POST-COVID CHALLENGES IN CRIMINAL JUSTICE

THE RISE OF EVIDENCE ON MOBILE DEVICES

Barcelona, 22-23 February 2024

FACE-TO-FACE

EXCELLENCE IN EUROPEAN LAW

Speakers

Patricia Ayodeji, Dual-Qualified Solicitor for England & Wales, Lawyer (Abogado) for Spain, Barcelona

María Barbancho, Criminal Lawyer, Member of the Committee of International Relations, ICAB, Barcelona

Steven David Brown, International Cybercrime Consultant, Vienna

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

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

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

Michael Rothärmel, Head of Unit, Fight against Terrorism and Extremism, Ministry of Justice, Munich

Chatrine Rudström, Senior Public Prosecutor, Prosecutor's Office, Stockholm; Member of the European Judicial Cybercrime Network (EJCN), The Hague

Rosa Peña, Deputy at the International Relations Commission, ICAB, Barcelona

Andreu Van den Eynde, Lawyer in Criminal Law, ICAB, Barcelona

Key topics

- Technical issues (internet caches, proxy servers, encryption, deep/dark web, etc.)
- Legal implications of e-evidence (collection, evaluation and admissibility)
- The rise of evidence on mobile devices
- Insights into different national criminal justice systems

Language
English

Event number
324DT06

Organisers
ERA (Laviero Buono) in cooperation with the Barcelona Bar Association (ICAB)

Co-funded by the European Union

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

Thursday, 22 February 2024

09:00 Arrival and registration of participants

09:30 **Welcome and introduction to the programme**
Rosa Peña & Laviero Buono

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

09:45 **Internet or Internot?**
- The different dimensions and manifestations of the Internet (LAN, WAN, WWW, Cloud, Deep & Dark)
- Understanding Internet Protocols
- Threats and opportunities in obtaining Internet evidence
- How users mask their locations
- Logs, browser fingerprints and data breadcrumbs

Steven David Brown

10:45 Discussion

11:00 Break

Chair: Laviero Buono

11:30 **Open-source tools, computer forensics on mobile devices and in the "Cloud"**
- Encryption and privacy
- Encrypted apps on mobile (smart)phones
- Physical and logical acquisition of data
- Cloud providers and replicated data on websites

Damir Kahvedžić

12:30 Discussion

12:45 Lunch

PART II: LEGAL ISSUES RELATED TO THE RISE OF EVIDENCE ON MOBILE DEVICES

Chair: Damir Kahvedžić

13:45 **Mobile phones: swipe right for evidence**
- Challenges posed by the type and volume of evidence found on a smartphone
- Comparing and contrasting cell site analysis with GPS systems for locating a phone
- Geofence warrants
- IMSI (International Mobile Subscriber Identity) catchers: their use and concerns about their deployment

Steven David Brown

14:30 Discussion

Chair: Steven David Brown

14:45 **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

15:15 Discussion

15:30 Break

Objective

Mobile devices such as smartphones and tablets contain personal information such as call history, text messages, e-mails, digital photographs, videos, calendar items, address books, passwords and credit card numbers. They can be useful as sources of digital evidence to be examined when criminal activities occur.

This seminar aims to share advanced knowledge and to exchange experience and best practice between judges, prosecutors and lawyers in private practice who deal with criminal proceedings involving e-evidence on mobile devices.

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 EU Member States.

Venue

ICAB Training Centre
C/Mallorca 283
08037 Barcelona
Spain

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.

16:00 **Prosecuting hate speech and other criminal online content: proactive cooperation by service providers**
- New obligations for service providers to submit e-evidence under Union law, incl. the Digital Services Act
- Additional national rules
- Codes of conduct

Michael Rothärmel

16:45 Discussion

17:00 End of first day

19:30 Dinner offered by the organisers

Friday, 23 February 2024

PART III: INVESTIGATING WEB 2.0 – BEST PRACTICES

Chair: Joachim Meese

09:30 **Social media and electronic evidence: some concrete cases**
Patricia Ayodeji

10:00 Discussion

10:15 **Handling electronic evidence on mobile devices in courts: perspectives of the defence**
- The importance of the chain of custody in handling the evidence
- Trial considerations: methods of presentation and admissibility tests

María Barbancho

11:00 Discussion

11:15 Break

Chair: María Barbancho

11:45 **Dealing with e-evidence in cross-border cases: best practices and possible new scenarios in light of the new EU legislation**
Joachim Meese

12:15 Discussion

12:30 **Handling electronic evidence on mobile devices in court: experiences in Spain**
Andreu Van den Eynde

13:00 Discussion

13:15 End of seminar and lunch

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

Your contact persons

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

Julia Reitz
Assistant
Tel.: +49(0)651 9 37 37 323
E-Mail: jreitz@era.int

Save the date

Annual Conference on EU Criminal Justice 2023
Lisbon, 9-10 November 2023

Countering Environmental Crime in the EU
Trier & Online, 30 Nov-1 Dec 2023

Criminal Law and Human Rights: Recent ECtHR Case Law
Online, 7-8 December 2023

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

Barcelona, 22-23 February 2024 / Event number: 324DT06/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 **8 December 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 Spain: 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.
7. For those travelling within Spain, the contribution for travel is fixed at €52 (for a distance between 50km and 399 km). 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
8. Accommodation costs: international participants and national participants travelling more than 50km one-way will receive a fixed contribution of €117 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
9. These rules do not apply to representatives of EU Institutions and Agencies who are required to cover their own travel and accommodation.
10. 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

11. Participation at the whole seminar is required and participants' presence will be recorded.
12. 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.
13. 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.
14. 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/?132493&en

Venue

ICAB Training Centre,
C/Mallorca 283,
08037 Barcelona, Spain

Language

English

Contact Person

Julia Reitz
Assistant
Tel.: +49(0)651 9 37 37 323
E-Mail: jreitz@era.int

TABLE OF CONTENTS

Co-funded by 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.

BACKGROUND DOCUMENTATION

*** *All documents are hyperlinked* ***

Work carried out by the European Union on e-evidence

1	Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (ST/6438/2022/INIT, OJ L 63, 28.2.2023)	
2	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings *(PE/4/2023/REV/1, OJ L 191, 28.7.2023, p. 118–180)*	
3	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (PE/3/2023/REV/1, OJ L 191, 28.7.2023, p. 181–190)	

Other EU criminal justice documents

A) The institutional framework for criminal justice in the EU

A1) Main treaties and conventions

A1-01	Protocol (No 36) on Transitional Provisions
A1-02	Statewatch Analysis, "The Third Pillar acquis" after the Treaty of Lisbon enters into force, Professor Steve Peers, University of Essex, Second Version, 1 December 2009
A1-03	Consolidated version of the Treaty on the functioning of the European Union, art. 82-86 *(OJ C 326/47; 26.10.2012)*

A1-04	Consolidated Version of the Treaty on the European Union, art. 9-20 *(OJ C326/13;, 26.10.2012)*
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	Court of Justice of the European Union: Presentation of the Court
A2-02	European Parliament Fact Sheets on the European Union: Competences of the Court of Justice of the European Union, April 2023
A2-03	Regulation (EU, Euratom) 2019/629 of the European Parliament and of the Council of 17 April 2019 amending Protocol No 3 on the Statute of the Court of Justice of the European Union, OJ L 111, 17 April 2019
A2-04	Consolidated Version of the Statute of the Court of Justice of the European Union (01 August 2016)
A2-05	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 Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, Council of Europe
A3-02	Guide on the case-law of the European Convention on Human Rights: European Union law in the Court's case-law, Council of Europe, updated on 31 August 2022
A3-03	Case of Grzeda v. Poland (Application no. 43572/18), Strasbourg, 15 March 2022
A3-04	Case of Mihalache v. Romania [GC] (Application no. 54012/10), Strasbourg, 08 July 2019
A3-05	Case of Altay v. Turkey (no. 2) (Application no. 11236/09), Strasbourg, 09 April 2019
A3-06	Case Beuze v. Belgium (Application no. 71409/10), Strasbourg, 09 November 2018
A3-07	Case of Vizgirda v. Slovenia (Application no. 59868/08), Strasbourg, 28 August 2018
A3-08	Case of Şahin Alpay v. Turkey (Application no. 16538/17), Strasbourg, 20 March 2018
A3-09	Grand Chamber Hearing, Beuze v. Belgium [GC] (Application no. 71409/10), Strasbourg, 20 December 2017
A3-10	Case of Blokhin v. Russia (Application no. 47152/06), Judgment European Court of Human Rights, Strasbourg, 23 March 2016
A3-11	Case of A.T. v. Luxembourg (Application no. 30460/13), Judgment European Court of Human Rights, Strasbourg, 09 April 2015

A3-12	Case of Blaj v. Romania (Application no. 36259/04), Judgment European Court of Human Rights, Strasbourg, 08 April 2014
A3-13	Case of Boz v. Turkey (Application no. 7906/05), Judgment European Court of Human Rights, Strasbourg, 01 October 2013 (FR)
A3-14	Case of Pishchalnikov v. Russia (Application no. 7025/04), Judgment European Court of Human Rights, Strasbourg, 24 October 2009
A3-15	Case of Salduz v. Turkey (Application no. 36391/02), Judgment, European Court of Human Rights, Strasbourg, 27 November 2008

A4) Brexit

A4-01	Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part *(OJ L 149, 30.4.2021)*
A4-02	Eurojust: Judicial cooperation in criminal matters between the European Union and the United Kingdom from 1 January 2021, 1 January 2021
A4-03	Draft text of the Agreement on the New Partnership between the European Union and the United Kingdom (UKTF 2020-14), 18 March 2020
A4-04	Draft Working Text for an Agreement on Law enforcement and Judicial Cooperation in Criminal Matters
A4-05	The Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (2019/742), 28th March 2019
A4-06	Brexit next steps: The European Arrest Warrant, House of Commons, 20 February 2020
A4-07	Brexit next steps: The Court of Justice of the EU and the UK, House of Commons, 7 February 2020
A4-08	The Law Society, "Brexit no deal: Criminal Justice Cooperation", London, September 2019
A4-09	European Commission, Factsheet, „A „No-deal"-Brexit: Police and judicial cooperation", April 2019
A4-10	CEPS: Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership, 29 August 2018
A4-11	Policy paper: The future relationship between the United Kingdom and the European Union, 12 July 2018
A4-12	House of Lords, Library Briefing, Proposed UK-EU Security Treaty, London, 23 May 2018
A4-13	HM Government, Technical Note: Security, Law Enforcement and Criminal Justice, May 2018
A4-14	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
A4-15	House of Commons, Home Affairs Committee, UK-EU Security Cooperation after Brexit, Fourth Report of Session 2017-19, London, 21 March 2018
A4-16	HM Government, Security, Law Enforcement and Criminal Justice, A future partnership paper
A4-17	European Criminal Law after Brexit, Queen Mary University London, Valsamis Mitsilegas, 2017
A4-18	House of Lords, European Union Committee, Brexit: Judicial oversight of the European Arrest Warrant, 6th Report of Session 2017-19, London, 27 July 2017
A4-19	House of Commons, Brexit: implications for policing and criminal justice cooperation (24 February 2017)

A4-20	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	Proposal for a Regulation of the European Parliament and of the Council on the transfer of proceedings in criminal matters, COM/2023/185 final, 5 April 2023
B2-02	European Parliament resolution of 20 January 2021 on the implementation of the European Arrest Warrant and the surrender procedures between Member States (2019/2207(INI)), *(OJ C 456, 10.11.2021)*
B2-03	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)*
B2-04	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)*
B2-05	Case law by the Court of Justice of the European Union on the European Arrest Warrant – Overview, Eurojust, 15 March 2020
B2-06	Case C-142/22, OE, Judgment of the Court (Second Chamber), 6 July 2023

B2-07	Case C-699/21, E.D.L, Judgment of the Court (Grand Chamber), 18 April 2023
B2-08	Joined Cases C-514/21 and C-515/21, LU and PH, Judgment of the Court (Fourth Chamber), 23 March 2023
B2-09	Case C-158/21, Puig Gordi and Others, Judgment of the Court (Grand Chamber), 31 January 2023
B2-10	Case C-168/21, Procureur général près la cour d'appel d'Angers, Judgment of the Court (Third Chamber), 14 July 2022
B2-11	Joined Cases C-562/21 PPU and C-563/21 PPU, Openbaar Ministerie (Tribunal établi par la loi dans l'État membre d'émission), Judgment of the Court (Grand Chamber), 22 February 2022
B2-12	Case C-649/19, Spetsializirana prokuratura (Déclaration des droits), Judgement of the Court (Fifth Chamber), 28 January 2021
B2-13	Case C-414/20 PPU, MM, Judgment of the Court (Third Chamber), 13 January 2021
B2-14	Joined Cases C-354/20 PPU and C-412/20 PPU, Openbaar Ministerie (Indépendance de l'autorité judiciaire d'émission), Judgement of the Court (Grand Chamber), 17 December 2020
B2-15	Case C-416/20 PPU, Generalstaatsanwaltschaft Hamburg, Judgement of the Court (Fourth Chamber), 17 December 2020
B2-16	Case C-584/19, A and Others, Judgement of the Court (Grand Chamber), 8 December 2020
B2-17	Case C-510/19, AZ, Judgement of the Court (Grand Chamber), 24 November 2020
B2-18	Case C-717/18, X (European arrest warrant – Double criminality) Judgement of the Court of 3 March 2020
B2-19	Case C-314/18, SF Judgement of the Court of 1 March 2020
B2-20	Joined Cases C-566/19 PPU (JR) and C-626/19 PPU (YC), Opinion of AG Campos Sánchez-Bordona, 26 November 2019
B2-21	Case C-489/19 PPU (NJ), Judgement of the Court (Second Chamber) of 09 October 2019
B2-22	Case 509/18 (PF), Judgement of the Court (Grand Chamber), 27 May 2019
B2-23	Joined Cases C-508/18 (OG) and C-82/19 PPU (PI), Judgement of the Court (Grand Chamber), 24 May 2019
B2-24	The Guardian Press Release: Dutch court blocks extradition of man to 'inhumane' UK prisons, 10 May 2019
B2-25	Case 551/18, IK, Judgement of the Court of 06 December 2018 (First Chamber)
B2-26	CJEU Press Release No 141/18, Judgement in Case C-207/16, Ministerio Fiscal, 2 October 2018
B2-27	CJEU Press Release No 135/18, Judgement in Case C-327/18 PPU RO, 19 September 2019
B2-28	Case C-268/17, AY, Judgement of the Court of 25 July 2018 (Fifth Chamber)
B2-29	Case C-220/18 PPU, ML, Judgement of the Court of 25 July 2018 (First Chamber)
B2-30	Case C-216/18 PPU, LM, Judgement of the Court of 25 July 2018 (Grand Chamber)
B2-31	InAbsentiEAW, Background Report on the European Arrest Warrant - The Republic of Poland, Magdalena Jacyna, 01 July 2018
B2-32	Case C-571/17 PPU, Samet Ardic, Judgment of the court of 22 December 2017
B2-33	C-270/17 PPU, Tupikas, Judgment of the Court of 10 August 2017 (Fifth Chamber)

B2-34	Case C-271/17 PPU, Zdziaszek, Judgment of the Court of 10 August 2017 (Fifth Chamber)
B2-35	Case C-579/15, Popławski, Judgement of the Court (Fifth Chamber), 29 June 2017
B2-36	Case C-640/15, Vilkas, Judgement of the Court (Third Chamber), 25 January 2017
B2-37	Case C-477/16 PPU, Kovalkovas, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-38	Case C-452/16 PPU, Poltorak, Judgement of the Court (Fourth chamber), 10 November 2016
B2-39	Case C-453/16 PPU, Özçelik, Judgement of the Court (Fourth Chamber), 10 November 2016
B2-40	Case C-294/16 PPU, JZ v Śródmieście, Judgement of the Court (Fourth Chamber), 28 July 2016
B2-41	Case C241/15 Bob-Dogi, Judgment of the Court (Second Chamber) of 1 June 2016
B2-42	C-108/16 PPU Paweł Dworzecki, Judgment of the Court (Fourth Chamber) of 24 May 2016
B2-43	Cases C-404/15 Pál Aranyosi and C-659/15 PPU Robert Căldăraru, Judgment of 5 April 2016
B2-44	Case C-237/15 PPU Lanigan, Judgment of 16 July 2015 (Grand Chamber)
B2-45	Case C-168/13 PPU *Jeremy F / Premier ministre*, Judgement of the court (Second Chamber), 30 May 2013
B2-46	Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, Judgment of of 26 February 2013
B2-47	Case C-396/11 Ciprian Vasile Radu, Judgment of 29 January 2013
B2-48	C-261/09 Mantello, Judgement of 16 November 2010
B2-49	C-123/08 Wolzenburg, Judgement of 6 October 2009
B2-50	C-388/08 Leymann and Pustovarov, Judgement of 1 December 2008
B2-51	C-296/08 Goicoechea, Judgement of 12 August 2008
B2-52	C-66/08 Szymon Kozlowski, Judgement of 17 July 2008

