damir.Kahvedzic@prosearch.us

32

Handling e-evidence from a technical point of view

ERA
european.law

(POST) Covid Challenges in Criminal Justice:

E-EVIDENCE AS NEW EVIDENTIARY FRONTIER FOR EU LEGAL PRACTITIONERS

Dublin

20-21 April 2023

Co-funded by the Justice Programme of the European Union 2014-2020

About the speaker

- Victor Voelzow
- Police Officer since 2001
- Working in Digital Forensics since 2007
- MSc Forensic Computing and Cybercrime Investigations (UCD, Dublin, Ireland, 2011)
- Trainer at Hesse State University for Public Management and Security
- Projects, trainings, guides for different national and international organisations, e.g.:

Agenda

1. Challenges and potential of AI on the examples of large language models and image generators
2. Gathering specific information from open sources
   a) Reverse-image search
   b) Historical website data
3. Open-source tool collections

1.) Challenges and potential of AI on the examples of large language models and image generators

Disclaimer:

- Time is limited, thus there will just be a small theoretical introduction and only few slides.
- We will concentrate on use cases and demos for ChatGPT-4 and Midjourney.
- All results are just example outputs of the technologies used by the services at a particular moment of time.
- The technology may produce inaccurate information about people, places, or facts.

A brief history of AI

1950: Alan Turing proposes the Turing Test, which becomes a foundational concept in AI to evaluate a machine's ability to exhibit human-like intelligence.

1956: The Dartmouth Conference marks the birth of AI as a field. John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon organize the conference, where the term "Artificial Intelligence" is coined.

1959: Arthur Samuel develops a program that learns to play checkers, pioneering the concept of machine learning.

1964: Daniel Bobrow's STUDENT program becomes one of the first examples of natural language processing, demonstrating the ability to solve algebra word problems.

1969: Marvin Minsky and Seymour Papert publish "Perceptrons," critiquing the limitations of neural networks, leading to reduced interest in neural network research for several years.

1972: The development of the Prolog programming language by Alain Colmerauer and Philippe Roussel, which becomes the dominant language for AI research in the 1970s and 1980s.

1980: The beginning of the Expert Systems era, as AI systems such as MYCIN and XCON become popular for their ability to solve specific problems in domains like medicine and configuration.

A brief history of AI

1986: Geoffrey Hinton, David Rumelhart, and Ronald Williams publish a paper on backpropagation, a technique for training multi-layer neural networks, paving the way for the resurgence of neural network research.

1997: IBM's Deep Blue chess computer defeats the reigning world champion Garry Kasparov, marking a significant milestone in AI development.

2011: IBM's Watson defeats two human champions on the quiz show Jeopardy!, showcasing the progress of natural language processing and knowledge representation in AI.

2012: Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton win the ImageNet Large Scale Visual Recognition Challenge using a deep convolutional neural network, AlexNet, which dramatically outperforms previous models and ignites the deep learning revolution.

2014: Google acquires DeepMind, a British AI research company, and later achieves significant advancements in reinforcement learning, with AlphaGo defeating the world Go champion in 2016.

2018: OpenAI's GPT-2, a large-scale generative language model, demonstrates impressive text generation capabilities, raising concerns about AI safety and ethics.

2020: OpenAI's GPT-3, a more advanced version of GPT-2, sets new benchmarks in natural language processing, showcasing the potential for AI applications in diverse domains.

Three types of AI

1.Narrow AI (Weak AI):
- designed to perform specific tasks or solve particular problems
- often outperforming humans in these limited domains.
- Examples include image recognition software, speech recognition systems, and recommendation algorithms used by online platforms.
- Narrow AI operates within a predefined set of rules and is incapable of generalizing its abilities beyond the specific tasks it was designed for.

2. General AI (Strong AI):
- a system that possesses the ability to perform any intellectual task that a human being can do.
- can learn, understand, and apply knowledge across a wide range of domains, adapt to new situations, and exhibit human-like cognitive abilities.
- General AI remains a theoretical concept, as no AI system has yet achieved this level of intelligence.

3. Superintelligent AI:
Superintelligent AI is a hypothetical type of AI that surpasses human intelligence in virtually every domain. It would possess greater problem-solving and creative capabilities than even the most intelligent humans. Superintelligence raises concerns about ethical considerations, AI safety, and the potential impact on human society, as its development could lead to unprecedented and unpredictable consequences.

AI use cases for law enforcement

1. Machine Learning (ML): Used for **crime prediction, risk assessment**, and **document analysis**. Techniques like supervised learning, unsupervised learning, and reinforcement learning can be employed to analyze data and make predictions.

2. Predictive Analytics: Predictive analytics involves using historical data and statistical algorithms to make predictions about future events. In the context of law enforcement and the judiciary, predictive analytics can be employed to **forecast crime hotspots, identify potential recidivism, and assess the risk of individuals involved in legal proceedings**.

3. Deep Learning (DL): Deep learning is a subfield of machine learning that uses artificial neural networks to model and solve complex problems. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are two popular types of deep learning architectures. Deep learning has proven effective in **image and speech recognition**, making it highly relevant for **surveillance, facial recognition, and voice analysis** in law enforcement.

AI use cases for law enforcement

4. Natural Language Processing (NLP): NLP is a branch of AI that focuses on enabling computers to understand, interpret, and generate human language. NLP techniques can be employed in the judiciary for tasks such as **legal document analysis, case law research, and court transcription**. **Sentiment analysis, entity recognition, and text summarization** are some of the NLP methods applicable in this domain.

5. Anomaly Detection: Anomaly detection is a technique used to identify unusual patterns or outliers in data that do not conform to expected behavior. In law enforcement, anomaly detection can be used for **fraud detection, cybercrime investigation, and monitoring social media for potential threats**.

6. Computer Vision: Computer vision is an interdisciplinary field that deals with enabling computers to interpret and understand visual information from the world. It has applications in law enforcement for tasks such as **surveillance, facial recognition, and analyzing crime scene images**.

AI case-studies law enforcement

Case Study 1: PredPol - Predictive Policing

PredPol is a predictive policing software that uses machine learning algorithms to analyze historical crime data and predict potential crime hotspots. The software generates real-time recommendations for patrol routes, enabling police departments to allocate resources more efficiently and prevent crimes before they occur. In a pilot project in Los Angeles, the LAPD reported a significant reduction in crime rates after implementing PredPol.

Case Study 2: NEC NeoFace - Facial Recognition

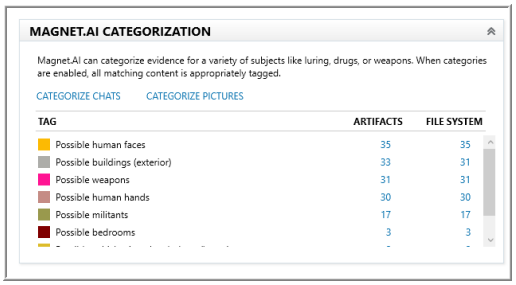
NEC's NeoFace is a facial recognition system that uses advanced AI algorithms to accurately match faces in real-time, even with low-resolution images and partially obscured faces. Law enforcement agencies around the world have adopted NeoFace for various applications, such as identifying suspects, locating missing persons, and enhancing security at public events. In 2018, South Wales Police successfully used NeoFace to identify and arrest several suspects during a major soccer match, marking the first arrest made using live facial recognition technology in the UK.

AI case-studies law enforcement

Case Study 3: ShotSpotter - Gunshot Detection and Location

ShotSpotter is an AI-driven system that utilizes acoustic sensors and machine learning algorithms to detect, locate, and alert law enforcement agencies of gunfire incidents in real-time. The system analyzes audio data to distinguish gunshots from other noises, providing accurate location information to police officers within seconds. Several cities in the United States, including New York City, Chicago, and San Francisco, have deployed ShotSpotter to reduce response times to shooting incidents and enhance public safety.

Further case-studies:



Picture source: Derek Eiri, https://mreerie.com

First demo: done ;)

The contents of all slides, that carried this logo were produced by ChatGPT-4.

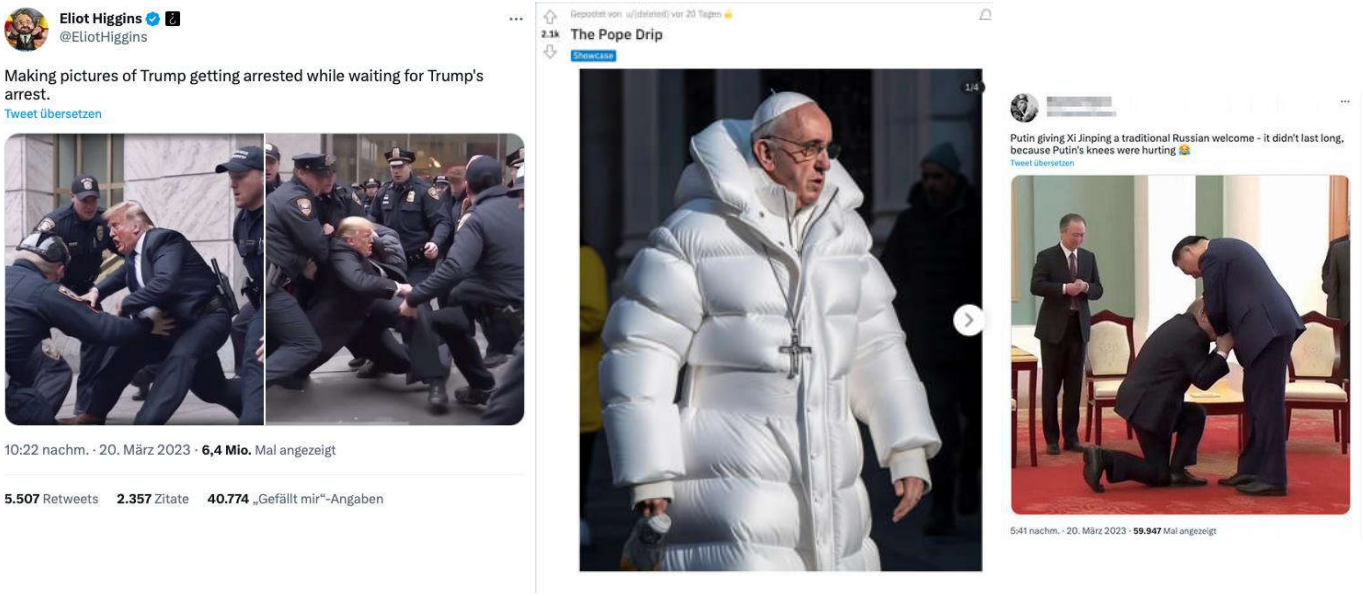
Impact on law enforcement

https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement (27/03/2023)

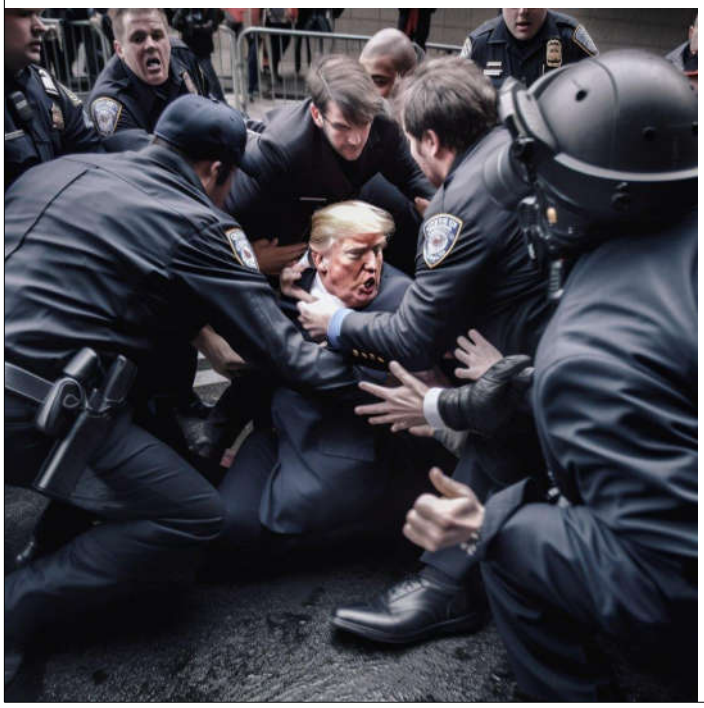
Demos ChatGPT-4 & Midjourney

Picture source: http://clipart-library.com/clipart/demo-cliparts_2.htm

The challenge of generated images…



A few examples



A few examples

A few examples

Demo

Picture source: http://clipart-library.com/clipart/demo-cliparts_2.htm

How to identify generated images?

- Visual inspection:
  - odd number of fingers
  - Deformations/transformations
  - incorrect perspective, dimensions, forms
  - Incorrect / missing shadows/highlights
- Image reverse search: Google images, Tineye, Yandex
- Picture analysis tools: e.g. Forensically https://29a.ch/photo-forensics/#forensic-magnifier

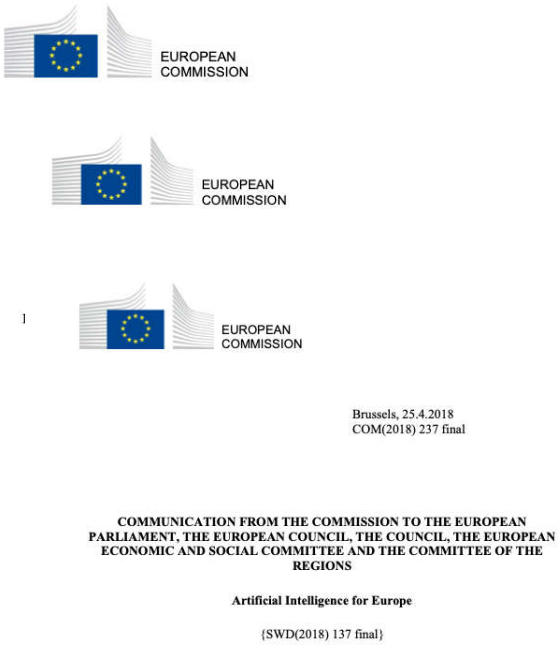
Potential countermeasures

- Visual / hidden Watermarks for fake media
- Visual / hidden Watermarks for real media (e.g. cryptographic signatures)
- Regulation?!