B3) Mutual recognition: freezing and confiscation and asset recovery

B3-01	European Judicial Network (for information on mutual recognition of freezing and confiscation orders, including on competent authorities), 14 December 2020, last reviewed on 24 July 2023
B3-02	Moneyval 64th Plenary Meeting report, Strasbourg, 5 January 2023
B3-03	Proposal for a Directive of the European Parliament and of the Council on asset recovery and confiscation *(Brussels, 25.5.2022, COM (2022) 245 final)*
B3-04	Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010, *(Brussels, 20.7.2021 COM(2021) 421 final)*
B3-05	FATF, COVID-19-related Money Laundering and Terrorist Financing Risk and Policy Responses, Paris, 4 May 2020
B3-06	Money-Laundering and COVID-19: Profit and Loss, Vienna, 14 April 2020
B3-07	FATF President Statement – COVID-19 and measures to combat illicit financing, Paris 1 April 2020
B3-08	Moneyval Plenary Meeting report, Strasbourg, 31 January 2020

B3-09	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
B3-10	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
B3-11	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
B3-12	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
B3-13	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
B3-14	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
B3-15	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)
B3-16	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)
B3-17	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)
B3-18	Consolidated text: Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union
B3-19	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
B3-20	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)
B3-21	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	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-02	Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, *(OJ L 191, 28.7.2023)*
B5-03	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *(Brussels, 20.7.2021, COM(2021) 409 final)*
B5-04	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
B5-05	Joint Note of Eurojust and the European Judicial Network on the Practical Application of the European Investigation Order, June 2019
B5-06	European Commission, Press Release, „Security Union: Commission recommends negotiating international rules for obtaining electronic evidence", Brussels, 05 February 2019
B5-07	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
B5-08	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
B5-09	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
B5-10	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
B5-11	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)
B5-12	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
B5-13	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

B5-14	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)*
B5-15	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace *(7 December 2016)*
B5-16	ENISA 2014 - Electronic evidence - a basic guide for First Responders (Good practice material for CERT first responders)
B5-17	Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130/1; 1.5.2014)
B5-18	Guidelines on Digital Forensic Procedures for OLAF Staff" (Ref. Ares(2013)3769761 - 19/12/2013, 1 January 2014
B5-19	ACPO Good Practice Guide for Digital Evidence *(March 2012)*
B5-20	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*)
B5-21	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*)
B5-22	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)*
B5-23	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	Report from the Commission to the European Parliament and the Council concerning the exchange through the European Criminal Records Information System (ECRIS) of information extracted from criminal records between the Member States. *(COM/2017/0341 final, 29.06.2017)*
B6-06	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)*
B6-07	Council Decision on the exchange of information extracted from criminal records – Manual of Procedure *(6397/5/06 REV 5; 15.1.2007)*
B6-08	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 Case-law by the Court of Justice of the European Union on the Principle of ne bis in idem in Criminal Matters, Eurojust, December 2021
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	Report from the Commission to the European Parliament and the Council on the implementation of 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, COM/2023/44 final, 1 February 2023
C-02	Commission Recommendation (EU) 2023/681 of 8 December 2022 on procedural rights of suspects and accused persons subject to pre-trial detention and on material detention conditions, *(OJ L 86, 24.3.2023)*
C-03	FRA Report, Presumption of innocence and related rights – Professional perspectives, Luxembourg, 31 March 2021
C-04	FRA Report, Rights in practice: Access to a lawyer and procedural rights in criminal and European Arrest Warrant proceedings, Luxembourg, 27 September 2019
C-05	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2013/48/EU of the European Parliament and of the Council 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 person informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, COM/2019/560 final, 26 September 2019
C-06	Report from the Commission to the European Parliament and the Council on the implementation of 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, COM/2018/857 final, 18 December 2018
C-07	Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, COM/2018/858 final, 18 December 2018
C-08	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-09	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-10	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-11	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-12	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-13	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-14	C-209/22 - Rayonna prokuratura Lovech, TO Lukovit (Fouille corporelle), 7 September 2023
C-15	C-660/21 - K.B. and F.S. (Relevé d'office dans le domaine pénal), 22 June 2023
C-16	C-430/22, C-468/22 - VB (Information du condamné par défaut), 8 June 2023
C-17	C-608/21 - Politseyski organ pri 02 RU SDVR, 25 May 2023
C-18	C-694/20 - Orde van Vlaamse Balies i in., 8 December 2022
C-19	C-348/21 - HYA and Others (Impossibilité d'interroger les témoins à charge), 8 December 2022
C-20	C-347/21 - DD (Réitération de l'audition d'un témoin), 15 September 2022
C-21	C-242/22 PPU - TL () and de traduction), 1 August 2022
C-22	C-564/19 - IS (Illégalité de l'ordonnance de renvoi), 23 November 2021
C-23	C-282/20 - ZX (Régularisation de l'acte d'accusation), 21 October 2021
C-24	C-649/19 - Spetsializirana prokuratura (Déclaration des droits), 28 January 2021
C-25	Case C-659/18, Judgement of the Court of 2 March 2020
C-26	Case C-688/18, Judgement of the Court of 3 February 2020
C-27	Case C467/18, Rayonna prokuratura Lom, Judgment of the Court of 19 September 2019
C-28	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-29	Case C377/18, AH a. o., Judgment of the Court of 05 September 2019

C-30	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-31	Case C-8/19 PPU, criminal proceedings against RH (presumption of innocence), Decision of the Court (First Chamber), 12. February 2019
C-32	Case C646/17, Gianluca Moro, Opinion of the AG Bobek, 05 February 2019
C-33	Case C-551/18 PPU, IK, Judgment of the Court (First Chamber), 6 December 2018
C-34	Case C-327/18 PPU, RO, Judgment of 19 September 2018 (First Chamber)
C-35	Case C-268/17, AY, Judgment of the Court (Fifth Chamber), 25 July 2018
C-36	Case C-216/18 PPU, LM, Judgment of 25 July 2018 (Grand Chamber)
C-37	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-38	Case C-439/16 PPU, Emil Milev (presumption of innocence), Judgment of the Court (Fourth Chamber), 27 October 2016
C-39	Case C-278/16 Frank Sleutjes ("essential document" under Article 3 of Directive 2010/64), Judgment of 12 October 2017 (Fifth Chamber)
C-40	C-25/15, István Balogh, Judgment of 9 June 2016 (Fifth Chamber)
C-41	Opinion of Advocate General Sharpston, delivered on 10 March 2016, Case C543/14
C-42	C-216/14 Covaci, Judgment of 15 October 2015 (First Chamber)

D) Approximating criminal law and Victims´ Rights

D1) Terrorism

D1-01	EU Centre of Expertise for Victims of Terrorism
D1-02	EU's Counter-Terrorism Coordinator
D1-03	Eurojust Meeting on Counter-Terrorism, 16-17 November 2022, Summary of Discussions, 05 April 2023
D1-04	Eurojust Casework on Counter-Terrorism: Insights 2020 – 2021, December 2021
D1-05	Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), *(OJ L 172, 17.5.2021)*
D1-06	European Commission, EU Handbook on Victims of Terrorism, January 2021
D1-07	2019 Eurojust Report on Counter- Terrorism, 09 December 2020
D1-08	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: A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 9 December 2020, COM(2020) 795 final
D1-09	Report from the Commission to the European Parliament and the Council based on Article 29(1) of 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, COM(2020) 619 final, Brussels, 30 September 2020
D1-10	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 on the EU Security Union Strategy, 24 July 2020, *(COM (2020) 605 final)*
D1-11	Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism, Brussels, 16 June 2020
D1-12	Terrorism Situation and Trend Report (TE-SAT) 2019
D1-13	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
D1-14	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
D1-15	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
D1-16	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)
D1-17	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
D1-18	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)*
D1-19	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), *(OJ L 156, 19.6.2018)*
D1-20	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)
D1-21	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)
D1-22	Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP, *(OJ L 255, 21.9.2016)*

D1-23	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)
D1-24	Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, *(OJ L 344, 28.12.2001)*

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

D2-01	European Parliament Briefing: Preventing and combating trafficking in human beings, June 2023
D2-02	European Parliament Briefing: Anti-trafficking in human beings, June 2023
D2-03	European Parliament resolution of 15 September 2022 on human rights violations in the context of the forced deportation of Ukrainian civilians to and the forced adoption of Ukrainian children in Russia (2022/2825(RSP)), *(OJ C 125, 5.4.2023)*
D2-04	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(COM/2022/732 final, 19 December 2022)*
D2-05	Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions report on the progress made in the fight against trafficking in human beings (Fourth Report), *(COM/2022/736 final, 19 December 2022)*
D2-06	Commission Staff Working Document Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(SWD/2022/425 final, 19 December 2022)*
D2-07	European Parliament resolution of 5 May 2022 on the impact of the war against Ukraine on women (2022/2633(RSP)), *(OJ C 465, 6.12.2022)*
D2-08	European Parliament At Glance: Russia's war on Ukraine: The risk of trafficking of human beings, May 2022
D2-09	Commission Staff Working Document Evaluation 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, SWD/2022/0179 final, 2022)*
D2-10	European Migrant Smuggling Centre 6th Annual Report – 2022
D2-11	Europol: The challenges of countering human trafficking in the digital era, As of 6 December 2021
D2-12	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the application of Directive 2009/52/EC of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals, *(COM/2021/592 final, 29 September 2021)*
D2-13	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025, *(COM/2021/171 final, 14 April 2021)*

D2-14	Eurojust Report on Trafficking in Human Beings, Best practice and issues in judicial cooperation, February 2021
D2-15	Report from the European Commission to the European Parliament and the Council, Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, *(COM(2020) 661 final, Brussels, 20 October 2020)*
D2-16	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum, *(COM (2020) 609 final, 23 September 2020)*
D2-17	European Commission, Study on Data collection on Trafficking in Human Beings in the EU, September 2020
D2-18	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
D2-19	European Migrant Smuggling Centre - EMSC
D2-20	European Migrant Smuggling Centre – 4th Annual Activity Report, The Hague, 15 May 2020
D2-21	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
D2-22	European Institute for Gender Equality (EIGE) report: Gender-specific measures in anti-trafficking actions, 17 October 2018
D2-23	UNODC – Global Study on Smuggling of Migrants 2018, Vienna/New York, June 2018
D2-24	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
D2-25	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 Assessment (IOCTA) 2023
D3-02	European Parliament Legislative Train Schedule: Horizontal cybersecurity requirements for products with digital elements in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-03	European Parliament Legislative Train Schedule: Review of the Directive on security of network and information systems in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-04	European Parliament Legislative Train Schedule: Digital operational resilience for the financial sector in “A Europe Fit for the Digital Age”, As of 20 September 2023
D3-05	European Parliament Briefing: EU cyber-resilience act, May 2023
D3-06	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-07	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector

	and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-08	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), *(OJ L 333, 27.12.2022)*
D3-09	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, *(COM/2022/454 final, 15 September 2022)*
D3-10	Internet Organised Crime Threat Assessment (IOCTA) 2021
D3-11	Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (Text with EEA relevance), *(OJ L 274, 30.7.2021)*
D3-12	European Commission, Public consultation on Fighting child sexual abuse: detection, removal and reporting of illegal content online, 11 February 2021
D3-13	European Judicial Cybercrime Network 9th Plenary Meeting - 2nd Outcome report 2020, 27 January 2021
D3-14	European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, Final report, September 2020
D3-15	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU strategy for a more effective fight against child sexual abuse, *(COM (2020) 607 final, Brussels, 24 July 2020)*
D3-16	Internet Organised Crime Threat Assessment (IOCTA) 2020
D3-17	Internet Organised Crime Threat Assement (IOCTA) 2019
D3-18	Special Eurobarometer 480, Report, “Europeans´ Attitudes towards Internet Security”, Brussels, March 2019
D3-19	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)
D3-20	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*)
D3-21	Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems *(OJ L 69/67; 16.3.2005*)
D3-22	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*)
D3-23	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)
D3-24	Convention on Cybercrime (Budapest, 23.XI.2001)

D4) Protecting Victims´ Rights

D4-01	Proposal for a Directive of the European Parliament and of the Council amending Directive 2012/29/EU establishing minimum standards on the rights, support, and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA *(COM/2023/424 final, 12 July 2023)*

D4-02	Commission Staff Working Document: Evaluation 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 *(SWD/2022/0179 final, 28 June 2022)*
D4-03	FRA Report: "Underpinning victims' rights: support services, reporting and protection", 22 February 2023
D4-04	Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence *(COM/2022/105 final, 8 March 2022)*
D4-05	D4-01 Victim Support Europe, Paper: Victim Support and Data Protection, 1st March 2021
D4-06	European Union Agency for Fundamental Rights (FRA), Report: Crime, safety, and victims' rights – Fundamental Rights Survey, 19 February 2021
D4-07	European Commission, EU Strategy on victims' rights (2020-2025), COM (2020) 258 final, Brussels, 24 June 2020
D4-08	Factsheet – EU Strategy on Victims' Rights (2020-2025), 24 June 2020
D4-09	Report from the Commission to the European Parliament and the Council on the 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 *(COM/2020/188 final, 11 May 2020)*
D4-10	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
D4-11	European Commission Factsheet: The Victims' Rights Directive: What does it bring?, February 2017
D4-12	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
D4-13	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
D4-14	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
D4-15	Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order
D4-16	Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims
D4-17	Website of the European Union Agency for Fundamental Rights (FRA) – Victims' rights
D4-18	Victim Support Europe
D4-19	European Commission: Victims' Rights Platform
D4-20	EC Coordinator for victims' rights

E) Criminal justice bodies and networks

E1) European Judicial Network

E1-01	European Judicial Network, The Report on activities and management 2019-20
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	Working Arrangement Between The European Anti-fraud Office And the European Union Agency for Criminal Justice Cooperation, 29 March 2023
E2-04	Eurojust Annual Report 2022
E2-05	Eurojust collection of anniversary essays, 20 years of Eurojust: EU judicial cooperation in the making, 8 August 2022
E2-06	Regulation (EU) 2022/838 of the European Parliament and of the Council of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences *(OJ L 148, 31.5.2022)*
E2-07	Guidelines for deciding on competing requests for surrender and extradition, October 2019
E2-08	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 Spotlight Series
E3-02	Europol Joint Reports
E3-03	Europol Consolidated Annual Activity Report (CAAR) 2022, 7 June 2023
E3-04	Europol Strategy: DELIVERING SECURITY IN PARTNERSHIP, 6 June 2023
E3-05	The European Union Agency for Law Enforcement Cooperation in Brief, 17 January 2023
E3-06	Europol Programming Document 2023 – 2025, Europol Public Information The Hague, 20 December 2022
E3-07	Case T-578/22: Action brought on 16 September 2022 — EDPS v Parliament and Council, *(OJ C 424, 7.11.2022)*
E3-08	Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation, *(OJ L 169, 27.6.2022)*
E3-09	Europol Report – Beyond the Pandemic – How COVID-19 will shape the serious and organised crime landscape in the EU, 30 April 2020
E3-10	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	EPPO: Internal Rules of Procedure, 29 June 2022
E4-02	Commission Implementing Regulation (EU) 2022/1504 of 6 April 2022 laying down detailed rules for the application of Council Regulation (EU) No 904/2010 as regards the creation of a central electronic system of payment information (CESOP) to combat VAT fraud, *(OJ L 235, 12.9.2022)*
E4-03	Commission Implementing Decision (EU) 2021/856 of 25 May 2021 determining the date on which the European Public Prosecutor's Office assumes its investigative and prosecutorial tasks, *(OJ L 188, 28.5.2021)*
E4-04	Working Arrangement between Eurojust and EPPO, 2021/00064, February 2021
E4-05	Working Arrangement establishing cooperative relations between the European Public Prosecutor's Office and the European Union Agency for Law Enforcement Cooperation, January 2021
E4-06	Regulation (EU, Euratom) 2020/2223 of the European Parliament and of the Council of 23 December 2020 amending Regulation (EU, Euratom) No 883/2013, as regards cooperation with the European Public Prosecutor's Office and the effectiveness of the European Anti-Fraud Office investigations, *(OJ L 437, 28.12.2020)*
E4-07	Commission Delegated Regulation (EU) 2020/2153 of 14 October 2020 amending Council Regulation (EU) 2017/1939 as regards the categories of operational personal data and the categories of data subjects whose operational personal data may be processed in the index of case files by the European Public Prosecutor's Office, *(OJ L 431, 21.12.2020)*
E4-08	Council Implementing Decision (EU) 2020/1117 of 27 July 2020 appointing the European Prosecutors of the European Public Prosecutor's Office, *(OJ L 244, 29.7.2020)*
E4-09	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*)
E4-10	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
E4-11	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)
E4-12	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
E4-13	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
E4-14	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')

E4-15	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)
E4-16	Csonka P, Juszczak A and Sason E, 'The Establishment of the European Public Prosecutor's Office : The Road from Vision to Reality', Eucrim - The European Criminal Law Associations' Forum, 15 January 2018
E4-17	Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')
E4-18	Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, *(OJ L 198, 28.7.2017)*

F) Data Protection

F-01	European Data Protection Board (EDPB)
F-02	European Data Protection Supervisor (EDPS)
F-03	Proposal for a Regulation of the European Parliament and of the Council amending Council Decision 2009/917/JHA, as regards its alignment with Union rules on the protection of personal data *(COM/2023/244 final, 11.5.2023)*
F-04	Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 amending Directive 2014/41/EU, as regards its alignment with Union rules on the protection of personal data, *(OJ L 39, 21.2.2022)*
F-05	Directive (EU) 2022/211 of the European Parliament and of the Council of 16 February 2022 amending Council Framework Decision 2002/465/JHA, as regards its alignment with Union rules on the protection of personal data, *(OJ L 37, 18.2.2022)*
F-06	European Parliament Legislative Observatory, Police cooperation - joint investigation teams: alignment with EU rules on the protection of personal data, 2021/0008(COD)
F-07	EPPO College Decision 009/2020, Rules concerning the processing of personal data by the European Public Prosecutor's Office, 28 October 2020
F-08	Communication from the Commission to the European Parliament and the Council: Way forward on aligning the former third pillar acquis with data protection rules, *(COM (2020) 262 final, 24 June 2020)*
F-09	Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, *(OJ L 336, 10.12.2016)*
F-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)*
F-11	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	Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, *(OJ L 134, 22 May 2023)*
G1-02	Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, *(OJ L 158, 13 June 2022)*
G1-03	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 *(COM/2021/170 final, 14 April 2022)*
G1-04	Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, *(COM/2021/784 final, 8 December 2021)*
G1-05	European Commission, Press Release, "Police Cooperation Code: Boosting police cooperation across borders for enhanced security", 8 December 2021
G1-06	European Commission, Factsheet, "Reinforcing police cooperation across Europe", 8 December 2021
G1-07	Commission Staff Working Document: Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817, and 2019/818 of the European Parliament and of the Council, *(SWD/2021/378 final, Brussels, 8.12.2021)*
G1-08	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, *(COM(2020) 791 final, Brussels, 9 December 2020)*
G1-09	European Commission, Inception Impact Assessment on EU Police Cooperation Code (PCC), Ref. Ares(2020)5077685, 28 September 2020
G1-10	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 Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union, *(OJ L 185, 12.7.2022)*

G1-11	Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, *(OJ L 210, 6.8.2008)*
G1-12	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)*
G1-13	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)*
G1-14	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)*
G1-15	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	Europol Information on JITs
G2-03	JIT Evaluation Form
G2-04	Council of Europe: Guidelines on the use of Joint Investigation Teams
G2-05	Riehle, C. “20 years of Joint Investigations Teams (JITs) in the EU”: An overview of their development, actors and tools. ERA Forum 24, 163–167, 29 June 2023
G2-06	Checklist for multilateral joint investigation teams, 22 June 2023
G2-07	Latest trends and novelties in JIT operations: first-hand experiences of JIT practitioners and Eurojust | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu) Fourth JITs Evaluation Report, 14 June 2023
G2-08	Regulation (EU) 2023/969 of the European Parliament and of the Council of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726, OJ L 132, 17 May 2023
G2-09	Guidelines on the Network of National Experts on Joint Investigation Teams, 2 December 2020
G2-10	Third JIT Evaluation Report, Eurojust, March 2020
G-11	Joint Investigation Teams: Practical Guide, 16 December 2021
G2-12	Council Resolution on a Model Agreement for Setting up a Joint Investigation Team (JIT) – 2017/C18/01, Strasbourg, 19 January 2017
G2-13	Council Document establishing the JITs Network, 08 July 2005
G2-14	Council Framework Decision of 13 June 2002 on joint investigation teams (*OJ L 162/1; 20.6.2002*)

Steven David Brown

Barcelona

22-23 February 2024

Swipe Right for Evidence

InZeit
Excellence in Acuity

ERA
Academy of European Law

The St(Ph)one Age

Telephone was fixed line (fixed location)

Linked to named subscriber

Itemised billing records (Call Detail Records)

Call trace had to wait for mechanical switching

Public callboxes

InZeit
Excellence in Acuity

The Information Age

Phones are 'mobile'

Not 'just' phones

GPS

Connect to base stations/cell sites/antennae (which then link to a wired network)

Can buy & use phone anonymously

InZeit
Excellence in Acuity

SIM Registration NOT Required March 2020 (Europe)

Bosnia & Herzegovina
Croatia
Czech Republic
Cyprus
Denmark
Estonia
Finland
Iceland
Ireland
Latvia
Liechtenstein
Lithuania
Malta
Moldova
Netherlands
Portugal
Romania
Serbia
Slovenia
UK

InZeit Excellence in Acuity

https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

(about) 160 Countries globally
… not UK

Heathrow 2019

Phones

Identifiers:

Subscriber Account details

SIM (Subscriber Identity Module) Card

IMSI
International Mobile Subscriber Identity
(Linked to SIM)

IMEI
International Mobile Equipment Identity
(Linked to Phone)

(Most phones display the IMEI when you key in ***#06#**)

Phones

Identifiers:

5G networks use a SUPI (Subscription Permanent Identifier) which is compatible with 4G IMSI network.

The SUPI is encrypted into a Subscription Concealed Identifier (SUCI)
SUCI is regenerated for each connection to antenna.

Key in *#06#)

https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/
https://www.5gworldpro.comt/blog/2023/10/25/what-are-the-major-security-threats-to-the-5g-air-interface/

SIM Card

Authorises phone number on a telecoms network.

May contain

- call history
- contacts and
- received texts

SIM can be switched between different phones

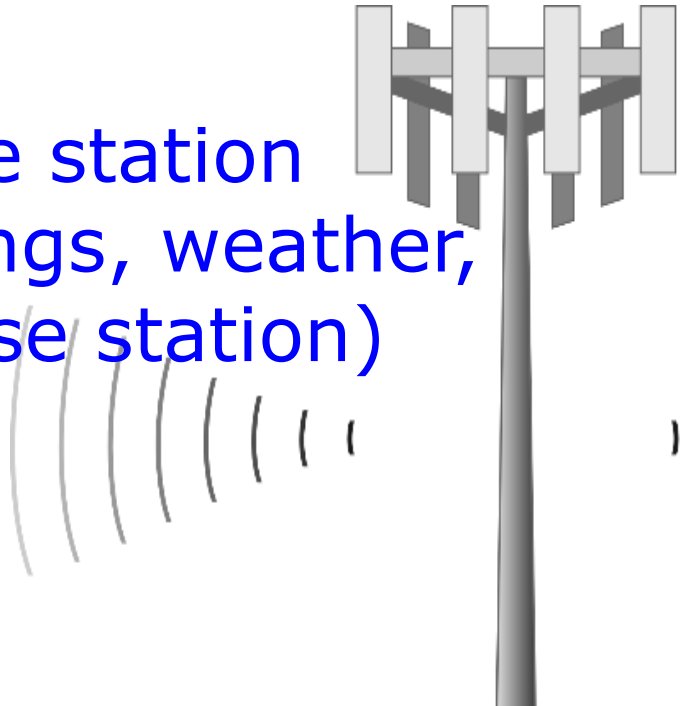
Some modern SIM cards have Secure Element that stores credit card details to allow use as payment device

When phone switched on sends a signal (‘ping’) to the network.

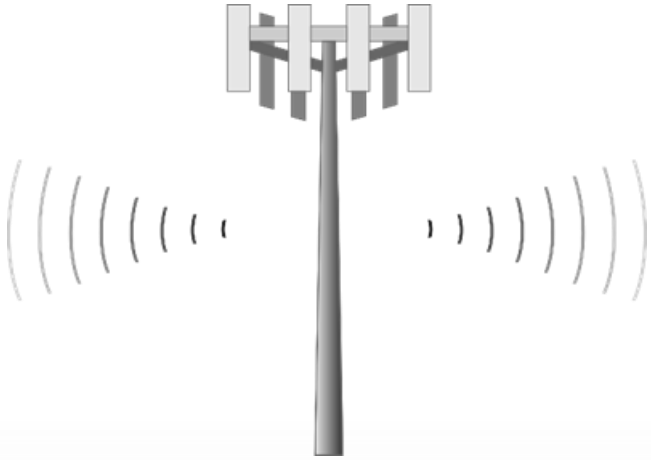
It selects the most powerful base station signal

Registered on system (if phone on standby will ‘ping’ periodically)

Not necessarily the closest base station (affected by topography, buildings, weather, reflected signal, load on the base station)



InZeit
Excellence in Acuity



Urban area: single tower can identify phone location to within an area of about 1km^2

Rural setting may be 10s of km^2

Note: Cell-site sectors are not neat shapes with clearly defined edges (diagrams can be misleading)

Cell-site sectors overlap

4G phones may connect to more than 1 cell-site

During a call, the network will control to which tower the phone is connected.

When crosses cell site boundary the phone is ‘handed off’ to the next tower.

Each ‘dish’ on a cell site antenna has an identifying number.

The antenna number is recorded.

Cell Site Analysis

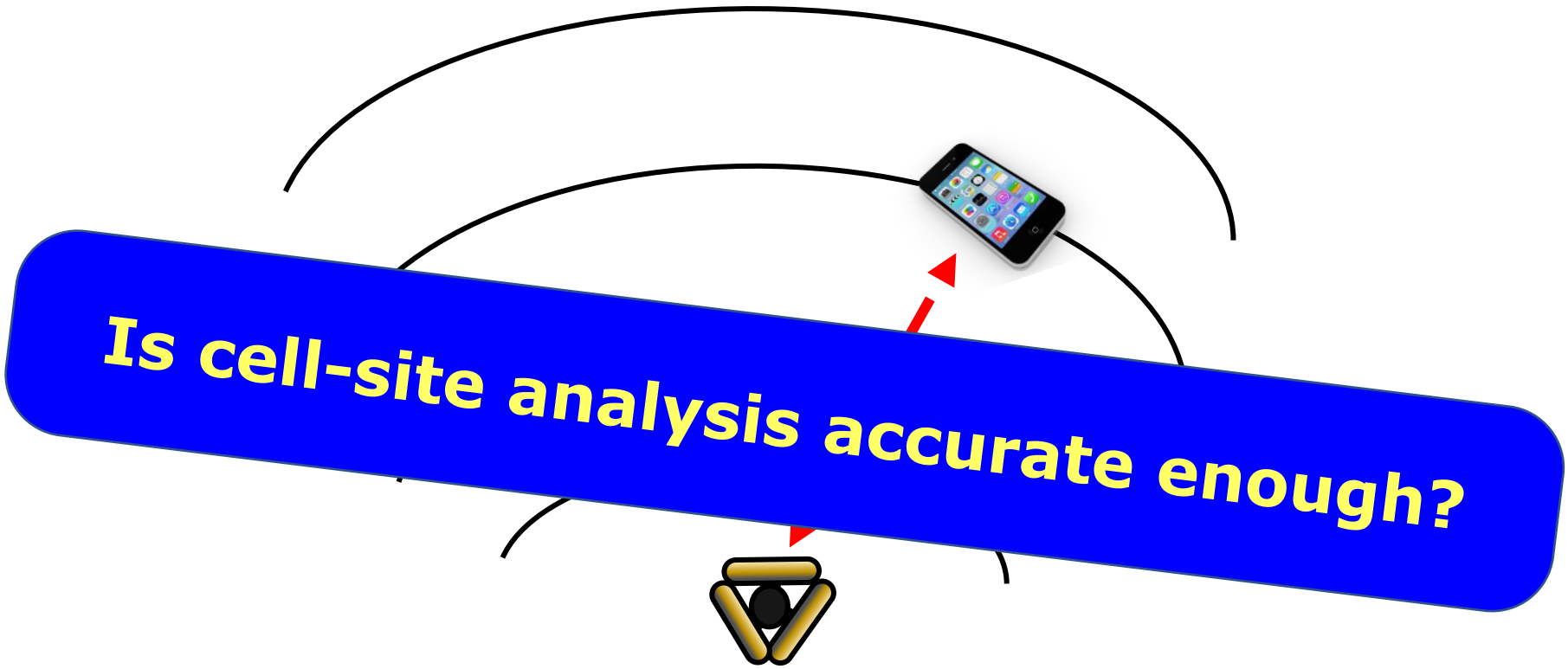
- Historical cell site & call data analysis
  - Which cell tower used
  - Number called
  - Time and duration of call
  - IMEI (physical number on phone)
  - IMSI (identifying the user account)
- Transaction records for billing
- Can be ‘near’ real time

Cell Site Analysis

- Can’t draw conclusions about coverage just from call details records
- Even site surveys can’t reproduce all variables

(Site survey is when you go to a location and physically measure cell tower signals)

Time difference of arrival (TDOA)



Is cell-site analysis accurate enough?

Possible to <u>estimate</u> phone distance from antenna from time signal takes (pinging)

InZeit
Excellence in Acuity

Oregon Offender Search

Public Information (Last Updated: 04/15/2014 18:48:35)

SID# 14776586

Offender Name: Roberts, Lisa Marie

Age: 48 DOB: 06/1965
Gender: Female Race: Black - African American
Height: 5' 04" Hair: Black
Weight: 170 lbs Eyes: Brown

Caseload: 15704 Sanjines, Cecilia

Location: Coffee Creek Correctional Facility

Status: Inmate

Institution Admission Date 12/02/2004
Earliest Release Date: 09/03/2016

Offenses | Names

Docket Number	County	Crime	Sentence Type	Begin Date	Termination Date
020834931/01	MULT	MANSLAUGHTER I	Inmate Sentence	12/02/2004	-

In 2004 Lisa Roberts pleaded guilty to manslaughter on a plea bargain on advice of her (court appointed) defence attorney

Prosecutor had told the defence attorney that phone records put Roberts at the scene and it was *'almost as accurate as DNA'.*

InZeit Excellence in Acuity

https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?utm_term=.e1ea86444ad2

Oregon Offender Search

Public Information (Last Updated: 04/15/2014 18:48:35)

SID# 14776586

Offender Name: Roberts, Lisa Marie

Age: 48 **DOB:** 06/1965
Gender: Female **Race:** Black - African American
Height: 5' 04" **Hair:** Black
Weight: 170 lbs **Eyes:** Brown

Caseload: 15704 Sanjines, Cecilia

Location: Coffee Creek Correctional Facility

Status: Inmate

Institution Admission Date 12/02/2004
Earliest Release Date: 09/03/2016

Offenses | Names

Docket Number	County	Crime	Sentence Type	Begin Date	Termination Date
020834931/01	MULT	MANSLAUGHTER I	Inmate Sentence	12/02/2004	-

2014 (9 ½ years imprisonment) Lisa Marie Roberts released. Cell-site analysis was found to be inaccurate.