EU's response to AI

- EU AI Strategy
  https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

- In April 2021, the Commission presented its AI package, including:
  - its Communication on fostering a European approach to AI;
  - a review of the Coordinated Plan on Artificial Intelligence (with EU Member States);
  - its proposal for a regulation laying down harmonised rules on AI (AI Act) and relevant Impact assessment.


EUROPEAN COMMISSION

EUROPEAN COMMISSION

1

EUROPEAN COMMISSION

Brussels, 25.4.2018
COM(2018) 237 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Artificial Intelligence for Europe

{SWD(2018) 137 final}

2. Gathering specific information from open sources

a)Reverse-image search

Example: Google image search

a)Historical website data

Example:

3. Open-source tool collections – just a few

a) Forensic software list
https://github.com/Cugu/awesome-forensics

b) Malware Analysis list
https://github.com/rshipp/awesome-malware-analysis

c) Incident Response list
https://github.com/meirwah/awesome-incident-response

d) OSINT
https://osintframework.com

Demo

Picture source: http://clipart-library.com/clipart/demo-cliparts_2.htm

Questions?

Please ask!

Electronic Evidence

Seminar at the European Academy of Law
April 2023

With the support of the European Union

Klaus Hoffmann, Senior Prosecutor, Freiburg

1

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

E-EVIDENCE AS THE NEW EVIDENTIARY FRONTIER FOR EU LEGAL PRACTITIONERS

Klaus Hoffmann, Senior Prosecutor, Freiburg

2

3

Online investigations and the challenges of dealing with electronic evidence in criminal proceedings

- Principles of dealing with electronic evidence
- Common procedures for recognizing and handling evidence on digital devices in Germany
- International investigations (search and seizure – obtaining evidence from the Internet, admissibility)
- challenges and possible solutions

3

quick introduction

4

- different kinds of electronic evidence - examples

→ Think of digital devices in your daily life incl. :

- many SIM cards in moderns cars,
- smart home devices,
- smart phones,
- smart refrigerators,
- washing machine and other electronic / smart devices

4

Principles of dealing with electronic evidence

5

- no specific regulations in the (German) Criminal Procedure Code
- various (soft) regulations within different authorities (e.g. police, federal authorities like the German Federal Office for Information Security (BSI))
- best practices and efforts to certificate certain IT forensic software
- general principles of dealing with analogue evidence also apply to digital / electronic evidence

5

Principles of dealing with electronic evidence

6

key aspect:

- ensuring authenticity of digital data
- chain of custody
- proper and detailed documentation of access to data, its storage, copying and analysis
- analysis and further work with digital data is only done with a copy, not the original set of data
- proper documentation of the police staff that is involved and the IT forensic software that is being used

6

How is digital evidence handled in German courts??

7

limited categories of evidence

- witness testimony
- expert testimony
- documentary evidence
- evidence by inspection(e.g. photos, videos, tangible objects like a gun)

▶ Digital evidence has to be presented in one of those categories.

7

How is digital evidence handled in court??

8

- case examples (WhatsApp messages, child porn files, telecommunication data)
- extra note on IT expert witnesses
- analysis of Bitcoin evidence - extra group of Landeskriminalamt (state police) to collect and analyse bitcoin evidence across many cases

8

Procedural rights (1)

9

- challenging the gathering of evidence
- Challenging authenticity of e-evidence
- motion to call extra (expert) witness
- cross-examination
- motion not to admit certain evidence

9

International investigations

10

- **Increased relevance of electronic evidence in criminal investigations**
  - increased volume of cross-border requests submitted by EU authorities to OSPs in 2019 with a large majority of them issued by Germany (37.7% of requests), France (17.9%) and the UK (16.4%)
  - requests to access electronic data doubled in Poland and nearly tripled in Finland. Furthermore, emergency disclosure requests increased by nearly half in one year.

10

International investigations (search and seizure – obtaining evidence from the Internet, admissibility)

11

- case: Online webshop for selling drugs
- European Investigation Order to seize date in The Netherlands
- here: especially bank data or records of orders of the webshop
- first step: seizure of data according to national law
- second step: transfer – how? digital - by which means or analogue: print out?

11

International investigations / admissibility

12

- case law by the German Federal Court: based on the idea of mutual trust – evidence obtained by means of MLA / EIO is in general admissible
- if requirements under German procedural law are fulfilled
- and international cooperation according to law on mutual cooperation has been applied

- how about direct access to online data? →

12

Proposed EU order

13

European production and preservation order (EPO) (COM/2018/225 final)

- relates to specific telecommunication data and social media files
- doesn't address the regular access to electronic evidence in other countries
- example: access to digital data seized from a webserver in France or Spain
- controversy discussion at the European Parliament; see e.g.: *review of Stanislaw Tosza in* Eucrim 4/2018

13

another example: access to Facebook data

14

- *access to an open account*
- *access to a closed account of a suspect*
  - *invitation to any other user (e.g. "Micky Mouse")?*
  - *restricted access – undercover agent needed?*
- *suspect/ witness opens his account to be used by police*

▶ *for more details see: Eucrim 3/2012 (p. 137 et seq.)*

14

Challenges and solutions

15

- **challenges in retrieving relevant data from abroad**
  - **length of relevant procedures in place**
  - **language barrier**
  - **different legal procedures and competences**
  - **very limited time that data is stored**
  - **different standards on cooperation by private companies**
  - **encrypted communication**

15

Challenges and solutions

16

- **Training, knowledge exchange and a centralised approach**
  - technical training of judges / lawyers
  - hiring more and better trained staff at the police (and in judiciary)
  - technical equipment in court
  - special point of contacts with private companies
  - GPEN – network of the IAP
  - SIRIUS – exchange platform of Europol /Eurojust

16

Challenges and solutions

17

- **issues at domestic level**
  - similar issues as before
  - technical equipment in court
  - technical training of judicial staff
  - massive volume of data (IT solutions like Palantir?)
  - new legal tools to deal with encryption?
  - despite specific rules on electronic evidence – its presentation and admission is mostly not a problem

17

Procedural rights (2)

18

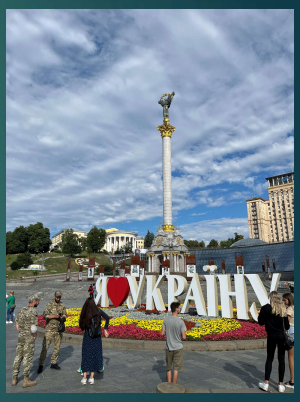
- limited challenges to cross-border gathering
- motion not to admit certain (internationally gathered) evidence
- in theory possible: motion to gather additional / exculpatory evidence across borders

18

Digital war crimes evidence

19

- Countless videos and photos, both from private phones/ cameras and official cameras / drones
- OSINT information
- Radio and other communication
- Investigations by ICC and at least 20 third countries
  - Different procedures and data format in place
  - Unclear how such data can be exchanged across borders
- Big issue: possible fake video and photos
- The Berkeley Protocol (on Digital open source investigations)
- IT solution for big data collection and analysis



19

Questions / Comments?

20

- For any comments or questions, please feel free to contact me:

Klaus Hoffmann
Staatsanwaltschaft Freiburg
Heinrich-von-Stephan-Straße 1, D-79100 Freiburg
email: klaus.hoffmann@stafreiburg.justiz.bwl.de
Currently on leave: hofklaus@yahoo.com

20

Faculté de Droit, d'Économie et de Finance

The collection of evidence located abroad and the challenges of cross border access to data

Assoc. Prof. Dr. Stanislaw Tosza
University of Luxembourg

20 April 2023

Co-financed by the European Union

1

Criminal investigation in cyberspace

- **Cross-border access to data**
  - The need to gather/have access to data
- **Cloud computing**
  - The problem of territoriality
- **European enforcement challenges in the online context**
  - Conflicting rules
  - Yahoo and Skype cases
- **Shortcomings and remedies**
  - Shortcoming of the MLA system
  - EIO – a remedy for e-evidence?
  - EPOR – proposal, negotiations and outcome

2

Criminal investigation in cyberspace

- Need to gather data
- Role of data in global economy and private life
- Ability to combat crime – ability to to access data
- Not only cybercrime

Territoriality and limits of enforcement

- Territoriality – concept
- Jurisdiction to prescribe
- Jurisdiction to enforce
- France v. Turkey (S.S. Lotus):

  [45] "The first and foremost restriction imposed by international law upon a State is that – failing existence of a **permissive rule to the contrary** – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".
- Ex. of exception: Art. 41 CISA

Criminal investigation in cyberspace – Jurisdiction – Cybercrime convention

Article 32 –Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

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

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

European enforcement challenges

Territoriality

Loss of location

Encryption problem

Enforcement capacity limitation

Cooperation of service providers

European enforcement - legal challenges

- **Mutual legal assistance and its shortcomings**
  - Functioning of the MLA system
  - MLA for data and US: probable cause
- **Problem of cooperation with the US: the blocking provision**
  - 18 U.S.C. § 2702
  - Content data vs Non-content
  - Microsoft Ireland Case
- **Unilateral / extended jurisdiction – "Belgian approach"**
  - Yahoo case
  - Skype case
  - Code d'instruction criminelle

European enforcement – solutions?

- **Voluntary cooperation**
  - Practice
  - Problems
- **European Investigation Order**
- **E-evidence initiative**
  - European Production/Preservation Order Regulation (EPOR)
  - Directive on appointment of legal representatives
- **Solution to the US problem of the blocking provision**
  - CLOUD Act
  - US-UK Agreement
- **Second Protocol to the CoE Cybercrime Convention**

Getting data under European Investigation Order

- European Investigation Order – a general instrument to gather data cross-border within the EU
- Mutual recognition
- EIO is a judicial decision to have specific investigative measure(s) carried out in another MS with the objective to obtain evidence
- Production orders?
- Issuing authority and addressee (executing authority)
- Measure must be available in the issuing state and ordered under the same conditions as would be necessary to its issuance in a similar domestic case.
- Necessity and proportionality
- Deadlines: 30 days and 90 days
- Grounds for refusal
- Remedies

European Production/Preservation Order

The justification for the need for a EU setting

- Internal EU reasons
- External reasons ⟹ Negotiations with the US

Basic premises of the new system

- Mutual recognition
- Area of Freedom, Security and Justice (taken seriously)
- Lack of territoriality as principle

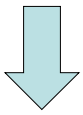
European Production/Preservation Order

State of play:

EU Commission's proposal – 04.2018

EU Council's General Approach – 12.2018

Position of the EU Parliament – 12.2020



Trialogue negotiations ended in 01.2023

Political agreement reached

European Production Order – Issuing

1. **Categories of data**
   - subscriber data
   - data requested for the sole purpose of identifying the user'
   - traffic data
   - content data
2. **Issuing authorities**
   - judge
   - court
   - investigating judge
   - prosecutor
3. **Conditions of issuing**
   - necessary and proportionate
   - availability of a similar measure in the national system
   - type of offence (transactional data or content data)

European Production Order – Reaction

4. Reception

- Legal representatives
- Directive
- Consequences of lack of legal representative

5. Reaction

- Role of notification
- Production of data
- 10 days/6 hours
- Problems with identifying / producing data

European Production Order – enforcement

6. Enforcement

- Enforcing State/authority
- Grounds for refusal

7. Sanctions

- Pecuniary
- Member States
- Who?

European Production Order – remedies

8. Remedies

- Member States
- Undefined

9. Conflict with other legal systems

- Problem
- Procedure

European Production Order – assessment

Positives:

- Solution
- Legal framework
- Time

Problems (some…):

- Mutual trust / legal basis
- Position of the service provider
  - Conflict of laws
  - Human rights choices
- Sanctions
- Remedies
- Relationship with the European Investigation Order
- Notification

CoU – Cybercrime Convention

- 2nd Additional Protocol to the Budapest Convention on Cybercrime
- Art. 6, 7.
- Open for signature since 12 May 2022

Contact

- stanislaw.tosza@uni.lu

Further reading:

- Stanislaw Tosza, *All evidence is equal, but electronic evidence is more equal than any other. The relationship between the European Investigation Order and the European Production Order*, New Journal of European Criminal Law 2/2020, https://journals.sagepub.com/doi/full/10.1177/2032284420919802
- Stanislaw Tosza, *Internet service providers as law enforcers and adjudicators. A public role of private actors*. Computer Law & Security Review: The International Journal of Technology Law and Practice, 2021, Vol. 43, https://doi.org/10.1016/j.clsr.2021.105614
- Stanislaw Tosza, *The public role of private actors: Internet service providers in the E-Evidence proposal*, European Law Blog 20 September 2022, available at: https://europeanlawblog.eu/2022/09/20/the-public-role-of-private-actors-internet-service-providers-in-the-e-evidence-proposal/
- 2023: Vanessa Franssen, Stanislaw Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press

Faculté de Droit,
d'Économie
et de Finance

Assoc. Prof. Dr. Stanislaw Tosza

The collection of evidence located abroad and the challenges of cross border access to data

Thank you for your attention !!

Questions?

19

Microsoft

Cooperation with EU public agencies

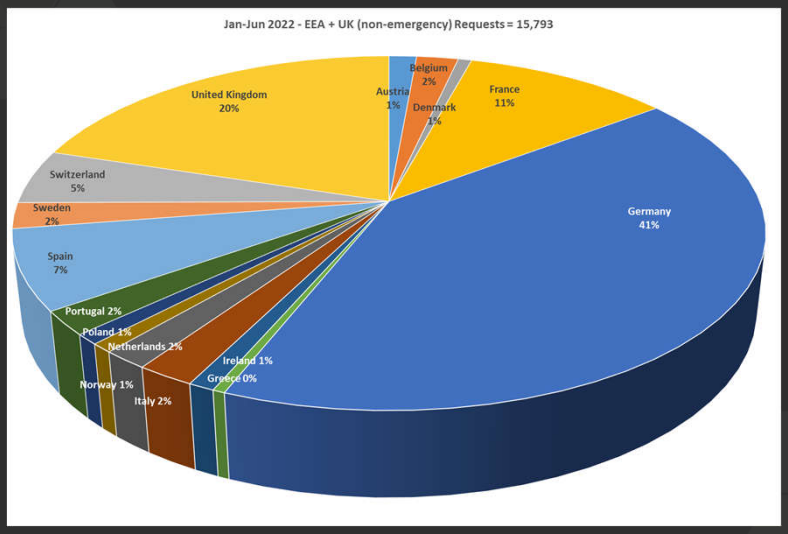
Aisling Kelly, Assistant General Counsel
Law Enforcement & National Security

April 2023

Co-financed by the European Union

1

Microsoft Transparency Report - 6 monthly volume of legal orders



2

What we will talk about today

Legal landscape in the EU

Different data types

Practical issues

International law outside EU

3

Legal landscape in the EU

4

Current legal landscape in the EU

EU27 domestic orders

Different legal thresholds

MLATs too slow

Inherent GDPR tension

5

GDPR concepts which impact on law enforcement

- Data processor
- Data controller (enterprise data)
- Lawfulness of processing – Article 6
- Data minimsation
- Purpose limitation
- Principles for third country transfers
- Europol's EDEN event, September 2023

6

What does the Microsoft Law Enforcement team do?