InZeit Excellence in Acuity

https://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html?utm_term=.e1ea86444ad2

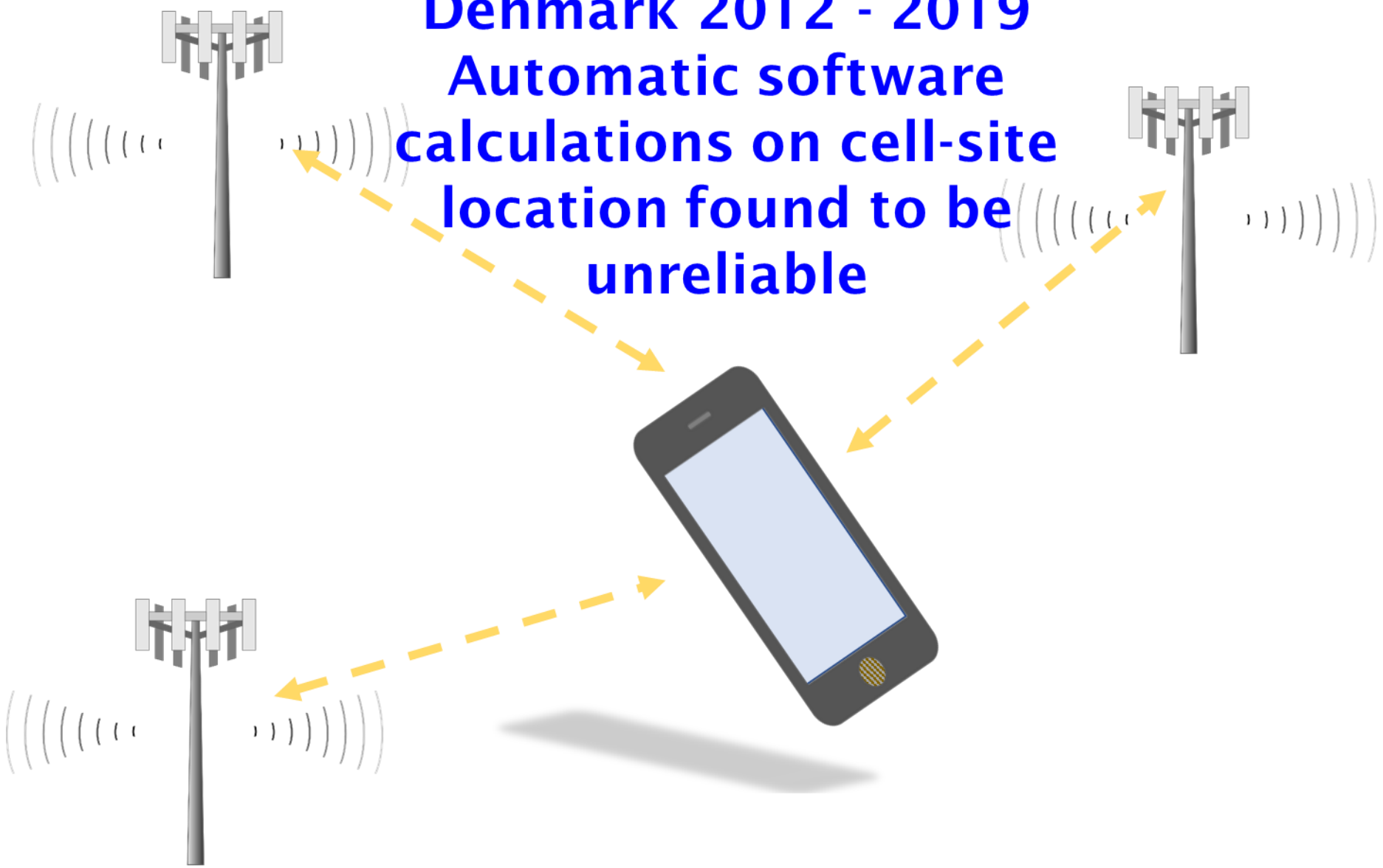
5G operates at higher frequencies, (up to) 10 Gbps download speeds, BUT less penetration, travel less far, affected by weather & humidity.

Small cell stations, denser networks. Still not materialised

3G networks being shutdown, but 2G networks may remain as backup for calls and texts in some countries.

https://www.anscorporate.com/blog/what-is-a-5g-cell-tower

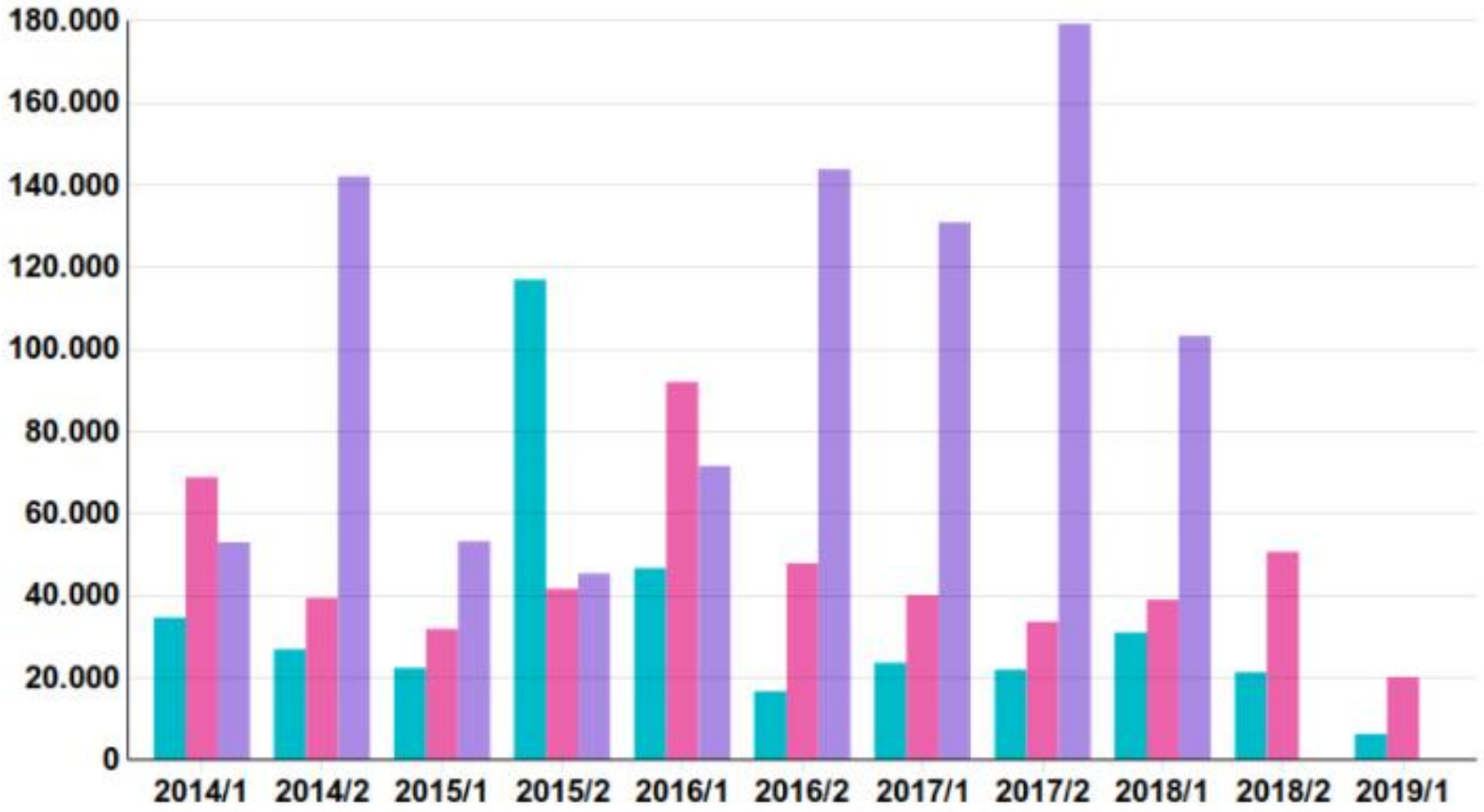
Denmark 2012 - 2019 Automatic software calculations on cell-site location found to be unreliable



InZeit
Excellence in Acuity

Stealth (sms) Ping

Causes phone to register on (nearest) mast



BKA Federal Criminal Police
BPOL Federal Police
BfV Federal Office for the Protection of the Constitution

InZeit
Excellence in Acuity

https://digit.site36.net/2019/08/20/less-stealth-sms-from-german-police-but-more-secrecy-for-domestic-intelligence/

GPS

Global Positioning System (GPS)

Handsets have GPS chip

Network of 30+ satellites 20,000 km orbit. Always 6 'in view'

Requires clear view of min. three (better four) satellites

Structures/reflected signals can cause error

Where no satellite connection, phone may use wifi or phone network

On average, location identifiable to 5-8 metres (can be 3-5 metres – future tech 30cm)

Google's Sensorvault

Google's Sensorvault database contains location data for hundreds of millions of devices all over the world.

Law enforcement officials use 'Geofence warrants' to obtain information from Sensorvault to identify suspects in vicinity of a crime.

Google Location History not enabled by default but users are prompted to enable it.

Initial data is anonymized, but once collated and analysed and potential suspect phones identified, Google provides the names of the owners of those devices.

- Gainsville Florida January 2020
- Keen cyclist
- RunKeeper Android App
- Email from Google
- ‘Will release data to Police unless get a court order preventing it’
- Burglary 97 years old woman’s home (8 months before)
- Passed 3 times in hour

InZeit
Excellence in Acuity

https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

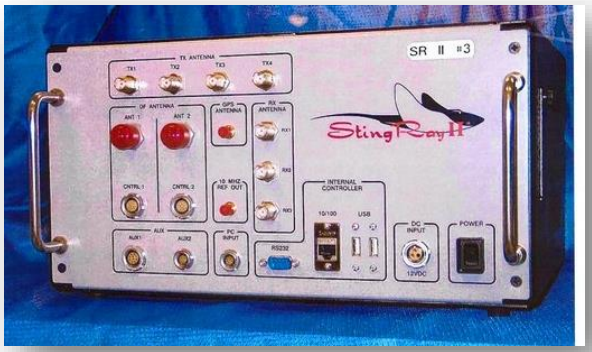
IMSI Catcher
(aka StingRay, Hailstorm, TriggerFish)

Device imitates mobile phone base station

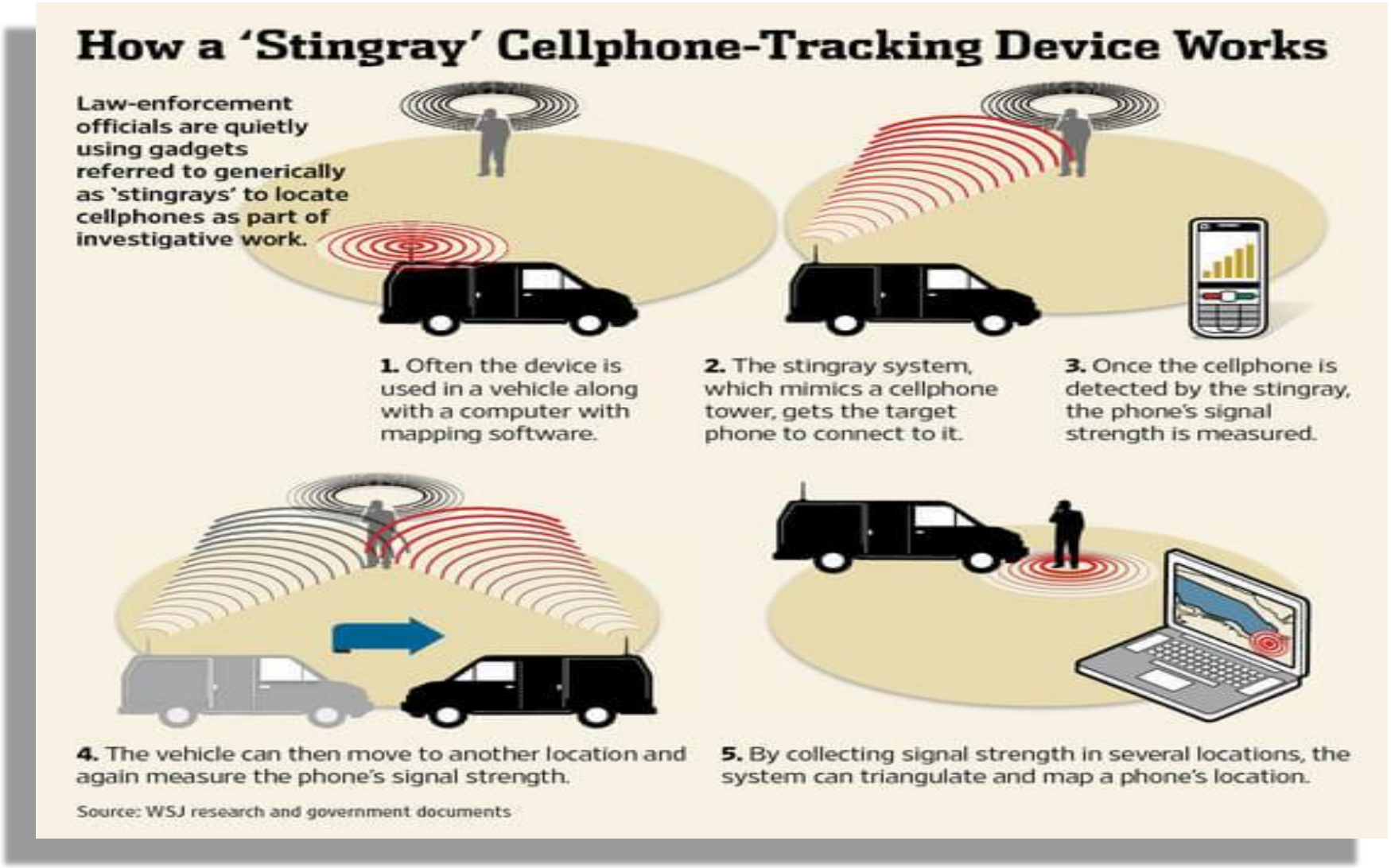
Phone automatically detects & connects to the IMSI catcher

All phone traffic passes through the IMSI catcher

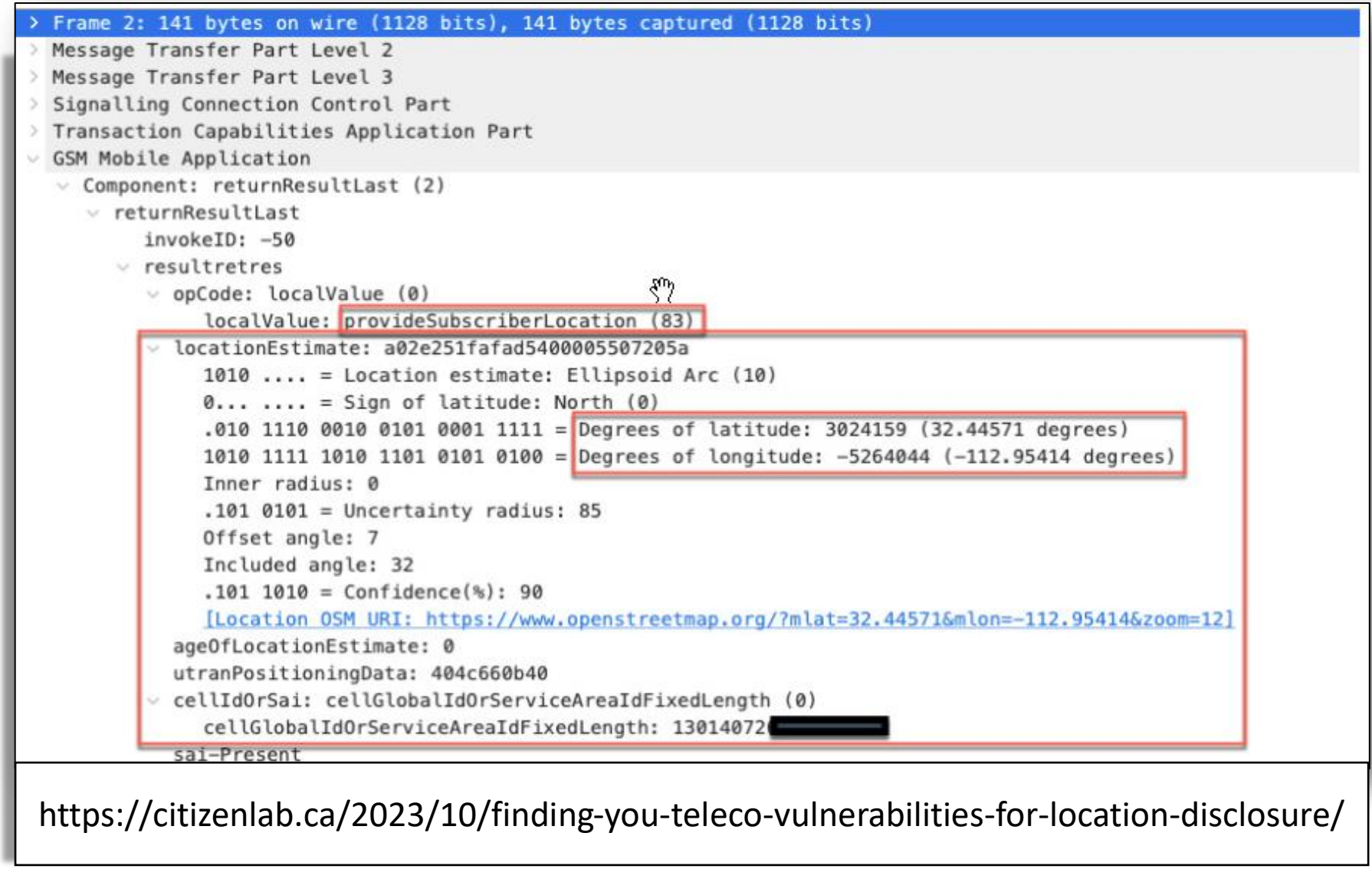
Based on 2G technology, but 3G/4G phones are compatible (3G/4G signal can be disrupted or suppressed)



InZeit
Excellence in Acuity

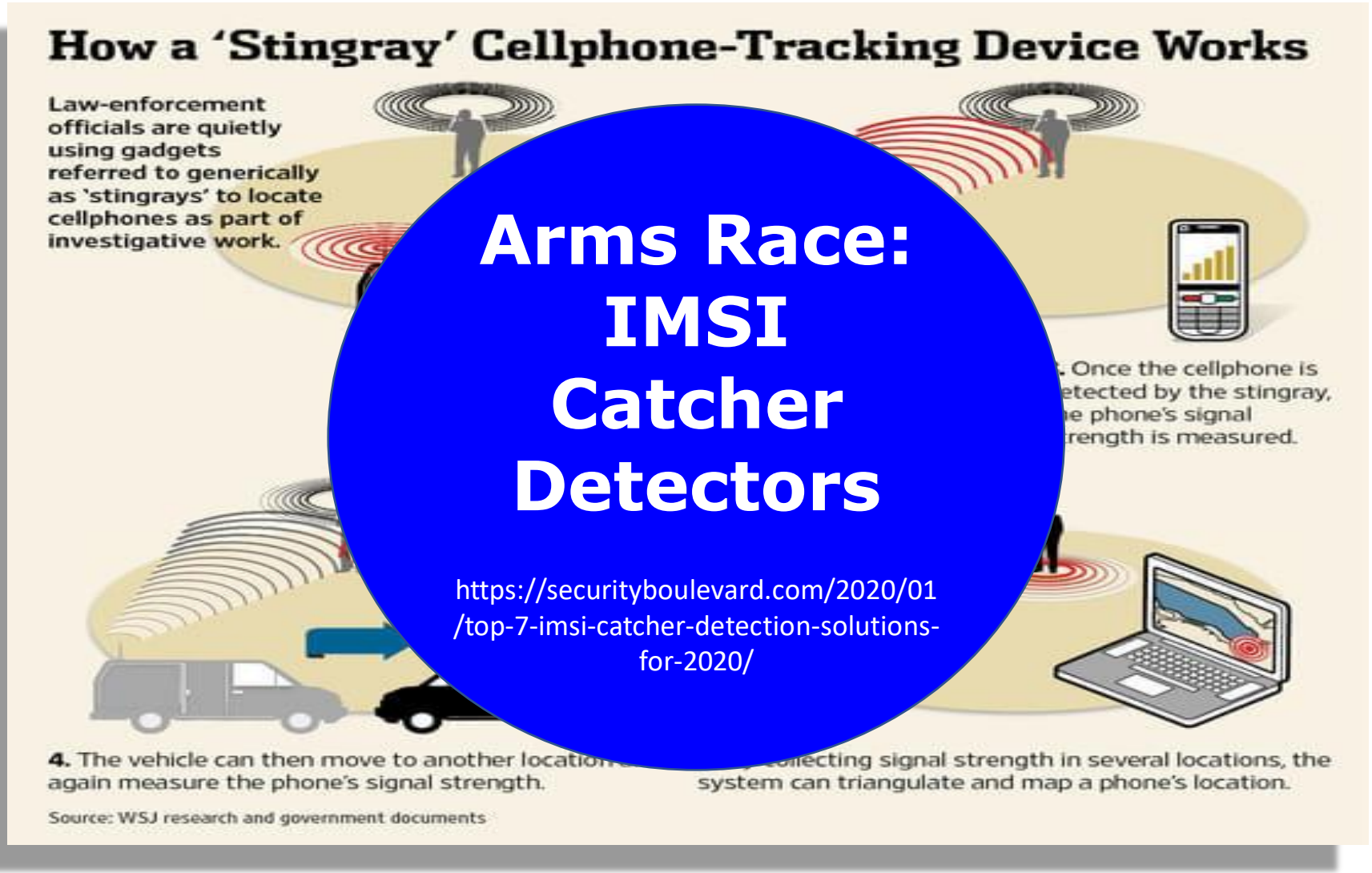


Source: https://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move



https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/

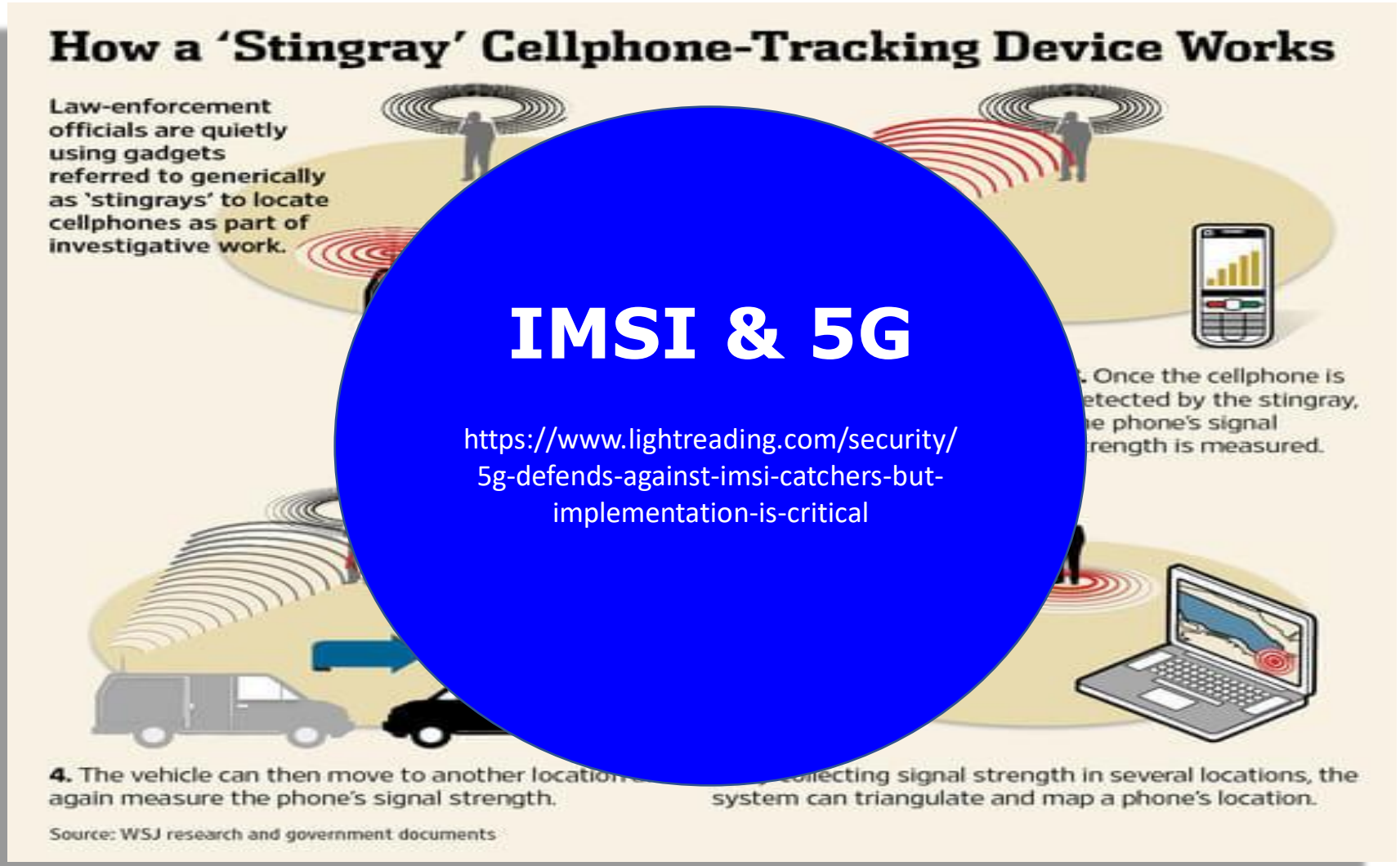
Source: https://www.extremetech.com/mobile/184597-stingray-the-fake-cell-phone-tower-cops-and-providers-use-to-track-your-every-move



Arms Race: IMSI Catcher Detectors

https://securityboulevard.com/2020/01/top-7-imsi-catcher-detection-solutions-for-2020/

InZeit
Excellence in Acuity

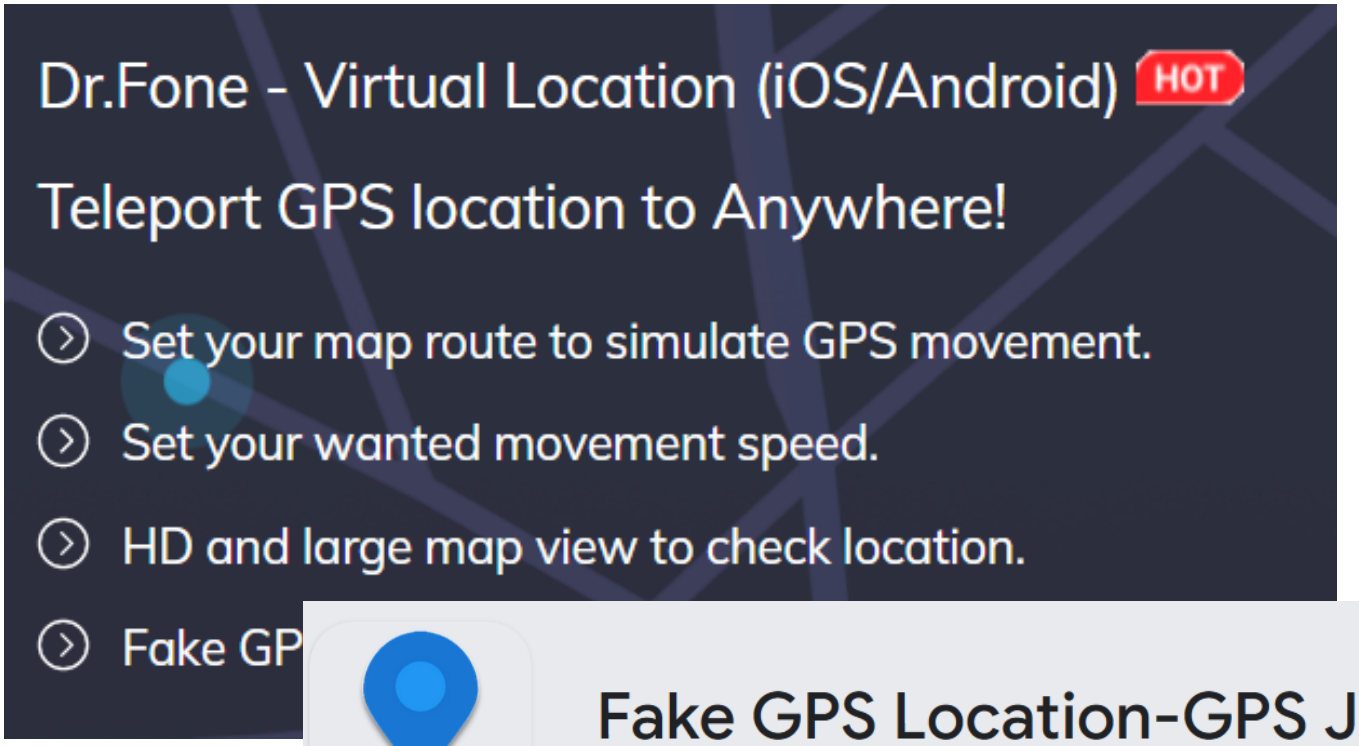

How a 'Stingray' Cellphone-Tracking Device Works
Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.
IMSI & 5G
https://www.lightreading.com/security/5g-defends-against-imsi-catchers-but-implementation-is-critical
Once the cellphone is detected by the stingray, the phone's signal strength is measured.
4. The vehicle can then move to another location and again measure the phone's signal strength.
collecting signal strength in several locations, the system can triangulate and map a phone's location.
Source: WSJ research and government documents

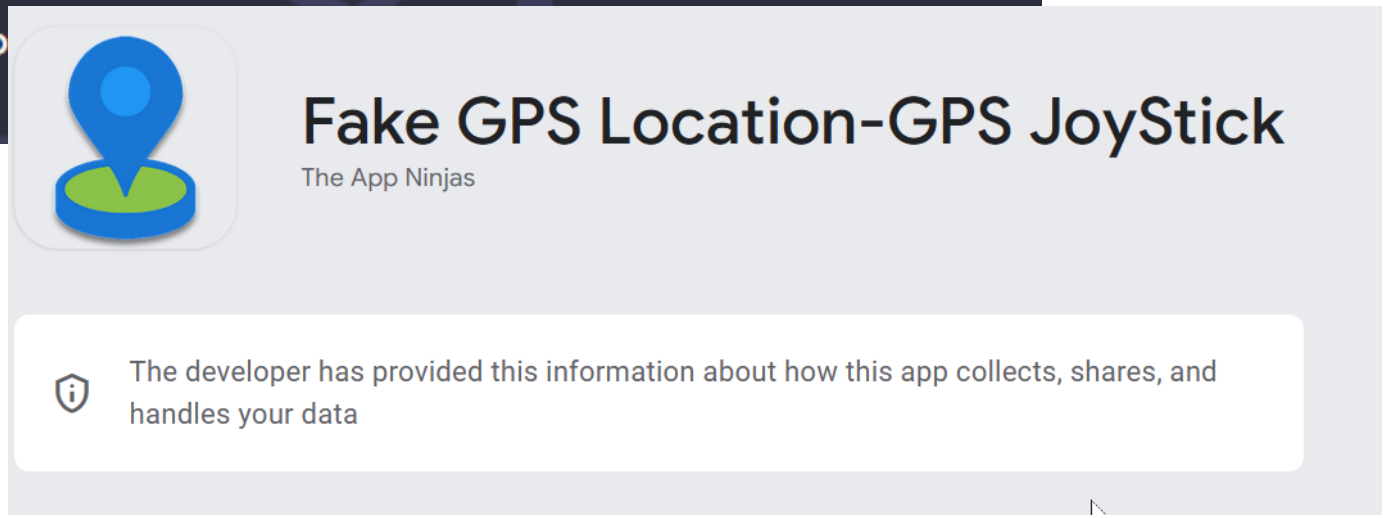
5G SUPI encryption is optional for operators. If 4G enabled, IMSI still works

Techniques exist to trace 5G phones

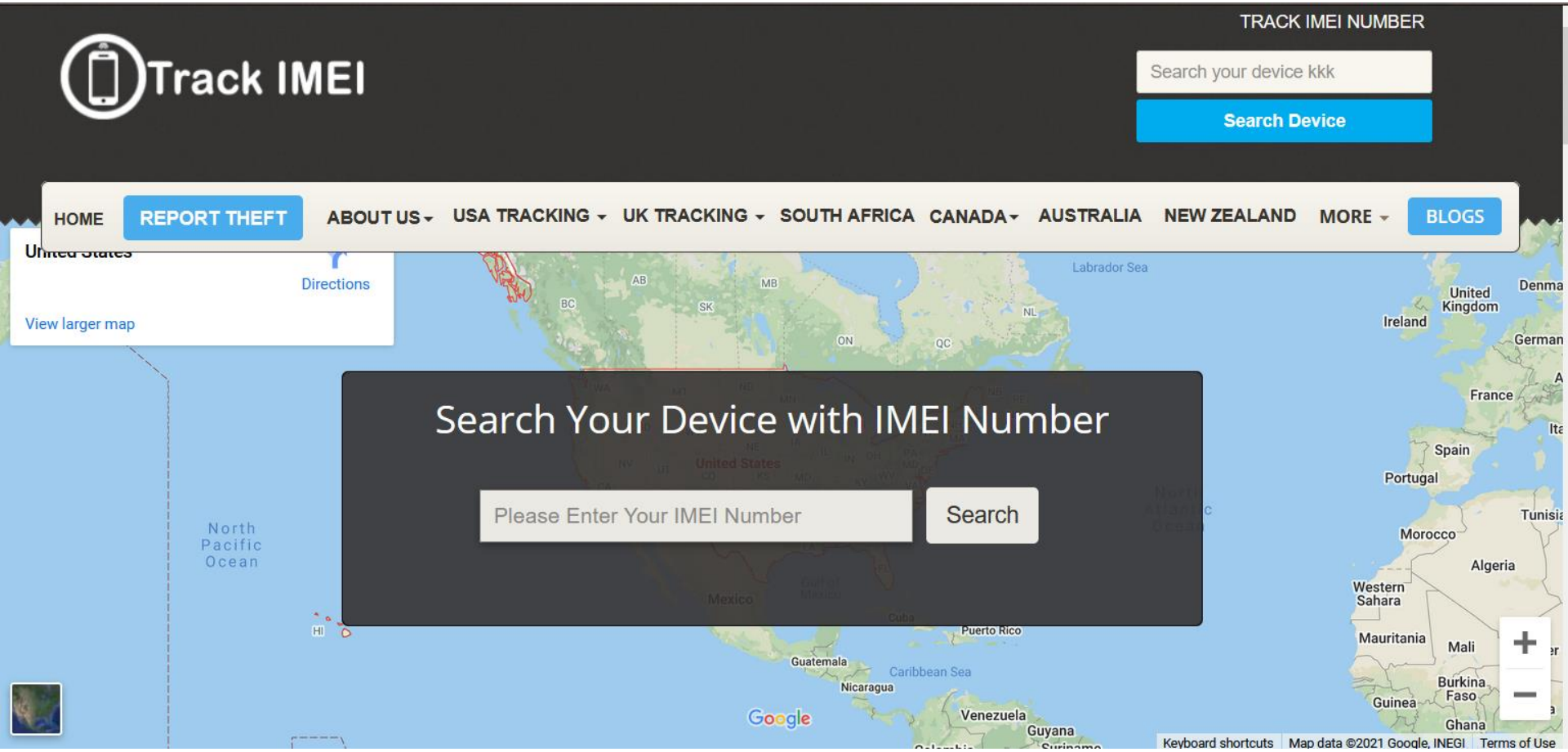
Chlosta, M. et al (2021) 5G SUCI-catchers: still catching them all? https://casa.rub.de/forschung/publikationen/detail/5g-suci-catchers-still-catching-them-all