Legal review of each order

Conducts a user check

Rejects orders where appropriate

Produces responsive data

7

What does the Microsoft Law Enforcement team not do?

Does not provide direct access to any government

Does not break encryption

Does not provide encryption keys

Does not respond to an Order without a valid identifier

8

Lawful Intercept Orders

- European Electronic Communication Code
- Extends definition of an Electronic Communication Service to number independent services – VoIP, email, IMs
- Member States can amend surveillance laws for intercept capability
- Microsoft will receive these orders via API – application programming interface
- Germany, France, Belgium
- European Technical Standards Institute

9

Cooperation between public and private entities

- eEvidence Regulation
- Integrated data platform for eEvidence between law enforcement and service providers
- Data management and cybersecurity
- Recognition of international data storage conflicts of laws

10


Data types

11

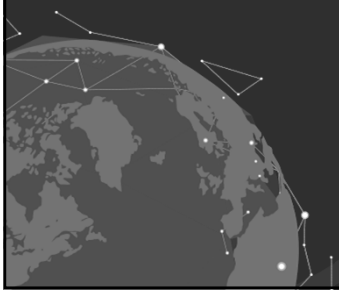

Outlook
Microsoft Azure
Windows
Skype
Windows Live Hotmail
Teams
OneDrive
Bing
XBOX 360

12

Microsoft Account

Non content data:

- Registration data: name, address, time zone.
- Alias
- Phone Number
- Alternate E-Mail
- Last 30 days or last successful login (if available) including date and time
- Billing information
- Services utilised



13

What is an identifier?

- Email address – any type not only Microsoft hosted, Gmail, iCloud etc
- Phone number
- Skype id (always has a live: prefix)
- Passport User id (Decimal or hexadecimal versions)
- Full credit card number
- Customer id (visible in the OneDrive URL)

14

Location data

15

Skype

username	number	country	provider	start_time	end_time	deliver_time
S[redacted]ple	123456789	FR	Voxbone	2019/03/11 14:59:12	2019/04/11 14:59:06	2019/03/11 14:59:18

Skype ID:
live:.cid.5c7867e50860ae3
live:lenstraining

PSTN dialed number with exact date, time and duration of call: +123145648974

Skype Number with a date range: +123145648974 or Victim's number to whom the call was placed

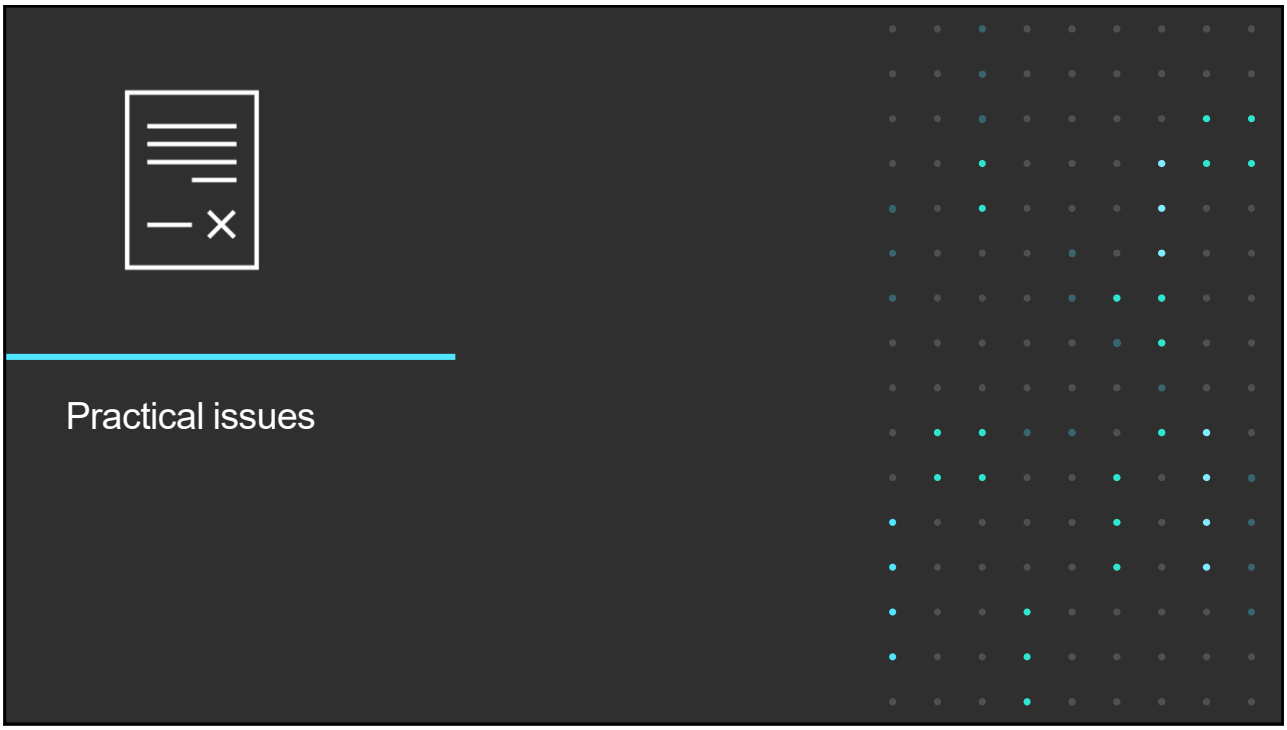
Caller ID (Phone pumber): +123145648974

Skype Order Number

Full Credit Card Number (full 16 digit number)

ALL communications between Skype users are stored in the Chat history: IMS, CDRs, Media files, SMS

16

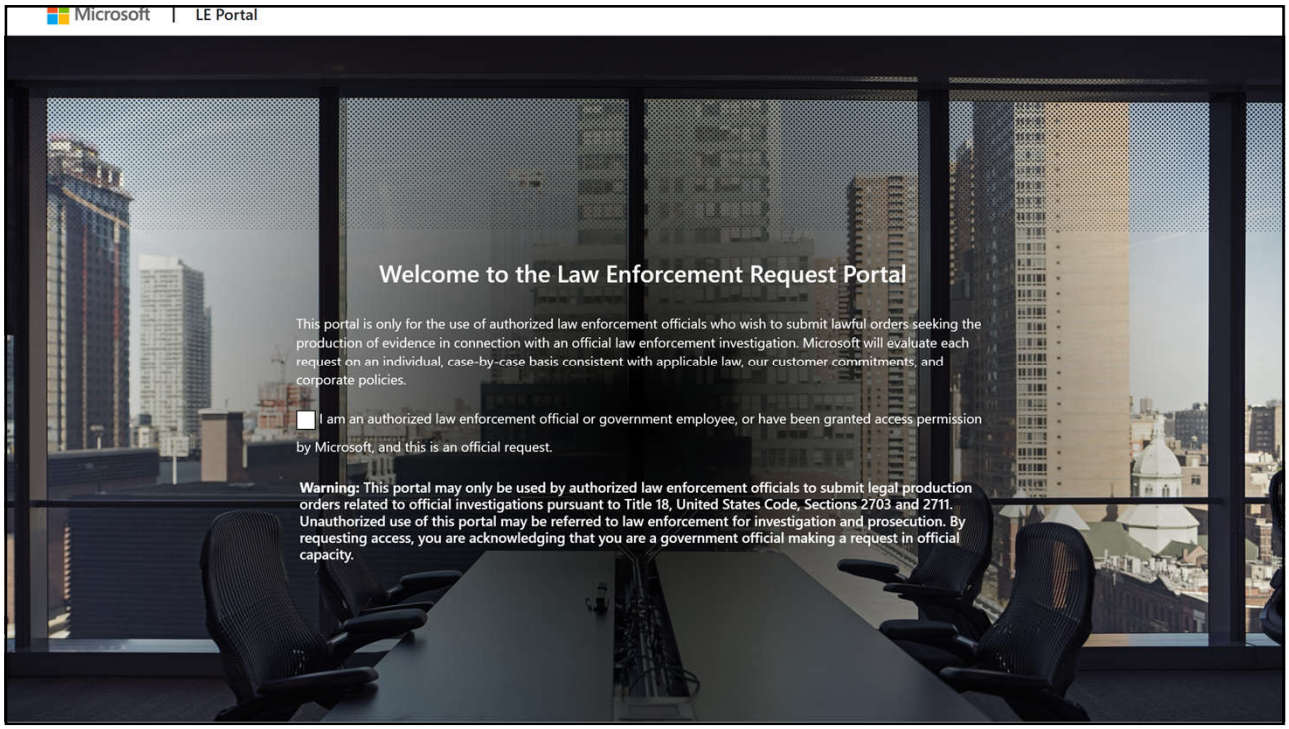


17

What is required in a legal order?

- Must be addressed to the EU data controller; Microsoft Ireland Operations Limited
- Must reference Microsoft services (Outlook etc) with an identifier
- Must include a date range and nature of criminal offence
- Must be signed (wet signature or electronic)
- Must specify production or preservation
- Must take responsibility for extending any preservation past 180 days pending MLAT

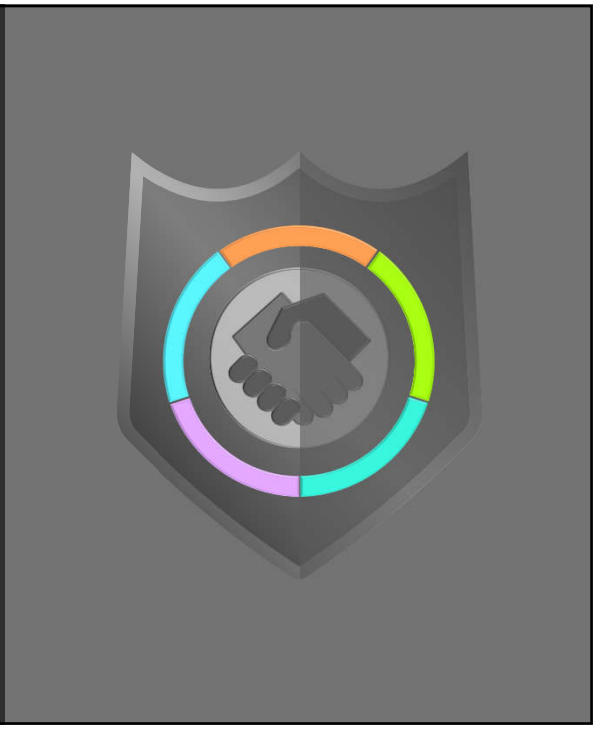
18



19

Emergency data disclosure

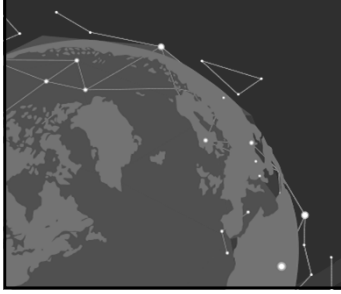
- Must be an immediate threat-to-life situation
- Do not use the Microsoft Law Enforcement Portal
- Submit via 24/7 e-mail to: **lealert@microsoft.com**
- All requests must be addressed to **Microsoft Ireland Operations Limited**
- Must state the facts of the emergency
- Must request what data is sought
- Can use Microsoft's **Emergency Form or headed and signed public agency letter**



20

Authenticating eEvidence

Algorithm : SHA256
Hash :
3CBCFDDEC145E3382D592266B
E193E5BE53443138EE6AB6CA09
FF20DF609E268



Hashing of files, used in computer security

It uses a secure hash algorithm (SHA) for any piece of data

Microsoft uses SHA256 – each zip file is hashed – digital fingerprint

Allows you to know that two files are identical, once you generate the return hash for trial

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.3

21

International law outside the EU

22

Geolocation of users

USA – Stored Communication Act, ECPA

India

Japan

Korea

Brazil

EU / US Cloud Act

US based messaging apps Discord, Snap

UN Cybercrime Treaty

OECD Trusted Government Access Declaration

2nd Additional Protocol to Budapest Convention

University of Antwerp
Faculty of Law

The European Investigation Order (EIO) and its effectiveness in collecting evidence abroad

Prof. dr. Joachim Meese
associate professor
attorney

Co-financed by the European Union

1

Introduction and background

- e-evidence, MLA, EIOD, and EPO in a nutshell -
- historical background -

University of Antwerp
Faculty of Law

2

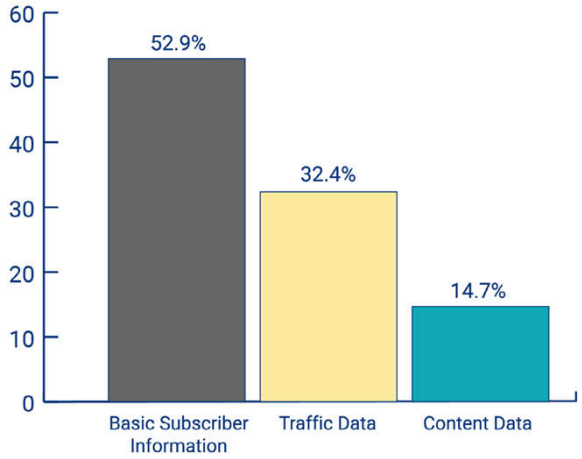
most common types of e-evidence

- **basic subscriber information**
  - e.g. name, e-mail, phone number, …
- **traffic data**
  - e.g. connection logs, number of messages, …
- **content data**
  - e.g. photos, content of messages or e-mails, files, …