InZeit
Excellence in Acuity



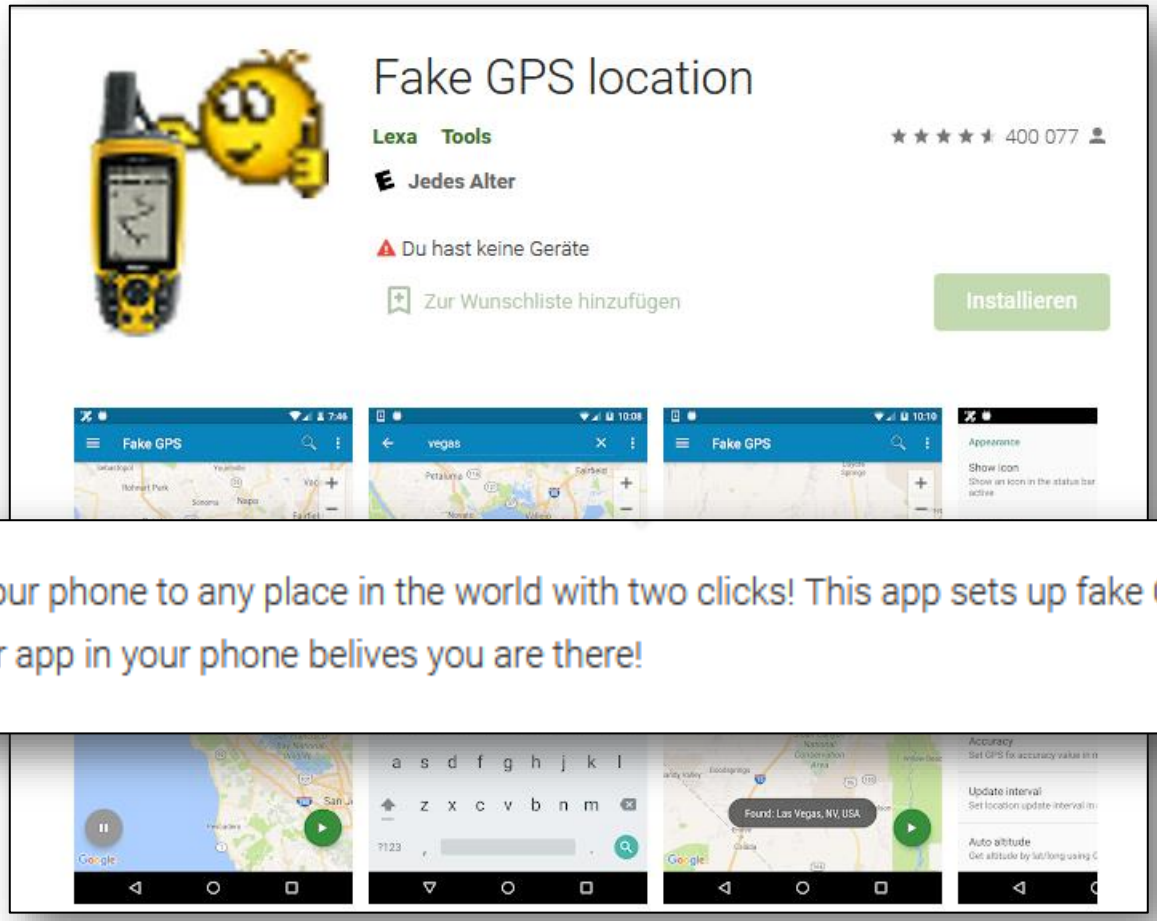


https://www.purevpn.com/uk/internet-privacy/how-to-spoof-your-location

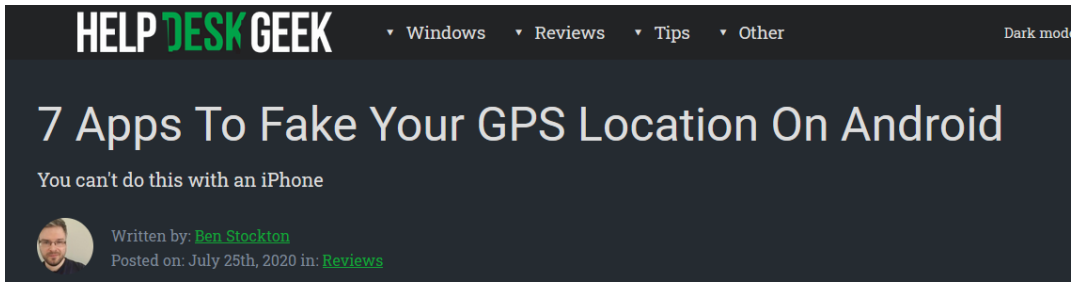


https://trackimei.net/

InZeit
Excellence in Acuity



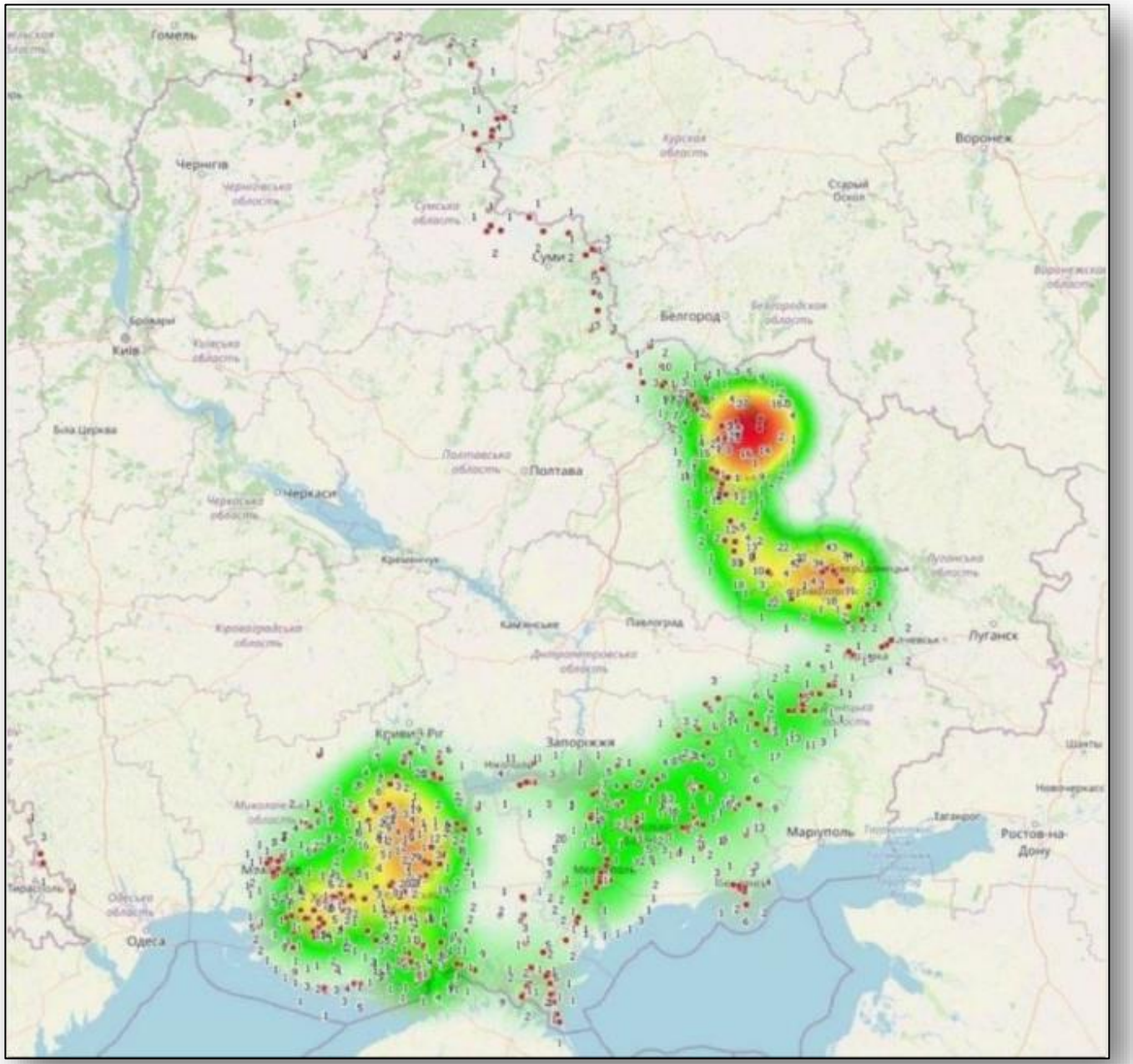
https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=de_AT&gl=US



https://helpdeskgeek.com/reviews/7-apps-to-fake-your-gps-location-on-android/

InZeit
Excellence in Acuity

Active Russian SIM cards (May 2022)



Source: Linkedin Post by Dan Kaine, Inherent Risks

InZeit
Excellence in Acuity

EXCLUSIVE: Russian spies are tracking British former special forces teams by their mobile numbers - and the data is then used to decide where to launch missile attacks

- **EXCLUSIVE: Kremlin has compiled a database of mobile phone numbers**
- **The information was gathered by spies near some of the UK's most sensitive military sites**
- **These include the headquarters of the Special Boat Service (SBS)**
- **Moment a mobile phone joins a local network their numbers are revealed to Russian agents**

By MARK NICOL DEFENCE EDITOR FOR THE DAILY MAIL
PUBLISHED: 22:01 GMT, 18 March 2022 | **UPDATED:** 22:34 GMT, 20 March 2022

https://www.dailymail.co.uk/news/article-10629125/Russian-spies-tracking-British-former-special-forces-teams-mobile-numbers.html

EXCLUSIVE: Russian spies are tracking British former special forces teams by their mobile numbers - and the data is then used to decide where to launch missile attacks

- EXCLUSIVE: Kremlin has compiled a database of mobile phone numbers
- The information was gathered by spies near some of the UK's most sensitive

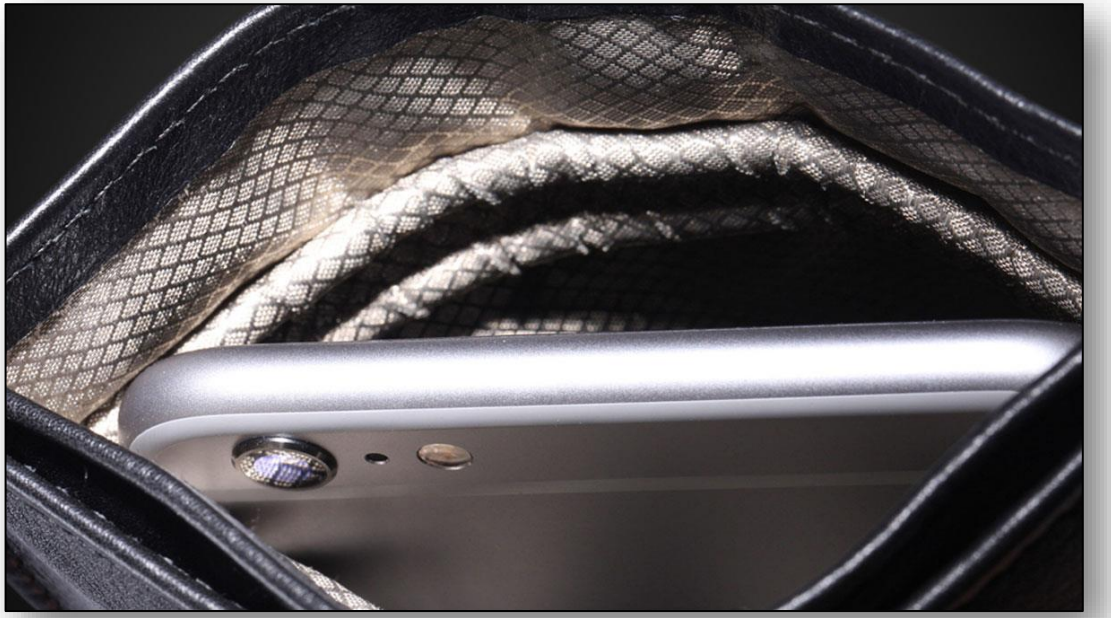
Moscow blames its troops' use of mobile phones for Makiivka missile strike

Ukrainian shelling that killed 89 recruits aided by mobiles switched on near frontlines, claims Russia defence ministry

https://www.theguardian.com/world/2023/jan/04/moscow-blames-its-troops-use-of-mobile-phones-for-makiivka-missile-strike

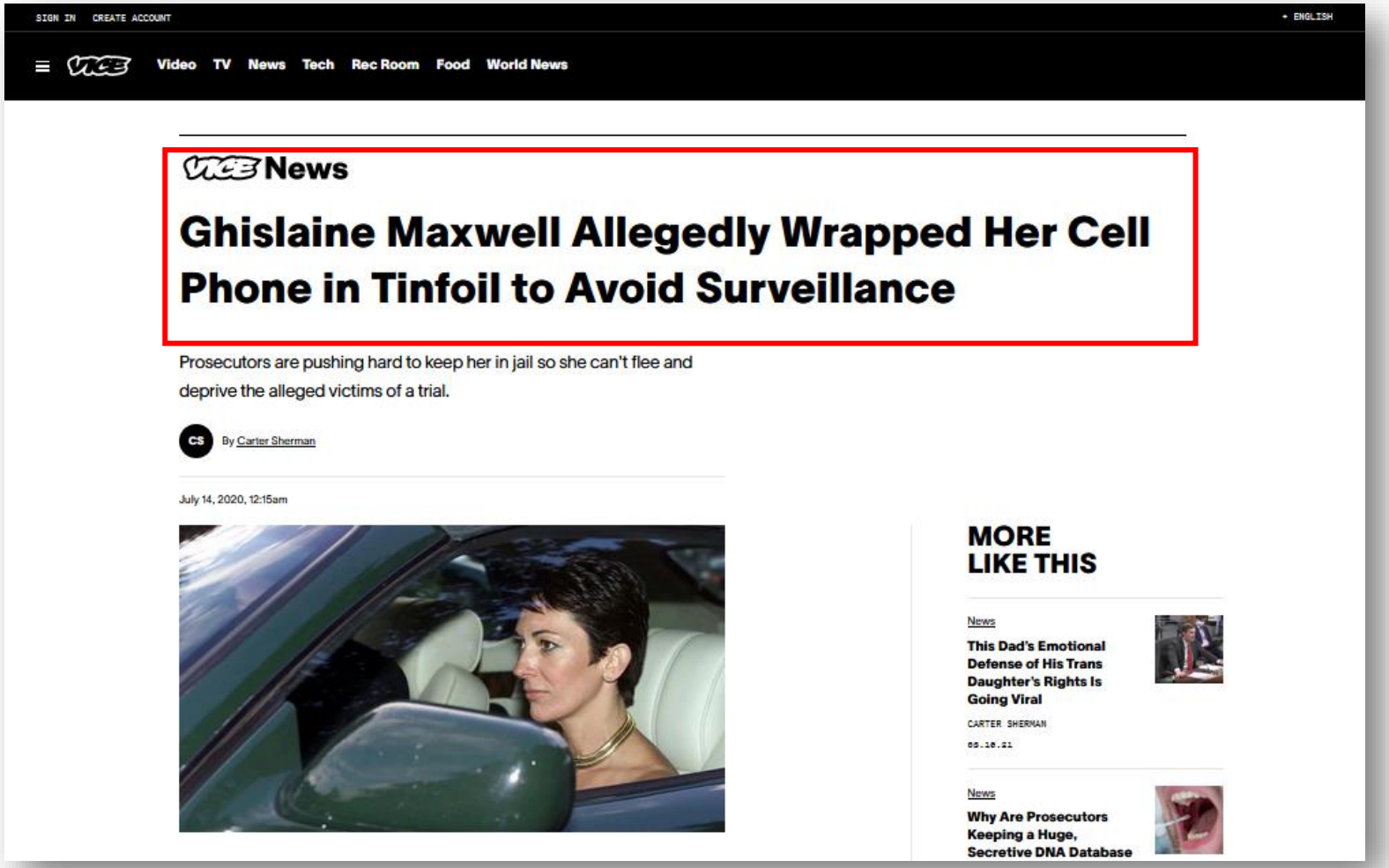
If phone powered off or isolated (e.g. inside a Faraday bag), can't be located.