3

most common types of e-evidence

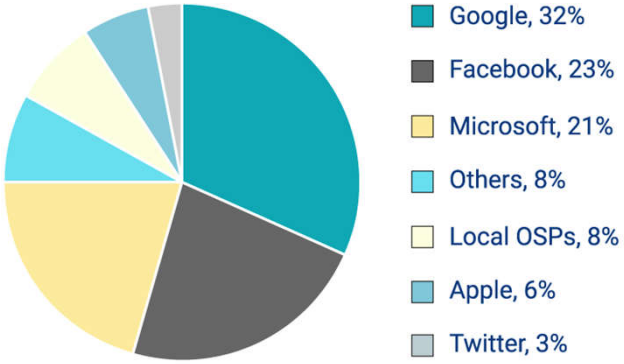
- **most often needed type of e-evidence from foreign authorities or online service providers in 2019:**



4

most common types of e-evidence

- **three most contacted online service providers in 2019:**



5

characteristics of e-evidence

- **volatile, can easily and quickly be deleted**
- **cross-border**
  - according the Commission 85% of criminal investigations require electronic evidence
  - approx. 2/3 of electronic evidence is located in another State (both within and outside the EU)
- **necessity for quick intervention**
- **hard to locate and access evidence**
  - e.g. in cases where the origin of cyber attacks or location of e-evidence is not (yet) known
  - data redundancy

6

dealing with e-evidence

- **cloud-stored data: what about jurisdiction?**
  - possible theories:
    - criminal event theory (territorial)
    - criminal instrument theory (territorial)
    - direct consequence theory (extra-territorial)
    - nationality principle theory (extra-territorial)

7

dealing with e-evidence

- **key aspects:**
  - ensuring authenticity of digital data
  - chain of custody
    - proper and detailed documentation of access to data, its storage, copying and analysis (without changing the data)
    - analysis and further work with digital data is only done with a copy, not the original set of data
    - proper documentation of the police staff that is involved and the IT forensic software that is being used
  - see ACPO Good Practice Guide for Digital Evidence

https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

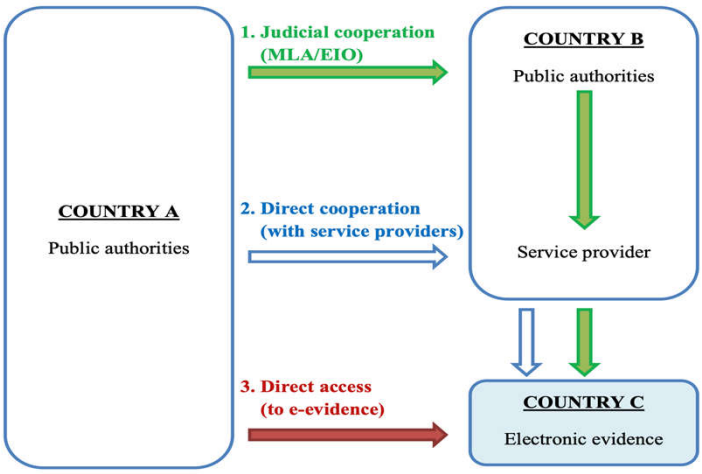
8

dealing with e-evidence

- **common procedures for recognising & handling e-evidence**
  - in most European member States: no specific regulations
    - e.g. Belgium
  - therefore:
    - general principles of dealing with analogue evidence also apply to digital/electronic evidence
    - (soft) regulations within different authorities (e.g. police, federal authorities like the Belgian FCCU)
    - best practices and efforts to certificate certain IT forensic software
    - legislation on the international/European level

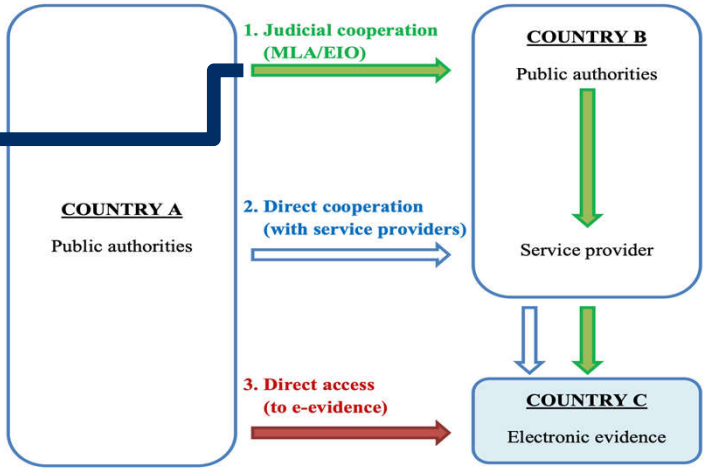
cross-border access to evidence

- **possible scenarios:**



cross-border access to evidence

- **possible scenarios:**



- ✓ within EU: EIO
- ✓ outside EU: international agreements
  - Budapest Convention on cybercrime
    - 2nd additional protocol can be signed by MS in the interest of the EU (Council decision of 5 April 2022)
      - ✓ improve international cooperation
      - ✓ enhance direct cooperation
      - ✓ emergency mutual assistance
  - bilateral agreements concluded by
    - the EU (e.g. the agreement with the US of 23 October 2009)
    - the member States (most frequently with the US, Canada or Australia)

University of Antwerp
Faculty of Law

11

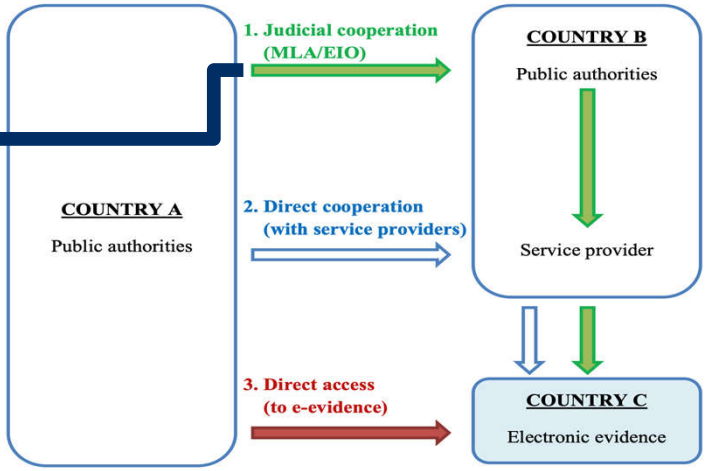
11

cross-border access to evidence

- **possible scenarios:**

number of requests per year on e-evidence:

- ✓ between EU member States: 13.000
- ✓ EU MS to US: 1.300



University of Antwerp
Faculty of Law

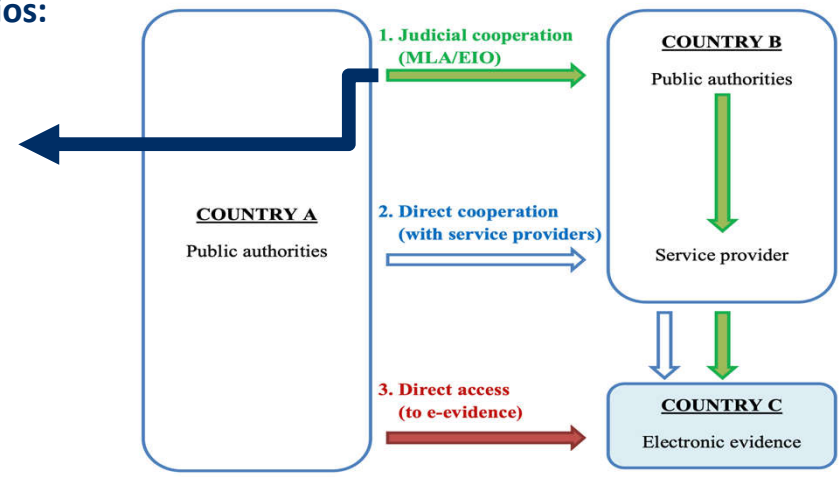
12

12

cross-border access to evidence

- **possible scenarios:**

✓ MLA challenges
- hard to get a timely response to a request
- too much formalities
- too complicated and technical to use

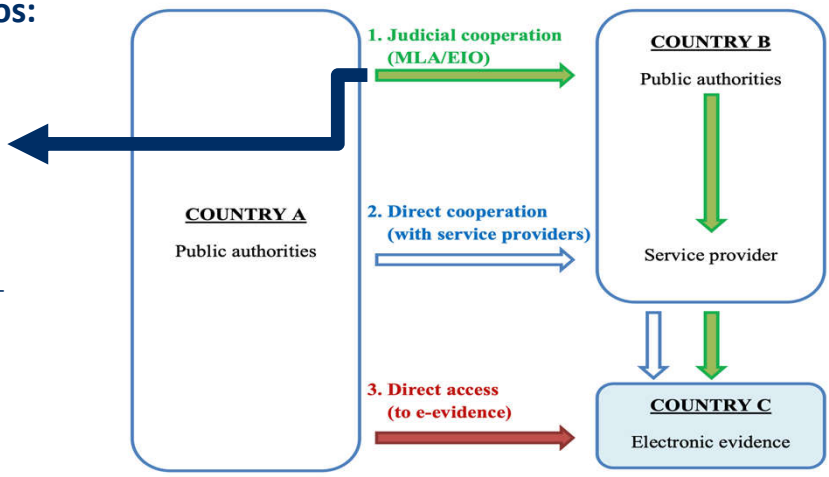


13

cross-border access to evidence

- **possible scenarios:**

✓ EIO challenges
- Ireland, Denmark and UK are not bound
- too slow for e-evidence
- too formalistic for e-evidence
- not adapted to complex e-evidence situations
- high cost and capacity requirements
- legal impediments



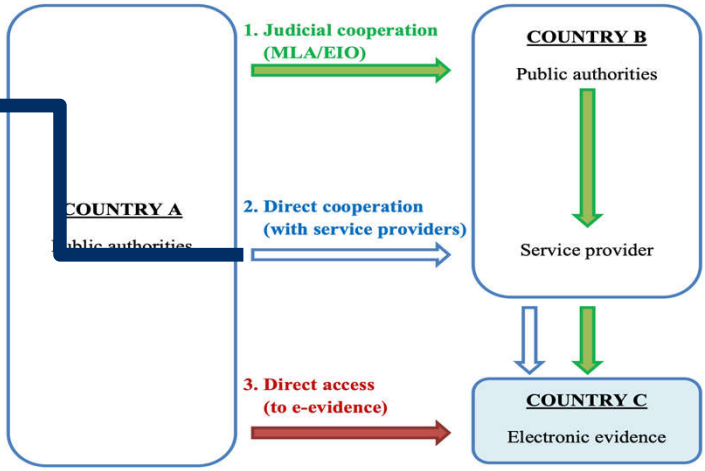
14

cross-border access to evidence

- **possible scenarios:**

✓ non-content data
- service providers established in the US and, to a more limited extent, in Ireland, which reply directly to requests from EU member States law enforcement authorities on a voluntary basis

✓ WHOIS data
- service providers make data directly available to authorities through a centralised search system which does not rely on individually reviewed requests

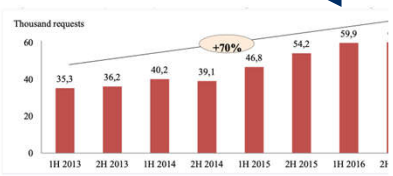


15

cross-border access to evidence

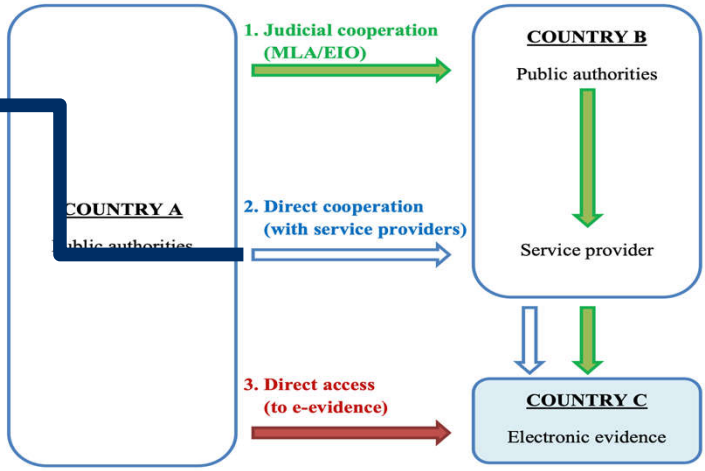
- **possible scenarios:**

numbers:



→ in 2018, 3 member States account for > 75% of all requests from the entire EU
- Germany: 35.271
- UK: 28.598
- France: 27.268

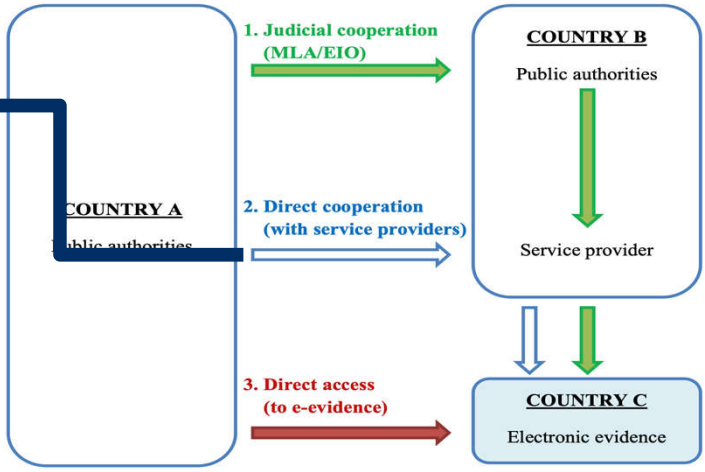
→ Google & Facebook: 70% of total requests