Faraday bag = container lined with metallic substance to block radio waves



InZeit
Excellence in Acuity

https://www.vice.com/en/article/pkyz3n/ghislaine-maxwell-allegedly-wrapped-her-cell-phone-in-tinfoil-to-avoid-surveillance



'Cell phone data' (GPS and/or cell site analysis?) > 1 square mile (2.59 km²)

InZeit
Excellence in Acuity

GSMA

Unique mobile subscribers

2022 **496m**

2030 **507m**

90% 2022

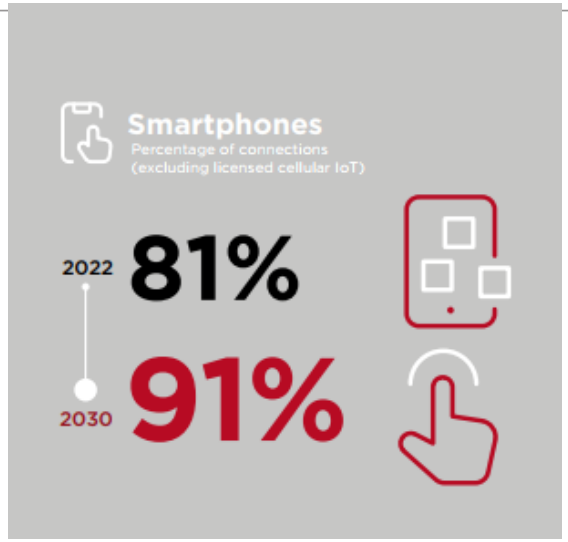
92% 2030

Penetration rate
Percentage of population

CAGR 2022-2030 **0.3%**

The Mobile Economy Europe 2023

Very high probability of phone evidence



Not just suspects … victims & witnesses

InZeit Excellence in Acuity

https://www.gsma.com/mobileeconomy/europe/

Typical smart phone:

Contains, text, images, video, games, applications like WhatsApp, FB messenger, Snapchat, Telegram, Instagram

64GB phone (6GB for operating system) = 58GB data

11,600 x Complete Works of William Shakespeare

Potentially 5,800,000 messages (some as small as 10 bytes) which may not be keyword searchable

InZeit
Excellence in Acuity

Verity Méchant blog 30 Jan 2018
https://encroaching.wordpress.com/

December 2017 Liam A. on trial for 12 counts of rape & sexual assault

- Case thrown out
- Alleged victim's phone contents downloaded
- Investigator said 'nothing relevant'
- Defence Counsel Julia Smart reviewed 40,000 SMS messages (pdf file 2,500 A4 pages) – 57,000 messages on phone

"I read them through the night and into the next morning. It was laborious but I found messages that completely undermined the case."

10:00PM – 04:00AM (6 hours non-stop)

Client Side Scanning

https://www.europol.europa.eu/media-press/newsroom/news/146-children-worldwide-saved-in-operation-targeting-child-abuse-online?mtm_campaign=newsletter

The problem: End to end encryption

Data encrypted in transit

Proposed solution 1: require a Backdoor

Proposed solution 2: scan data on sender's device before encryption

Apple introduced in USA in August 2021 to scan photo libraries on iPhones.
Ceased 3rd Sept 2021.

Obligatory & Indiscriminate

Scope for abuse?

"The EU wants to oblige providers to search all private chats, messages, and emails automatically for suspicious content – generally and indiscriminately. The stated aim: To prosecute child pornography. The result: Mass surveillance by means of fully automated real-time messaging and chat control and the end of secrecy of digital correspondence."

Patrick Breyer MEP

11 May 2022: Presentation of Commission proposal on mandatory messaging and chat controls for online service providers (tbc)

https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/

InZeit
Excellence in Acuity

Court of Justice of the European Union

PRESS RELEASE No 58/22

Luxembourg, 5 April 2022

Press and Information

Judgment in Case C-140/20
Commissioner of An Garda Síochána and others

The Court confirms that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime

The national court may not impose a temporal limitation on the effects of a declaration of invalidity of a national law that provides for such retention

(Compare Google's Sensorvault & AI "Act" Art.20 on High Risk AI system logs)

https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-04/cp220058en.pdf

InZeit
Excellence in Acuity

Phone Kiosks

Phones contain intimate and confidential material

Extracts more that the 'evidence'

Witnesses view it as invasion of privacy

What if data discloses offences by the owner?

Consent Forms: Victims of sexual offences felt psychologically manipulated ("if you don't let us, we won't be able to prosecute")

Summary

Phone location evidence not as accurate as often portrayed

Influenced by lots of factors (technical/topographical/meteorological)

Our personal data is traded for profit

Mobile devices pose unresolved challenges:

- **Volume of data**
- **Cost & time to review**
- **Comingling relevant/not relevant data**

InZeit
Excellence in Acuity

Robust investigation inevitably involves invasive powers (nothing new there)

No ideal options for extracting phone data

3rd party spyware
Encryption Backdoors
Client-Side Scanning
Phone kiosks
Consent
Digital Forensic Examination

Oversight, regulation and Codes of Conduct essential

info(at)inzeit(dot)eu

References & Further Reading

Barratt, B. (2018) A Location-Sharing Disaster Shows How Exposed You Really Are https://www.wired.com/story/locationsmart-securus-location-data-privacy/

Berkeley Law (2015)"Cell Site Simulator Primer" https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_Cell-Site-Simulator-Primer_Final.pdf

Bischoff,P. (2023) *Which governments ipose SIM-card registrationlaws to ollect data on their citizens?* https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/

Bowcott,O. (2019*) Rape cases 'could fail' if victims refuse to give police access to phones* The Guardian 29/04/2019 https://www.theguardian.com/society/2019/apr/29/new-police-disclosure-consent-forms-could-free-rape-suspects

CARPENTER v. UNITED STATES (2018) *Supreme Court of the United States No. 16–402. (22 June 2018)* https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Court Listener (2018) *STATE OF FLORIDA v. QUINTON REDELL SYLVESTRE* https://www.courtlistener.com/opinion/4532524/state-of-florida-v-quinton-redell-sylvestre/

Cox, J. (2019) *I Gave a Bounty Hunter $300. Then He Located Our Phone* https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile

Crown Prosecution Service (2018) Disclosure - Guidelines on Communications Evidence *https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence*

Chlosta, M. et al (2021) 5G SUCI-catchers: still catching them all? https://casa.rub.de/forschung/publikationen/detail/5g-suci-catchers-still-catching-them-all

Daniel. L (2019) *Cell phone location evidence for Legal Professionals* Academic Press

Dearden, L. (2017) Rape trial collapse over undisclosed sex messages blamed on police funding cuts https://www.independent.co.uk/news/uk/crime/rape-trial-collapse-sex-text-messages-police-funding-cuts-liam-allan-disclosure-phone-innocent-miscarriages-justice-a8113011.html

Hollister, S. (201) Carriers can sell your location to bounty hunters because ISP privacy is broken https://www.theverge.com/2019/1/8/18174024/att-sprint-t-mobile-scandal-phone-location-tracking-black-market-bounty-hunters-privacy-securus

UK Home Office (2021) Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheethttps://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet

Information Commissioner's Office (2020) Mobile Phone Data Extraction https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/

Krebs, K. (2018) *Tracking Firm LocationSmart Leaked Location Data for Customers of All Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site* https://krebsonsecurity.com/2018/05/tracking-firm-locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-via-its-web-site/

Miller, G. and Parsons, C. (2023) *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure* Citizen Lab Research Report No. 171 https://citizenlab.ca/2023/10/finding-you-telecommunications-vulnerabilities-for-location-disclosure

Krebs, K. (2021) *Can We Stop Pretending SMS Is Secure* Now? https://krebsonsecurity.com/2021/03/can-we-stop-pretending-sms-is-secure-now/

McCubbin, S (2018) *Summary: The Supreme Court Rules in Carpenter v. United States* https://www.lawfareblog.com/summary-supreme-court-rules-carpenter-v-united-states

Metropolitan Police Service (2015) *MPS – Digital, Cyber and Communications Forensics Unit Information for Prospective Bidders* https://www.documentcloud.org/documents/3280381-MPS-Digital-Cyber-and-Communications-Forensics.html

NPCC (2020) DPNb Witness Information Sheet https://news.npcc.police.uk/resources/dpnb-witness-information-sheet

Ouziel, N (2020) Top 7 IMSI Catcher Detection Solutions for 2020 https://securityboulevard.com/2020/01/top-7-imsi-catcher-detection-solutions-for-2020/

Privacy International Digital Stop and Search: How UK police can secretly download everything on your mobile phone(2018) https://www.privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile

Ramasamy, S. (2021) *5G Security - SUCI Catcher* https://www.linkedin.com/pulse/5-security-suci-catcher-ramasamy-cissp-cism-gcti-gnfa-gcda-cipm

Schuppe, J. (2020) *Google tracked his bike ride past a burglarized home. That made him a suspect.* https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

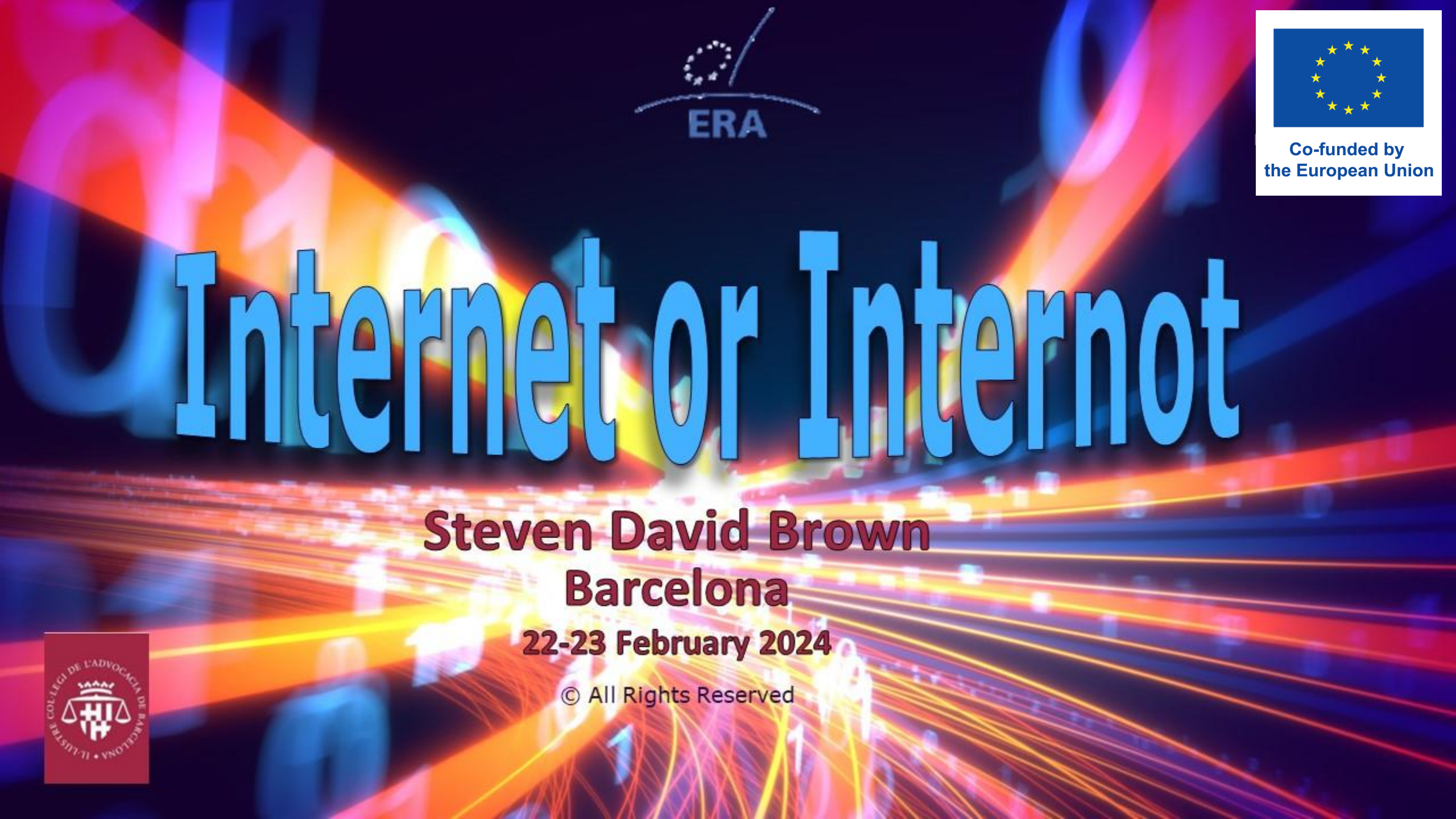
U of Derby DECM (2019) *Accuracy of Location Services on Smart Devices* Blog https://computing.derby.ac.uk/c/accuracy-of-location-services-on-smart-devices/

Valentino-DeVries, J. (2019) *Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works* New York Times (13/04/2013)

Valentino-DeVries, J. (2018) Service Meant to Monitor Inmates' Calls Could Track You, Too New York Times (10/05/2018)

Whittaker, Z (2019) *Despite promises to stop, US cell carriers are still selling your real-time phone location data* https://techcrunch.com/2019/01/09/us-cell-carriers-still-selling-your-location-data/

Kim Zetter (2015) *Hackers Could Heist Semis by Exploiting This Satellite Flaw* https://www.wired.com/2015/07/hackers-heist-semis-exploiting-satellite-flaw/


ERA
Co-funded by
the European Union
Internet or Internot
Steven David Brown
Barcelona
22-23 February 2024
© All Rights Reserved

What is the Internet ?

Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

https://www.britannica.com/technology/Internet

World Wide Web (WWW) […] the leading information retrieval service of the Internet (the worldwide computer network). The Web gives users access to a vast array of documents that are connected to each other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of information in order to allow a user easy access to them.

https://www.britannica.com/topic/World-Wide-Web

Please note: Information has been simplified to make it easier to understand and remember

What is the Internet ?

Internet, a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect. Sometimes referred to as a "network of networks"

https://www.britannica.com/technology/Internet

World Wide Web (WWW) […] the leading information retrieval service of the Internet (the worldwide computer network). The Web gives users access to a vast array of documents that are connected to each other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of information in order to allow a user easy access to them.