16

cross-border access to evidence

- **possible scenarios:**

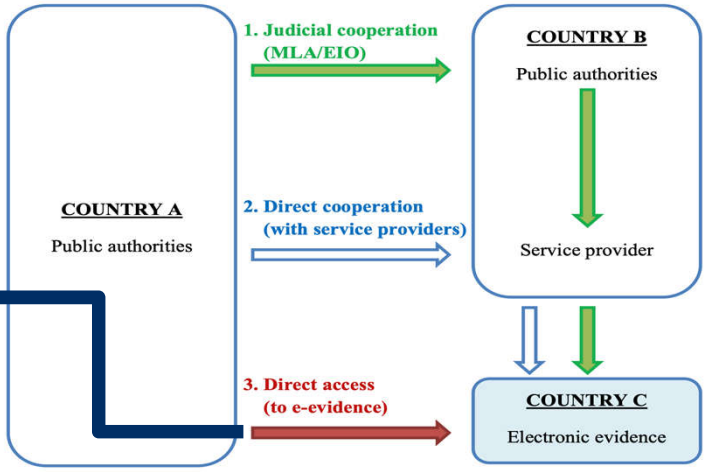


✓ challenges
- can be unreliable
- can take too long
- only possible with a limited number of service providers
- providers all apply different policies
- not transparent
- lacks accountability in case of non-compliance
  - see, however the Belgian case of YAHOO! (Cass. 1 December 2015, P.13.2082.N)

17

cross-border access to evidence

- **possible scenarios:**



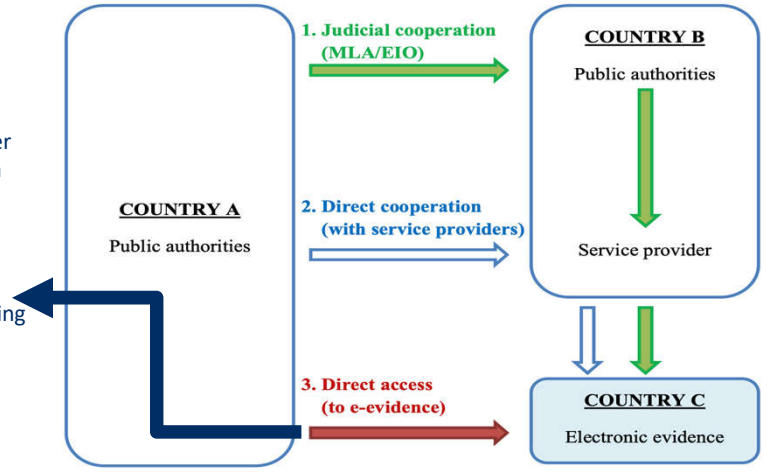
✓ extended search (following seizure of a device)
✓ remote search (following lawful acquisition of login information)

→ possible under national law of at least 20 member States
→ this tool becomes more relevant
- data are regularly stored on servers in a different location
- in case of loss of knowledge of location of data (e.g. Darknet)

18

cross-border access to evidence

- **possible scenarios:**



✓ challenges
- different approaches by member States to direct access & to data storage location
- risk of losing data
  - ✓data can easily and swiftly be deleted from another device
  - ✓data can be lost when gathering and moving it

19

cross-border access to evidence: what about EPO?

- **EPO (not into force yet)**
  - what: legal framework laying down the rules under which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data
    - European Production Order (EPOC)
    - European Preservation Order (EPOC-PR)
  - title: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters
  - background: driven by the fight against terrorism
    - establishing security is one of top policy priorities of the EU
    - an instrument for transnational access to e-evidence in the EU is a pressing issue

20

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - original Commission proposal (17 April 2018)
      - https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0225/COM_COM(2018)0225_EN.pdf
    - the Council's general approach (11 Juni 2019)
      - https://data.consilium.europa.eu/doc/document/ST-10206-2019-INIT/en/pdf
    - Report Committee on Civil Liberties, Justice and Home Affair (11 December 2020)
      - https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html
    - Report from the Commission to the European Parliament and the Council (20 July 2021)
      - https://data.consilium.europa.eu/doc/document/ST-11007-2021-INIT/en/pdf
      - launch of EU-US negotiations to facilitate access to electronic evidence: 19 July 2021
    - Draft regulation:certain issues (26 August 2021)
      - https://db.eurocrim.org/db/en/doc/3646.pdf

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - State of play and possible ways forward (16 September 2021)
      - https://www.statewatch.org/media/2739/eu-council-e-evidence-regulation-state-of-play-11681-21.pdf
      - Report of 20 December 2021: https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html
      - update of 23 February 2022: https://www.statewatch.org/media/3175/eu-council-e-evidence-4-col-doc-regulation-6487-22.pdf
      - letter of EP's rapporteur (16 February 2022): https://www.statewatch.org/media/3174/eu-council-e-evidence-mep-rapporteur-letter-6323-22.pdf
    - Final compromise text (20 January 2023): https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf

cross-border access to evidence: what about EPO?

- **EPO**
  - texts & sources
    - Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings
      - https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2018:226:FIN
      - general approach: https://data.consilium.europa.eu/doc/document/ST-7348-2019-INIT/EN/pdf
      - final compromise text (20 January 2023): https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf

23

Comparative scheme: key characteristics

MLA

- traditional instrument of international cooperation
- all kinds of investigative measures
- important in the relationship with third States, mainly with the USA
- complex, lots of formalities, takes time

EIO

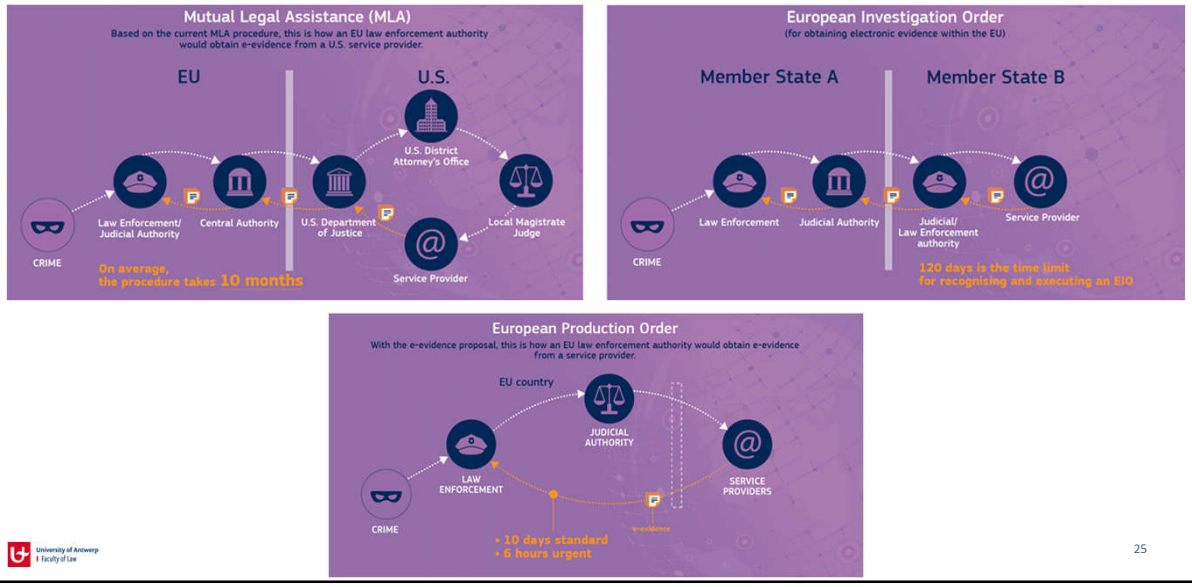
- all kinds of investigative measures (except in the framework of JIT)
- inspired by mutual recognition
- execution by domestic authorities or by third parties
- in theory within 120 days
- Directive

EPO

- only for electronic information
- restricted to criminal proceedings
- directly addressed to service provider and to executing authority
- some orders can be issued for all criminal offences and for most types of data stored
- location of data is not relevant
- a new type of cooperation instrument based on advanced form of mutual trust
- (extraordinary?) simplification of procedure
- Regulation (no transposition!)

24

Comparative scheme: visual representation



University of Antwerp
Faculty of Law

25

More about EIO

- basic premise & scope -
- procedure -
- challenges and limitations -

University of Antwerp
Faculty of Law

26

EIO – basic premise

- **Replace existing legal framework by creating 1 single legal instrument (introductory remark 7 EIOD)**
- **Mutual recognition (art. 1(2) EIOD)**

  => inspired by:
  - mutual recognition of judgments and judicial decisions
  - mutual recognition of orders to prevent the destruction, transformation, moving, transfer or disposal of evidence
  - European evidence warrant
  - European arrest warrant

  ⇒ principally an instrument for the authorities to gather evidence abroad
  - the EIOD doesn't regulate the position of the defence, e.g. possibility to be present at the execution of specific investigative measures (such as witness examination), or the right for the defence to have a EIO issued

27

EIO – including e-evidence?

- **Applicable to any investigative measure (art. 3 EIOD):**
  - including gathering of e-evidence
  - except in framework of Joint Investigation Team (JIT)
- **In the context of e-evidence:**
  - specific provisions on the interception of telecommunications (art. 30 EIOD)
  - no other specific provisions regarding electronic evidence
    - except for a reference to the identification of a person holding an IP address or telephone number (art. 10(2)(e) EIOD)

28

EIO - procedure

- **EIOD: procedural steps (1/3)**
  1. national request prepared and judicially approved based on individual national standard and EIO rules (art. 5-6 EIOD)
     - particular form + content requirements: art. 5 EIOD + Annex A
     - translation of the EIO is required (art. 5, §3 EIOD)
  2. EIO sent directly to relevant judicial authority in relevant country (art. 7 EIOD)
     - by any means capable of producing a written record to guarantee authenticity
     - via the telecommunications system of the European Judicial Network
     - via E-Codex (https://www.e-codex.eu)

EIO - procedure

- **EIOD: procedural steps (2/3)**
  3. EIO examined by receiving judicial authority
     - verification of EIO (art. 5-6 EIOD)
     - verification of grounds of refusal
       - ➢ important in a cybercontext:
         - ✓ similar investigative measure exception (art. 11 (c) + (h) EIOD)
         - ✓ dual criminality exception (art. 11 (e) + (g) EIOD)
         - ✓ fundamental rights exception (art. 11 (f) EIOD)
  4. execution
     - executed directly by domestic investigative authorities OR
     - EIO served and then executed (if possible) by third parties (e.g. service provider)
     - recourse to a different type of investigative measure (art. 10 EIOD)

EIO - procedure

- **EIOD: procedural steps (3/3)**
  5. evidence is sent back to executing judicial authority (art. 13 EIOD)
  6. costs: art. 21 EIOD
     - borne by the executing State
     - if exceptionally high: possibility to share or modify

31

EIO - procedure

- **EIO: timeline**
  - in theory: within 120 days (art. 12 EIOD)
    - 30 days for Member States to decide to accept request
    - then 90 days to execute requested investigative measure
    - unless urgency
  - but …
    - many consultation options (art. 6(3) EIOD, art. 7(7) EIOD), art. 10(4) EIOD, art. 11(4) EIOD, art. 21(2) EIOD)
    - grounds for non-recognition or non-execution (art. 11 EIOD)
    - grounds of suspension of transfer of evidence (art. 13(2) EIOD)
    - grounds for postponement of recognition or execution (art. 15 EIOD)
    - legal remedies (art. 14 EIOD)

32

EIO - procedure

- **EIO: specific regimes**
  - see Chapter IV EIOD
  - Relevant from e-evidence perspective: *the interception of telecommunications* (chapter V)
    - art. 30 §§7-8 + 31 EIOD
    - important aspects from an e-evidence perspective:
      - ➢ EIO shall be sent to only one Member State if more Member States are available to provide technical assistance
      - ➢ possibility to request decoding or decrypting of the recording
        - BUT no obligation
      - ➢ notification of Member State where the subject of the interception is located from which no technical assistance is needed

33

EIO - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - territorial limitations
    - only EU countries
      - ⇒ no access to data held by service providers headquartered in non-EU countries
    - Ireland, Denmark and UK are not bound by the Directive
      - ⇒ no access to data held by service providers headquartered in these countries
      - ⇒ particularly in Ireland and UK a number of US service providers store data and have European headquarters
  - too slow for e-evidence
  - too formalistic for e-evidence?
    - long EIO forms to be completed
    - EIO translation is required
    - impossibility to directly address service providers

34

EIO - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - not adapted to complex e-evidence situations, where:
    - a number of information systems are used simultaneously in multiple jurisdictions to commit one single crime
    - relevant e-evidence moves between jurisdictions in short fractions of time
    - sophisticated methods are used to conceal the location of e-evidence or the criminal activity, leading to "loss of location"
  - high cost and capacity requirements
    - significant investment of resources/capacity from the receiving Member State, which may not be appropriate or necessary for all cases, especially when there is no link with the receiving jurisdiction besides the seat of the service provider
    - specialised training/personnel required to collect e-evidence in an appropriate manner

35

EIOD - challenges and limitations

- **EIO: challenges in the field of e-evidence**
  - legal impediments
    - on investigative acts-level:
      - ➢ risk for inconsistent interpretations
      - ➢ risk for conflicts between existing regulations
        - ✓ e.g.: dual criminality-requirements, domestic equivalent of investigative acts, …
      - ➢ 'limitations' due to data protection (art. 20 EIOD) and fundamental rights requirements
        - ✓ e.g.: obligation to decrypt vs. privilege against self-incrimination
    - on evidence level
      - ➢ no 'free movement' of evidence or minimum standards for evidence-gathering
      - ➢ risk of important discussions on admissibility/authenticity of e-evidence in criminal procedures due to different domestic standards
        - ✓ e.g. SKY ECC procedures
        - ✓ e.g. Cass. Belgium 11 January 2022, P.21.1245.N (https://juportal.be/content/ECLI:BE:CASS:2022:ARR.20220111.2N.1/NL)

36

Thank you!

@ joachim.meese@uantwerp.be
www.linkedin.com/in/joachimmeese/
@JoachimMeese

University of Antwerp
Faculty of Law

37

Hessisches Ministerium der Justiz

HESSEN

Ransomware, Online Child Sexual Abuse and Non-Cash Payment Fraud

E-EVIDENCE AS THE NEW EVIDENTIARY FRONTIER FOR EU LEGAL PRACTITIONERS

Dublin
20-21 April 2022

With the support of the European Union

Rainer Franosch, Deputy Director-General for Criminal Law
Ministry of Justice of the German Federal State of Hesse

Hessisches Ministerium der Justiz

HESSEN

Ransomware

- **Ransomware was once again the primary overall cybercrime threat. The threat and damage potential increased noticeably again in 2021.**
- **2021 was characterized by attacks on critical infrastructures, public administration and international supply chains. In addition to monetary damage, such attacks also impair the ability of the community to function.**
- **The damage potential of ransomware is increasing rapidly.**
- **Annual damage caused by ransomware**

2021: approx. € 24.3 billion

2019: approx. € 5.3 billion

Hessisches Ministerium der Justiz

HESSEN

The Emotet investigation

Hessisches Ministerium der Justiz

HESSEN

The Emotet investigation

EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Emotet opened doors for:

- Trojans
- Ransomware
- Information stealers

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

HESSEN

What was Emotet?

- Emotet was a prolific spam-based malware and botnet.
- During its lifespan, Emotet sent billions of spam phishing emails and infected millions of victim computers.
- Emotet caused hundreds of millions of dollars in total loss. Some cybersecurity researchers estimate more than two billion in loss.

HESSEN

What was Emotet? (cont'd)

- As malware, Emotet was identified by cybersecurity researchers as early as 2014 as a banking Trojan.
- Over time, Emotet evolved into a loader or dropper of other malware, including ransomware: Trickbot (and Ryuk), Dridex, Qakbot, IcedID/Bokbot, and ZeuS Panda.
- Malware-as-a-Service

HESSEN

Emotet disruption

- In January 2021, Emotet was dismantled through an international effort coordinated through Eurojust.
- It was important to understand the technical details of the malware and its distribution and control infrastructure.
- Equally essential was focusing on people, in particular the Emotet server administrator.

HESSEN

How was Emotet spread?

- Emotet malware spread primarily through spam phishing emails with malicous scripts or attachments.
- Spam was targeted against particular countries and industries with custom attachments.
- During initial infection, victim computers downloaded Emotet malware from a distribution server and then received instructions from control servers.

HESSEN

Characteristics of Emotet malware

- Emotet malware was polymorphic, meaning parts of the code changed periodically.
- Emotet could detect being run in a virtual machine.
- Emotet harvested credentials from the victim computer and then spread within the network by brute-force guessing credentials to other networked computers.

HESSEN

Emotet malware (cont'd)

- Emotet malware on victim computers was hard-coded with Internet Protocol (IP) addresses of control servers.
- The malware cycled through these IPs until making a successful connection. Then, every 15 minutes, the malware was updated, including new control server IPs.
- Other malware, including ransomare, was loaded through Emotet.

HESSEN

Emotet tiered infrastructure

- Emotet distribution and control networks were tiered.
- Tier 1 servers, which tended to be compromised servers, communicated with Tier 2 servers, which communicated with Tier 3 servers.
- All communications were encrypted.

HESSEN

Why was Emotet so prolific?

- The Malware: Relentless spam campaigns. Persistence within networks. Updated every 15 minutes.
- The Infrastructure: Tiered distribution and control servers. Multiple epochs. Different encryption keys.
- Scale: By January 2021, there were more than 1500 distribution and control servers located in more than 60 countries.

HESSEN

The beginning of the investigation

- Phenomenological evaluation on Emotet by the BKA.
- Malware analysis by the BKA.
- In August 2018, the BSI shared the address of a server hosted in Brazil from which Emotet was being downloaded and whose log files were freely accessible.

HESSEN

The beginning of the investigation

- In these log files, a technical address of a server hosted at a provider in Germany relevant within the Emotet infrastructure could be detected.
- Cybercrime Center of the GPPO Frankfurt started a formal investigation, wire-tapping this server – many should follow.

HESSEN

Who has been affected in Germany?

- Courts
- Federal agencies
- Municipalities
- Hospitals
- Medical practices
- Universities
- Schools
- Companies

HESSEN

The Emotet investigation

HESSEN

International partners
Law enforcement agencies and judicial authorities from 7 countries:

The Netherlands:	*Politie* and *Landelijk Parket*
USA:	*Federal Bureau of Investigation, U.S. Department of Justice* and *US Attorney's Office for the Middle District of North Carolina*
Canada:	*Royal Canadian Mounted Police*
UK:	*National Crime Agency und Crown Prosecution Service*
France:	*Police Nationale* and *Tribunal Judiciaire de Paris*
Ukraine:	*National Police of Ukraine (Національна поліція України) and Prosecutor General's Office (Офіс Генерального прокурора)*
Lithuania:	*Lithuanian Criminal Police Bureau (Lietuvos kriminalinės policijos biuras) and Prosecutor General's Office of Lithuania*

HESSEN

Coordination of international cooperation

EUROJUST

Conferences coordinated by Eurojust for the development of common strategies and the exchange of information between representatives of law enforcement agencies and judicial authorities from the participating countries, with the involvement of representatives of Europol on a regular basis.

EUROPOL

HESSEN

Challenges and solutions

Planning of an international action day with joint actions in individual countries, including national measures as well as measures by way of mutual legal assistance under COVID-19 restrictions

- **operational centers at Europol and Eurojust with colleagues on site as well as supporting video conferences**
- **national operational centers**

HESSEN

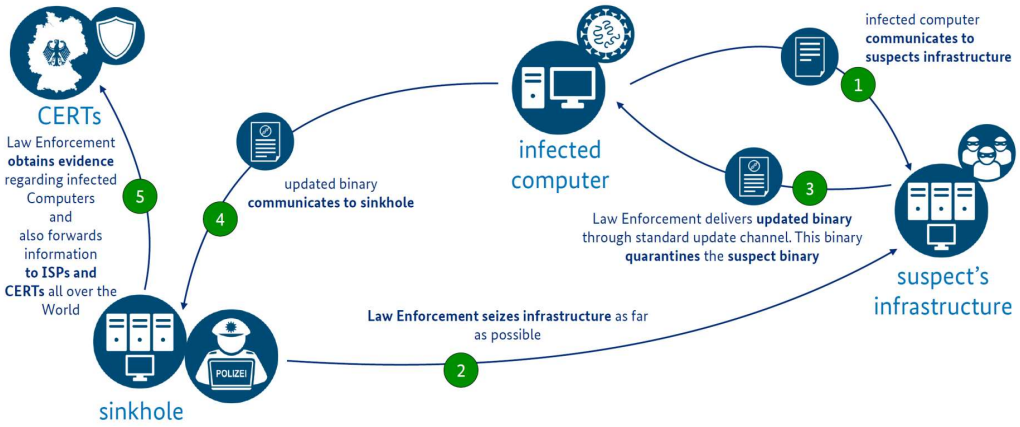
Challenges and solutions

Legal basis of rerouting the traffic of the purely IP-based, constantly changing Emotet infrastructure

- **„ hybrid court order" with elements of seizure, as well as the usage of the so-called annex competence with extension to systems newly discovered through technical measures**

HESSEN

Challenges and solutions



HESSEN

Challenges and solutions

Limits of the legal and factual implementation possibilities of the measures in the countries involved, in particular the legal transfer of the measures requested by way of mutual legal assistance

- **requests for legal assistance were prepared in close coordination with colleagues from the requested and requesting countries**

HESSEN

State of play

- Takeover of the bot net through joint action within the framework of the international action day on 01/26/2021
- Searches of the accused and two witnesses in Ukraine with subsequent interrogations
- Seizure of servers in Germany (victim control site, distribution site and unique bots) as well as in NL, USA, Canada, UK, France, Lithuania and Ukraine
- Evaluation of the data is ongoing – as well as the chase…

HESSEN

Online Child Sexual Abuse

HESSEN

What has the COVID-19 pandemic changed?

- The global impact of COVID-19 means people are spending more time online. This includes both children and adults.
- Adults working remotely are less able to spend time with their children, who are allowed greater unsupervised internet access. As a result, children are:
  - more exposed to offenders through online gaming, the use of chat groups in apps, unsolicited contact in social media and through less secure online educational applications;
  - more inclined towards making explicit material to exchange with peers, eventually reaching child sex offenders;
  - in some cases, becoming lonely and isolated, which offenders try to benefit from, connecting with them to produce explicit material or to arrange a meeting in real life.

HESSEN

2021-2022 trends

- There has been a steep increase in online grooming activities on social media and online gaming platforms.
- The production of selfgenerated material is a key threat. This material is displaying increasingly younger children.
- The Dark Web remains an important platform for the exchange of child sexual abuse material (CSAM).

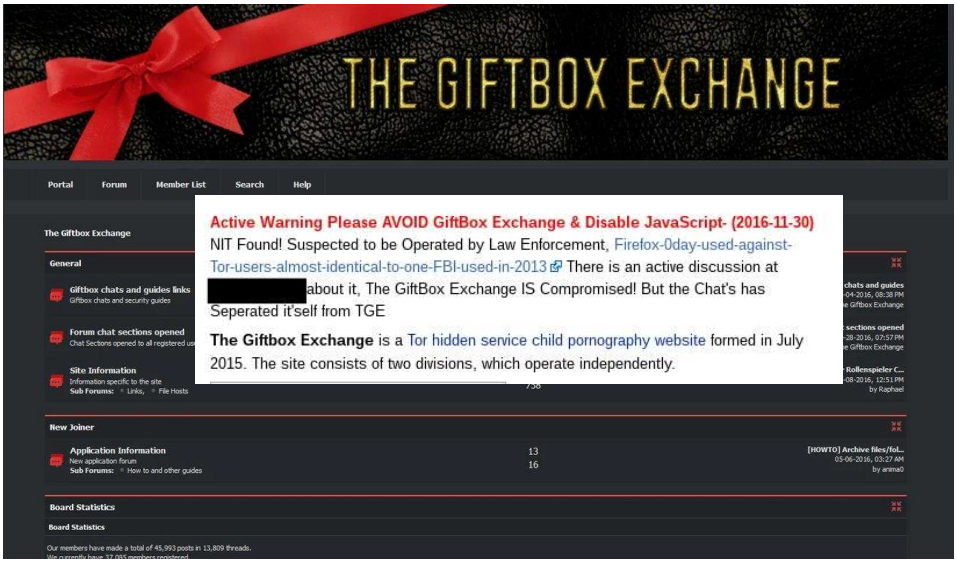
HESSEN

2021-2022 trends

- There has been a steep increase in online grooming activities on social media and online gaming platforms.
- The production of selfgenerated material is a key threat. This material is displaying increasingly younger children.
- The Dark Web remains an important platform for the exchange of child sexual abuse material (CSAM).

HESSEN

Operation ARTEMIS (The Giftbox Exchange / Elysium) – a combined approach



HESSEN

"Those Who Live by Anonymity, Die by Anonymity"

"Criminals are attracted to the dark net and Bitcoin due to the perceived anonymity that these technologies provide. TOR browsers and other programs limit law enforcement's ability to track IP traffic back to the target. Dark net marketplaces by their very nature are unfriendly to law enforcement. (…) The use of these anonymizing technologies gives criminals a sense of invulnerability.

And that is how we get them.

As any experienced investigator will attest, de-anonymizing criminals on the internet is as much a matter of psychology as technology."

Matthew J. Cronin, Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT'Y BULL. (July 2018), p. 65 et seq.

HESSEN

"Those Who Live by Anonymity, Die by Anonymity"

"Dark net operators rely heavily on the powerful shield of anonymity that the dark net and cryptocurrencies provide them. Use their greatest asset against them. Just as agents cannot immediately identify a dark net target, the dark net target cannot identify an agent. Cloaked in the same anonymous technology, a well-trained federal agent can infiltrate any dark net criminal community. Operating undercover on the dark net, agents are able to generate tremendous amounts of information about their targets, potentially becoming a target's valued customer or even a "friend." That is especially true when an undercover agent gains access to an account with significant criminal transaction history (and thus digital street cred) or, even better, has longstanding ties to the target."

Matthew J. Cronin, Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies, 66 U.S. ATT'Y BULL. (July 2018), p. 65 et seq.

HESSEN

Operation ARTEMIS

- In May 2016, Australian LEA (Taskforce ARGOS) were being offered access to the account details of a European moderator of the CSAM darknet site "The Giftbox Exchange" by a third-party LEA.
- This European agency sought out Taskforce ARGOS due to the stricter regulations placed on controlled operations in its own jurisdiction.
- At the same time, another CSAM forum, "Child's Play", was founded.
- Officers monitoring the Giftbox Exchange suspected a connection with Child's Play due to a range of similarities in messages posted by Giftbox Exchange moderator CuriousVendetta and Child's Play founder WarHead.

HESSEN

Operation ARTEMIS

- Both usernames could be traced to a Canadian man, Benjamin Faulkner, who was subsequently arrested along with Giftbox Exchange founder Patrick Falte in Montpelier, Virginia, on 1 October 2016.
- U.S. LEA was able to extract the passwords for Child's Play from Faulkner, which were then passed on to Taskforce ARGOS and allowed them to take over control over the CSAM site.

HESSEN

The „ELYSIUM“-investigation

- At the beginning of 2017, the Australian police took over the account of the moderator of the website The Giftbox Exchange on the Darknet and came across a German who was already planning another CSAM site called “Elysium”.
- The Cybercrime Prosecution Centre of the State of Hesse (ZIT), a specialized unit of the General Public Prosecutor's Office in Frankfurt am Main took over the investigation.
- In June 2017, the site Elysium was shut down by the authorities. So far, 14 suspects and 29 victims have been identified and images have been found that pointed to perpetrators in Germany.

Hessisches Ministerium der Justiz

HESSEN

The „ELYSIUM“-investigation

- After locating the server of the Elysium platform, German law enforcement commenced electronic surveillance of the server and defendant one as well as undercover operations.
- The surveillance measures included uploading avatar images to confirm the server location as well as surveillance of messages sent.
- This helped identify defendants one and two.
- Additionally, in 2016 the German Bundeskriminalamt was sent abuse images of defendant three from which the image of a fingertip and, hence, the fingerprint of the abuser could be deduced thereby identifying defendant three.
-
- By locating an in-memoriam site for the at-that-point-already-arrested defendant one, defendant four could be identified.

HESSEN

The „ELYSIUM“-investigation

- **The well-documented case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group.**
- **The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium.**

HESSEN

The „ELYSIUM“-investigation

SHERLOC SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

UNODC United Nations Office on Drugs and Crime

Sprache auswählen
Powered by Google Google Übersetzer
English

Case Law Database

Cybercrime

Computer-related specific acts

- Production/distribution/ possession of child pornography

Keywords

- Child online abuse
- Electronic Evidence

BGH, Beschluss vom 15.01.2020, 2 StR 321/19

Germany

Fact Summary

This case involved the dissemination of child sexual abuse material via darknet forums by an organized criminal group as well as the sexual abuse of children by the members of the group. The defendants in this case had been part of the online pedophile scene before they got together with several other separately prosecuted offenders to create private forums and chat rooms, including the Giftbox Exchange and Elysium. After registering on these forums, the defendants undertook an increasing number of tasks necessary for the operations of the sites and were promoted to leadership positions, if they did

HESSEN

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

Section 184b (5) of the German Penal Code (StGB) was supplemented by p. 2:

„Paragraph 1, numbers 1 and 4, shall not apply to official acts within the scope of criminal investigation proceedings if the act relates to child pornographic content that does not reflect an actual event and was also not produced using a picture recording of a child or juvenile, and the clarification of the facts would otherwise be futile or substantially impeded“

Hessisches Ministerium der Justiz

HESSEN

New German legislation: police is now allowed to distribute fictual (computer generated) CSAM for the purpose of arresting perpetrators

The offence exception is flanked by Section 110d of the German Code of Criminal Procedure (StPO), which provides that operations require

- **A court order (in case of imminent danger, the consent of the public prosecutor's office is sufficient, but that the measure must be terminated unless there is a court order is given within three working days);**
- **It must be stated in the application by the PPO that the acting police officers have been comprehensively prepared for the operation; and**
- **The court order must be given in writing and be limited in time.**

Online Fraud

Online Fraud

- **COVID-19 has a significant impact on the European fraud landscape even after the pandemic.**
- **Phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication.**
- **Investment fraud is thriving as citizens incur devastating losses, but business email compromise (BEC) and CEO fraud also remain key threats.**

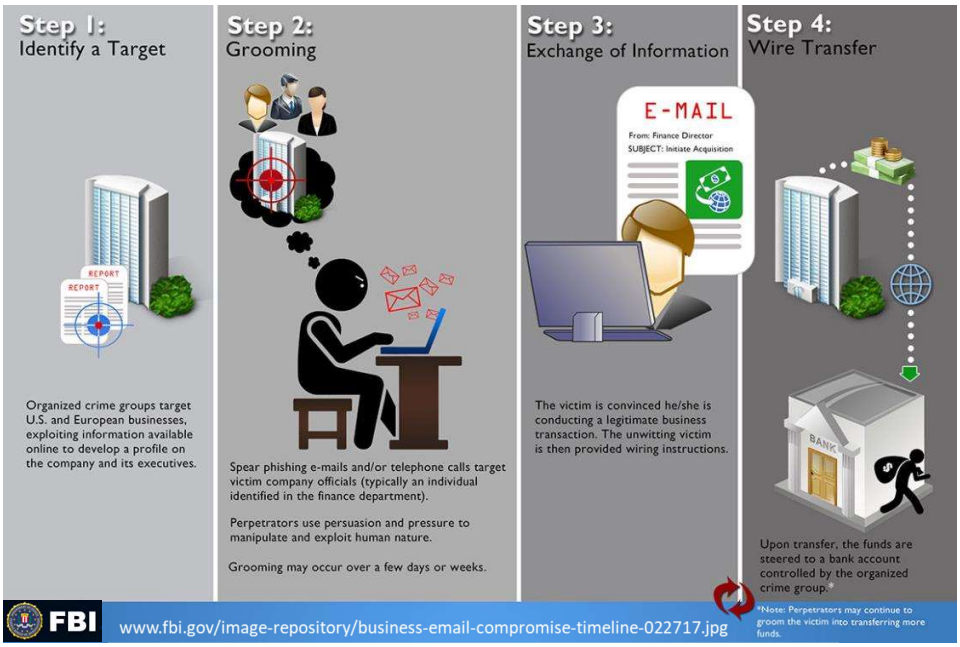
HESSEN

Business Email Compromise (BEC)

- **BEC is defined as a fraud targeting businesses that regularly perform wire transfer payments.**

- **The scam is carried out when perpetrators compromise e-mail accounts through social engineering or through computer intrusion techniques to fraudulently direct electronic fund transfers.**

HESSEN



HESSEN

Social engineering attacks – CEO fraud

- **A refined variant of spear phishing, CEO fraud, has evolved into a key threat as a growing number of businesses are targeted by organised groups of professional fraudsters.**
- **CEO fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential tax information.**
- **Successful CEO frauds often result in significant losses for the targeted companies.**

HESSEN

CEO-fraud: Example

From: Michael [redacted]com]
Sent: Tuesday, March 22, 2016 2:30 PM
To: [redacted]
Cc: [redacted]
Subject: Payment [redacted] to [redacted]

Hi [redacted]

Please send $1.0M from the USD cash pool account to [redacted] at the instructions below. Please send first thing tomorrow morning (Wednesday) . This will go as a loan decrease with [redacted] UK. ase note we will use only Deutsche Bank for USD transactions as of now and have the details saved for ire payments.

Bank Name: Deutsche Bank Europe S.A.

USD:

Account Name: [redacted]

IBAN : PL0[redacted]

BIC/SWIFT [redacted]

Please reply to confirm the payment will be completed by tomorrow morning.

Thank you,

Michael

CEO-fraud: Example

Von: Michael [redacted]
Gesendet: Montag, 28. März 2016 17:36
An: [redacted]
Cc: [redacted]

Betreff: RE: Payment [redacted] to [redacted]

Hi [redacted]

I hope you had a great weekend. Unfortunately we had a miscalculation and it seems the total amount intended for [redacted] UK is 3.0M USD. Please send another $2.0M from the USD cash pool account to [redacted] using same instructions as last week. Please send this first thing tomorrow morning (Tuesday) . This will also go as a loan decrease with [redacted] UK and this way we can complete this cycle before end of march if everything goes smoothly.

Please email me back to confirm you can complete this in time.

Thanks

Michael

CEO-fraud: Example

R: L 200204 I

Weiterleiten ...

Mo 17.02.2020 10:14

image002.jpg
19 KB

Dear Mrs. [redacted]
Happy New Week.

As per previous advise please kindly update us on your payment schedule against the return payment of the total amount of € 1,915,400.00 (1,570,000.00 + 22% VAT).
In addition prior internal governmental taxation issues in our banking, please note that we now receive all International payments with Our Subsidiary Malaysia Branch and we need to keep them updated accordingly as per payment date, because we expect to receive this payment with our Offshore Malaysia Bank information to facilitate financial aids for our New offices therein.
Again, please accept our apologies for any inconvenience this might have caused you: rest assured we'll do our utmost to avoid repeating mistakes, thank you.

Awaiting your kind reply, we remain
With our Best Regards
S. M [redacted]

Da: [redacted]
Inviato: [redacted]
A: [redacted]
Cc: [redacted]
Oggetto: [redacted]
Dear [redacted]
thank you very much for your information.
Actually, the payment of the second invoice, originally scheduled at the end of January 2021, was our mistake: sorry for that!
As your colleagues well know, we have a strong constraint on the cash flow related to this project: that's why we unfortunately cannot agree with your proposal.

Thank you for your attention!

Questions? Remarks?

Handling electronic evidence in courts

Senior Public Prosecutor Chatrine Rudström

Co-funded by the Justice Programme of the European Union 2014-2020

ÅKLAGARMYNDIGHETEN

1

Agenda

- About me
- EJCN
- Prosecution in cyberspace
  - Challenges
  - Typical questions regarding admissibility
  - Presenting electronic evidence in court

ÅKLAGARMYNDIGHETEN

2

2

About me

- Senior public prosecutor
- Cybercrime since 2000
- International and organised crime

ÅKLAGARMYNDIGHETEN

3

3

European Judicial Cybercrime Network

- Network of representatives of Member States´ judicial authorities specialised in dealing with cybercrime, cyber-enabled crime and investigations in cyberspace

EUROPEAN JUDICIAL CYBERCRIME NETWORK

ÅKLAGARMYNDIGHETEN

4

4

European Judicial Cybercrime Network

- Eurojust, network of practitioners
- Established 2016
- Plenary meetings, topical discussions
- Subgroups
- Training

ÅKLAGARMYNDIGHETEN

5

5

Challenges

- Data retention
- Encryption
- Cross-border nature
- Jurisdiction
- Virtual currencies
- New technology, old laws
- Education
- New role for the prosecutor

ÅKLAGARMYNDIGHETEN

6

6

ÅKLAGARMYNDIGHETEN

7

European Union

- 27 countries – 24 languages
- Different legal systems: common, civil
- Mutual recognition
- European Investigation Order
- Mutual Legal Assistance
- JIT – European Council Framework Decision on joint investigation teams

ÅKLAGARMYNDIGHETEN

8

Jurisdiction

- Not just Cybercrime -> Cyber-enabled crime
- Jurisdiction issues
  - Where is a crime committed?
  - Who is the competent authority to investigate?
- Loss of location

9

9

The Supreme Court of Norway - Order - HR-2019-610-A

- "A search in a case like this would also not entail any violation of other states' exclusive enforcement jurisdiction. In this regard, it was emphasised that the coercive measure had been commenced on Norwegian soil, and that the relevant data had been made available by a coercive measure against a Norwegian company with offices in Norway."

10

10

The Supreme Court of Sweden – Ö 5686-22, March 30 2023

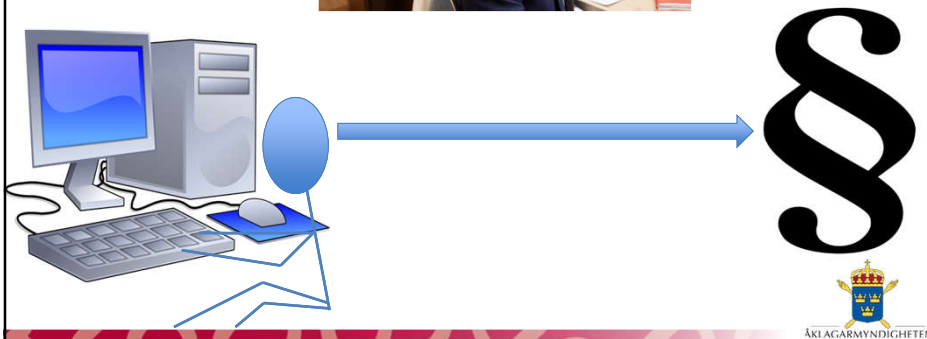
- The provisions of the Code of Judicial Procedure on remote searches are designed to allow retrieval of information that is stored outside Sweden. There are no international legal obstacles to such search. It is irrelevant if it is known in which country where the information is stored or if the location of the storage is unknown. What has been said applies under the condition that the measure is taken within the framework of a Swedish criminal investigation and thus is prompted by a suspicion of crime, which falls within Swedish judicial jurisdiction; with Swedish criminal investigation may in this context be equated to a case for legal assistance a competent foreign authority. It must also be assumed that the action is taken with the use of equipment that is available in Sweden and that it takes place in one in such a way that the information sought is not deleted or otherwise affected to its content.

ÅKLAGARMYNDIGHETEN

11

11

Prosecutor as a "link"



ÅKLAGARMYNDIGHETEN

12

12

Prosecutor as a “link”

Special demands on the “link”

- Knowledge

- Objectivity

- Presentation

Admissibility of e-evidence at court

- No rules on international level
- Different rules in different countries
- But: typical questions, e.g. related to
  - **Data categories** (and authorization of investigative measures by the competent authority)
  - **Character of an investigative measure** (and its existence under procedural law)
  - **Cross-border gathering** of e-evidence

Data categories

- Communication
  - Subscriber information
  - Traffic data
  - Location
  - Content
- Stored information
  - Content
  - Meta data

15

Character of the investigative measure

- Coercive measures
- Secret coercive measures
- Voluntary disclosure
  - Anyone
  - According to US law

16

Cross-border gathering

- Different legal systems
- Different laws
- Different competent authorities
  - Police
  - Prosecutor
  - Judge

17

Presenting digital evidence in court

- What is ”evidence”?
  - Identification
  - What
  - Where
  - How
- What is electronic evidence?
- Supporting evidence

18

18

Contact information

Chatrine Rudström
Senior Public Prosecutor

chatrine.rudstrom@aklagare.se
+46 10 562 54 41
+46 70 346 35 57

ÅKLAGARMYNDIGHETEN

19

19

Digital Evidence in Court

John Berry
Barrister

THE BAR OF IRELAND
The Law Library

Co-funded by the Justice
Programme of the European Union 2014-2020

1

Background

- Mechanical Engineering (1998)
- MSc Technology Management (2003)
- Barrister at Law (2007)

- PwC – Management Consulting
- Oracle
- Xerox
- Pfizer

- Principally practice in criminal law as both prosecution and defence counsel

2

3

Principles

- Privacy – "right to be let alone"
- Not absolute – Article 8(2)
- Presumption of unreliability – *People (DPP) v. Kelly* [2008] 3 I.R. 697

4

The Digital Space

People(DPP) v. Quirke, [2023] IESC 5

"…entry into the digital space involves the automatic loss of privacy rights on a vast scale. Without judicial scrutiny [of] seizure for the purpose of a non-physical search into mobile phones and other computer devices of vast memory and carrying the private dimensions of a human life over years or months[,] no balancing of rights can be undertaken whereby a court may authorise such a search and seizure."

5

Warrant search

Hussein v. Commissioner An Garda Síochána [2016] IEHC 612

CRH v. CCPC [2018] 1 I.R. 521

Nexans v. Commission (Case T-135/09)

People(DPP) v. Quirke [2023] IESC 5

6

Warrant search

Hussein v. Commissioner An Garda Síochána [2016] IEHC 612

- Barrister investigated for fraud offences
- Claimed legal privilege
- Framework proposed

7

Warrant search

CRH v. CCPC [2018] 1 I.R. 521

- Anti competitive practices investigated
- Seized computer and email server
- Obtained an injunction preventing search of server
- Article 8 breach found

8

Warrant search

Nexans v. Commission (Case T-135/09)

- Inspection into anti-competitive practices
- Questions of scope raised
- *…if the Commission were not subject to that restriction, it would in practice be able, every time it has indicia suggesting that an undertaking has infringed the competition rules in a specific field of its activities, to carry out an inspection covering all those activities, with the ultimate aim of detecting any infringement of those rules which might have been committed by that undertaking.*

9

10

Warrant search

People(DPP) v. Quirke [2023] IESC 5

- Warrant sought to search farm, not computers
- Judge who issued warrant not informed of intention to seize computers and search them
- *"For centuries, our polity has required the intervention not only of a positive legal power specifically conferred by statute but also the objective evaluation by the judicial arm of government to ensure that a balanced use of such powers conforms with the fundamental requirement of reasonable suspicion and that police powers be only used for the purposes for which they are granted"*

11

Warrantless search of physical devices?

R. v. Fearon, [2014] SCC 77 (Canada)

Our digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas. Our digital devices are windows to our inner private lives.

…our law must also evolve so that modern mobile devices do not become the telescreens of George Orwell's 1984.

12

Warrantless search of physical devices?

R. v. Fearon, [2014] SCC 77 (Canada)

- Lawful arrest
- Incidental to arrest – protection & preserving
- Nature and extent of search tailored – recent materials of obvious
- Detailed record of examination – after the fact judicial review

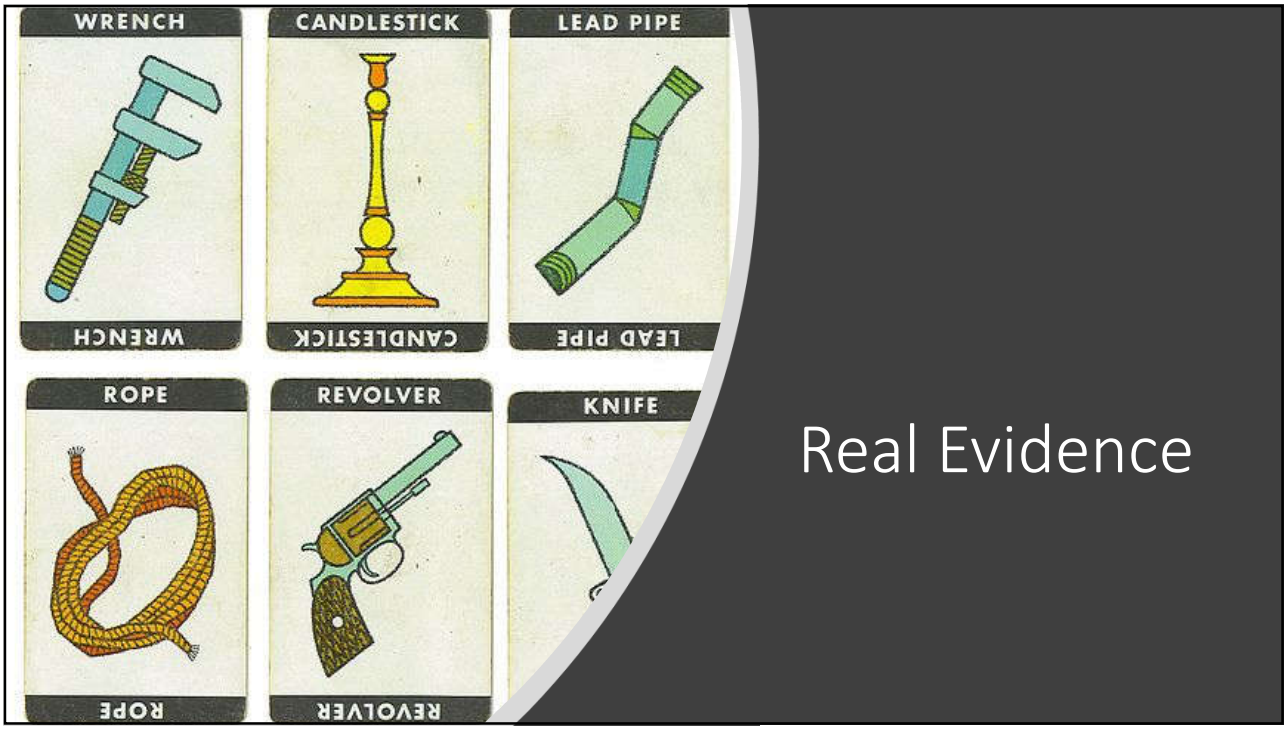
13

14

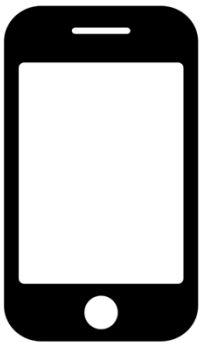
Classification of Evidence

- Real evidence
- Documentary evidence
- Automatically generated evidence
- Hearsay?

15



16




17

Admissibility of data

People(DPP) v. AMcD [2016] 3 I.R. 123

…the evidence should prove the provenance and authenticity of the footage; the recording must be intelligible and of sufficient quality, and must also be relevant and have probative value. In addition, the party seeking to adduce such evidence must be able to account for its history from the moment of its recording until its production in court, this to exclude the possibility that it may have been interfered with

18

Automatically generated evidence

R v. Cochrane (1993) Crim. L.R. 48

…it was necessary that appropriate authoritative evidence should be called to describe the function and operation of the mainframe computer

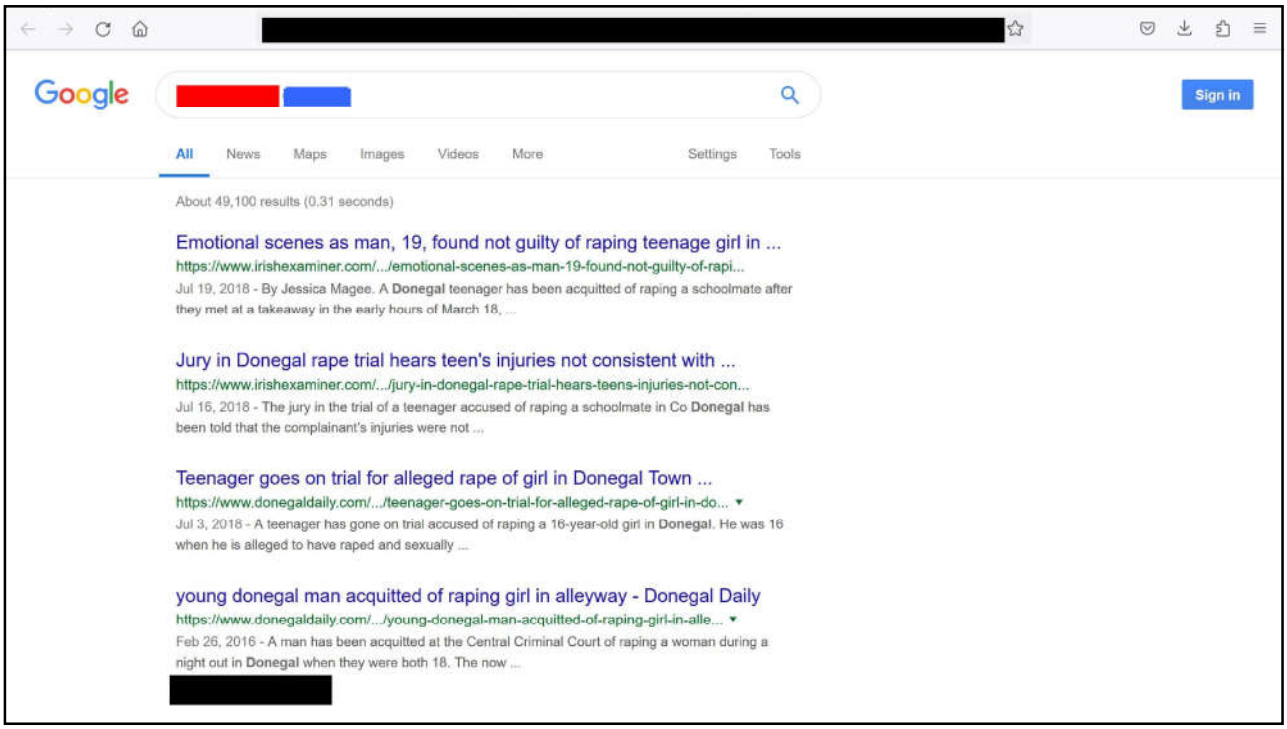
…what [the trial judge] required was authoritative evidence about the operation of the relevant machines rather than legal authority.

19

Data Analysis Tools

- Is there a requirement to prove operation?
- Expert evidence or pseudo-science?
- *DPP v. Power* [2018] IECA 119
- ACPO Good Practice Guide for Digital Evidence (2012)
- International Standards (ISO 17025)

20



21

Civil Law Case

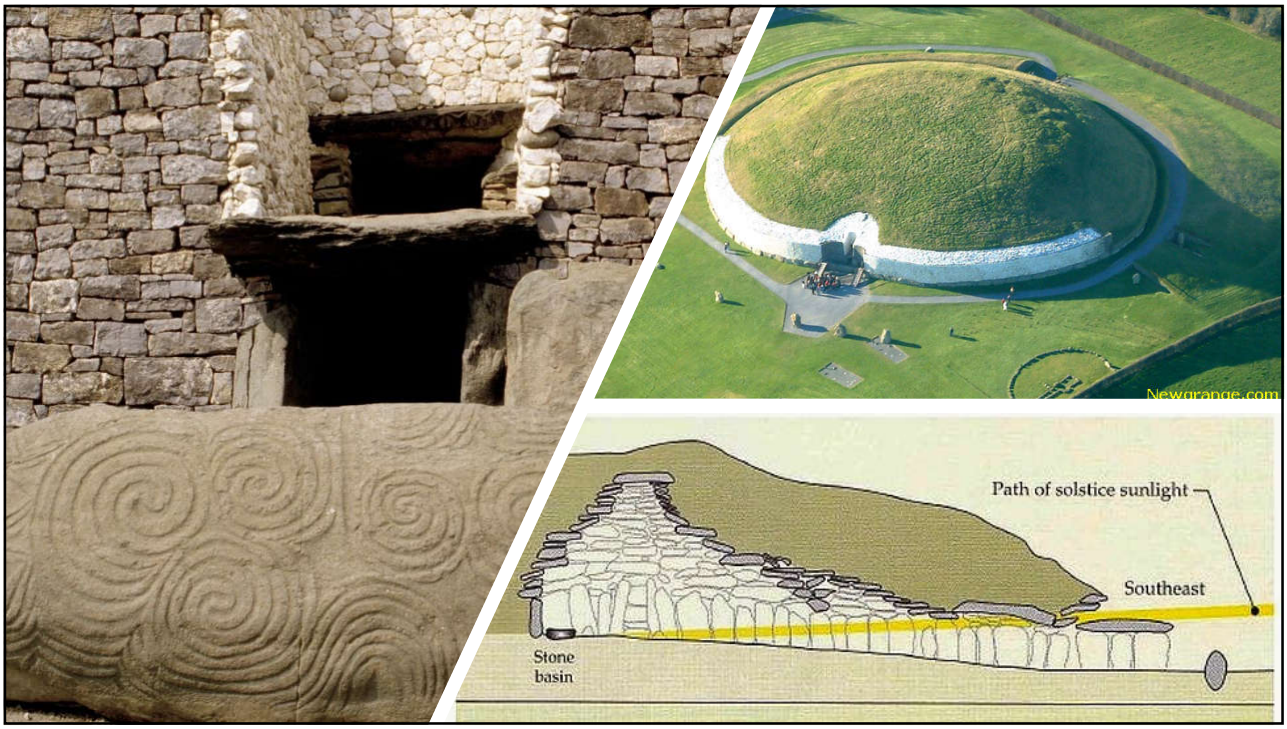
- Rape accused entitled to anonymity
- Google searches showing anonymised newspaper reports
- Proceedings brought to prevent searches returning certain results
- Preservation/presentation of evidence

22

Challenging digital evidence

- Procedure based
- Hash values
- Mutual legal assistance requests
- Unallocated clusters -*DPP v. O'Connor* [2020] IECA 14, *US v. Flyer* 633 F.3d 911 (9th Cir. 2011)
- Attribution -*US v. Reynolds* 626 F. App'x 610, 612-13 (6th Cir. 2015)
- Proving communication

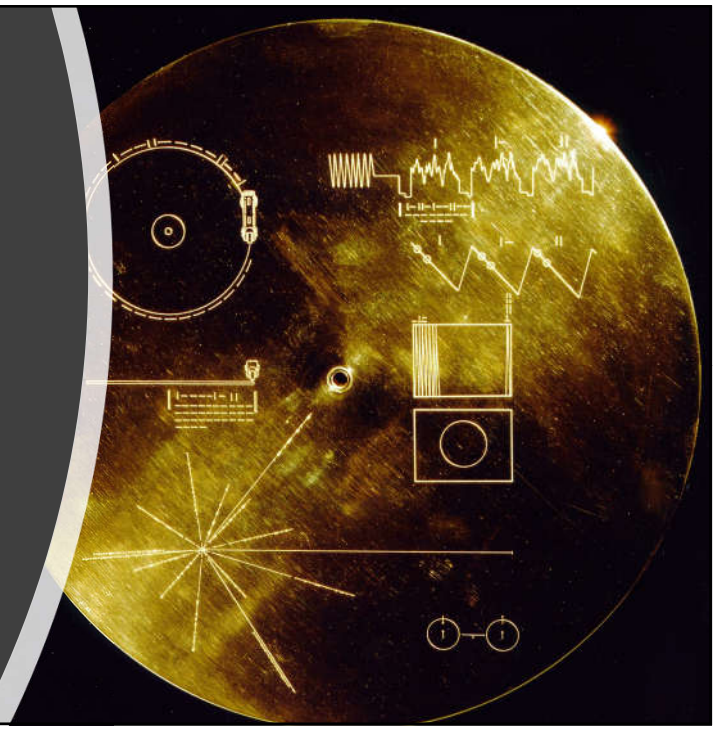
23



24

Good practice

- Limited bandwidth
- Relevance
- Digital display, not paper
- Core Booklet
- Narrative assistance



25