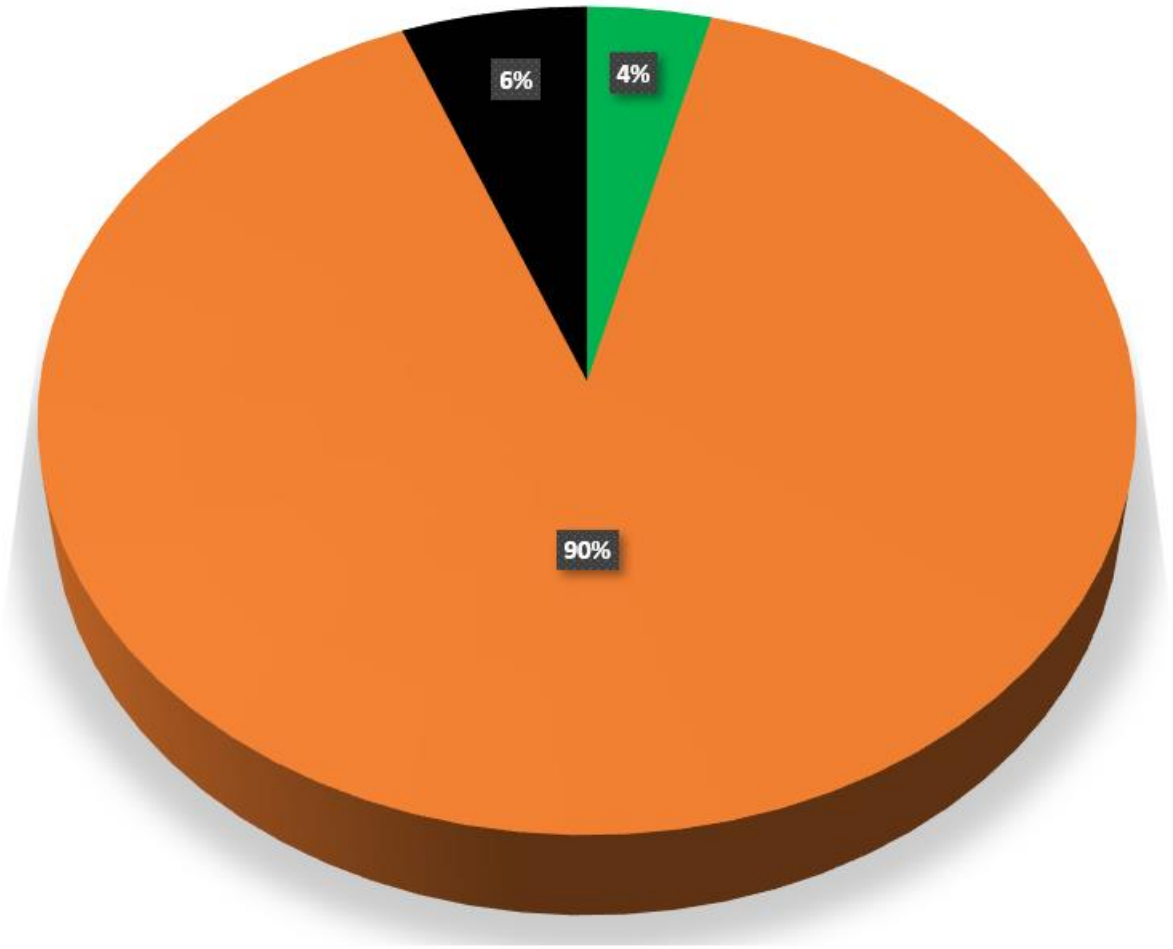
https://www.britannica.com/topic/World-Wide-Web

Internet - a "network of networks"

Different types and scope of network:

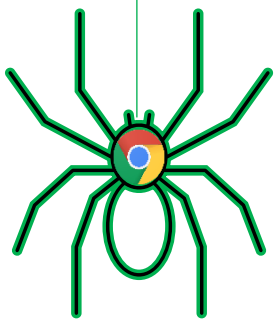
WAN	Wide Area (Not confined geographically)
LAN	Local (Short Distance)
WLAN	Wireless Local Area
MAN	Metropolitan Area
PAN	Personal Area (one or two main devices)
CAN	Campus Area

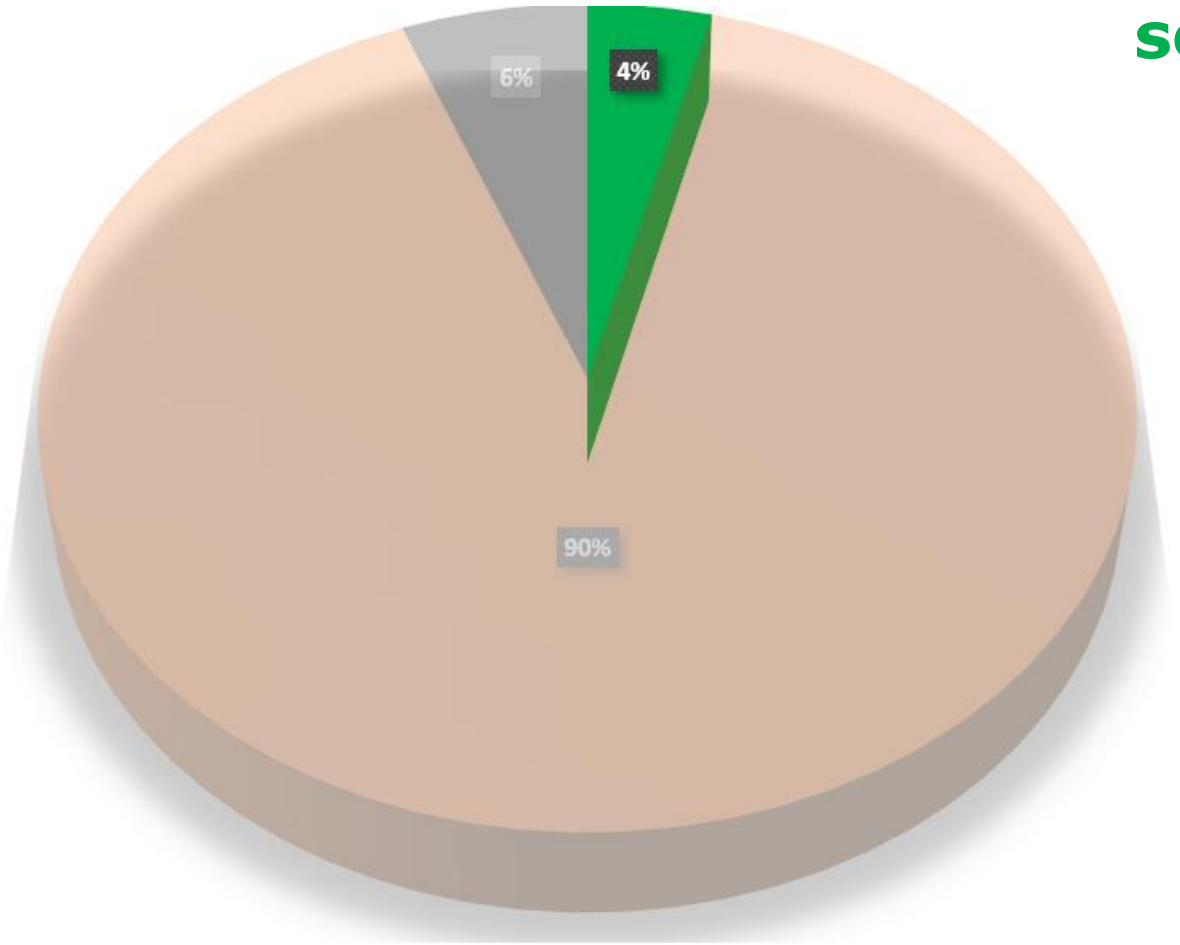
The Internet



N.B. The percentages are educated guesswork.

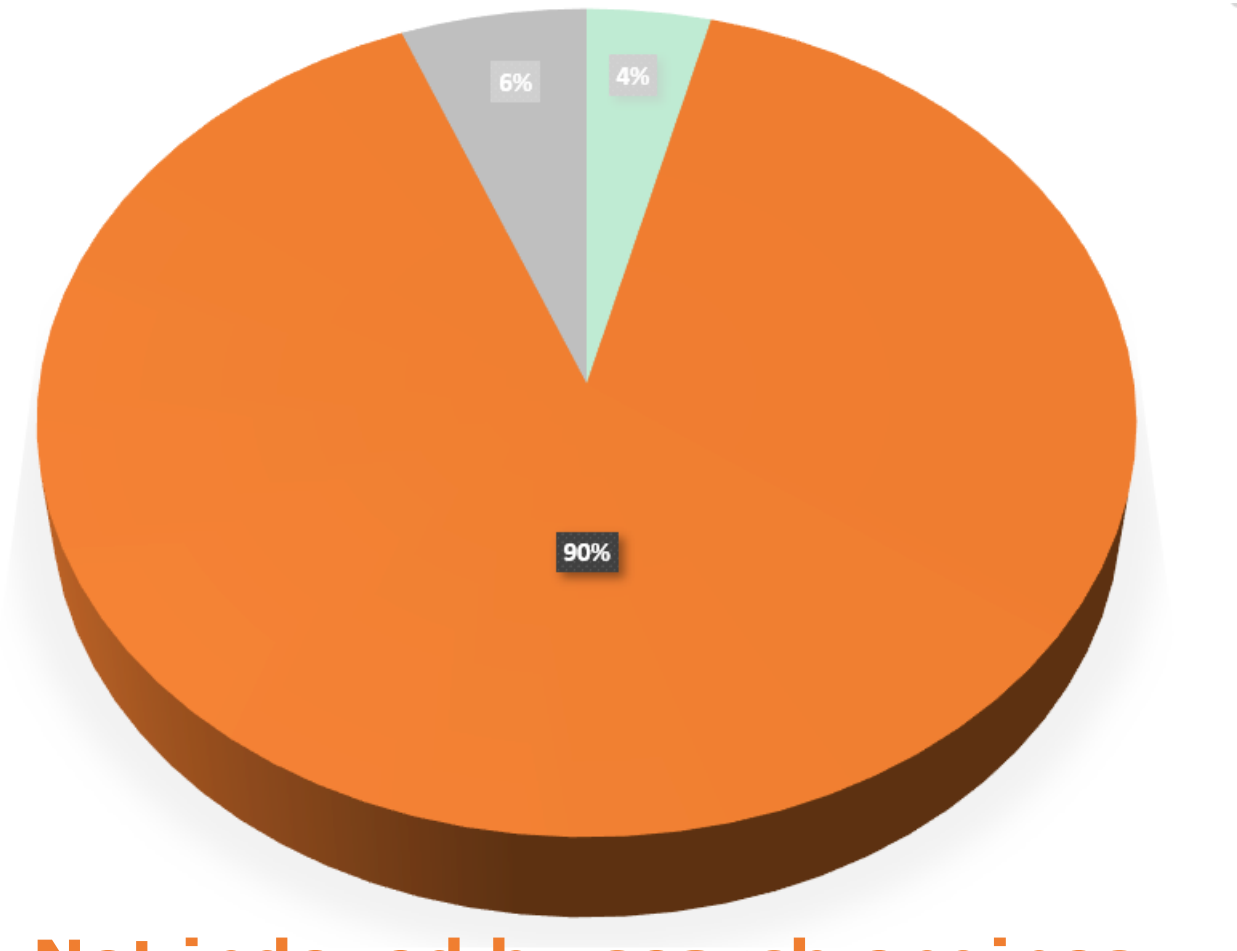
WWW 4%





WWW
Indexed by search engines; publicly accessible

Deep Web 90%

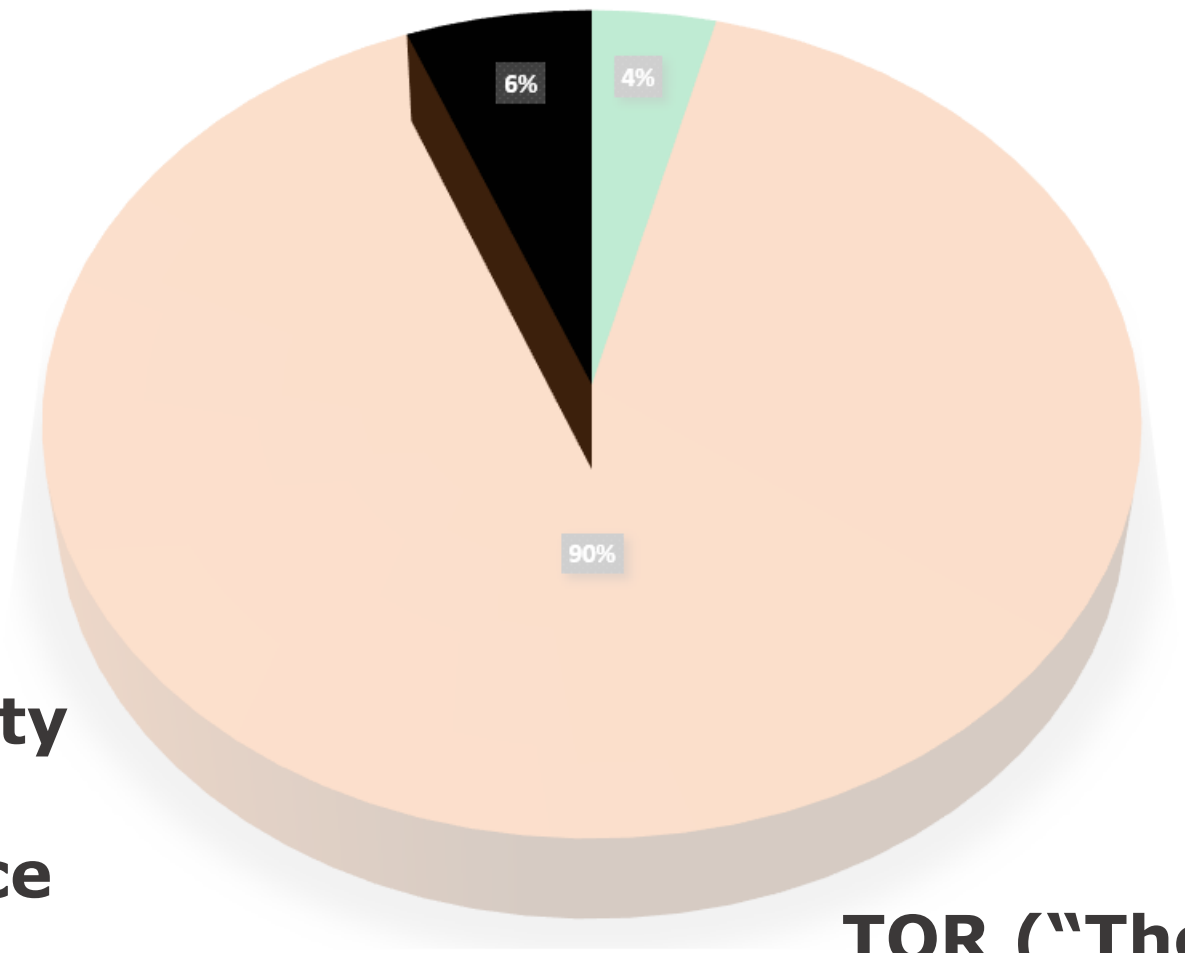


Not indexed by search engines:
Govt. communications;
banks; corporations; medical records;

InZeit
Excellence in Acuity

DarkNet 6%

Special software for access; spies, dissidents & criminals



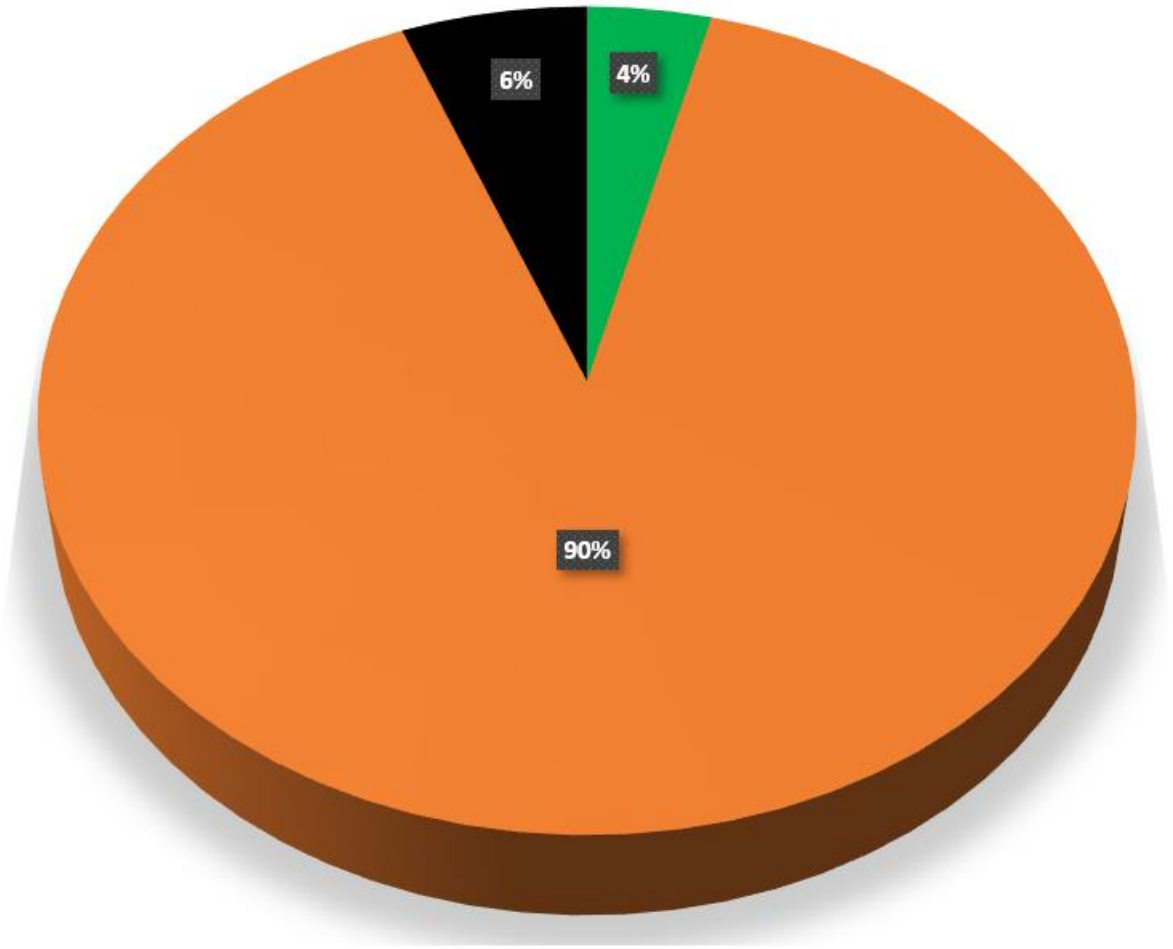
Internet Anonymity and prevents online surveillance

TOR (“The Onion Router”) Started as US Navy-funded project 1995

InZeit
Excellence in Acuity

DarkNet 6%

WWW 4%

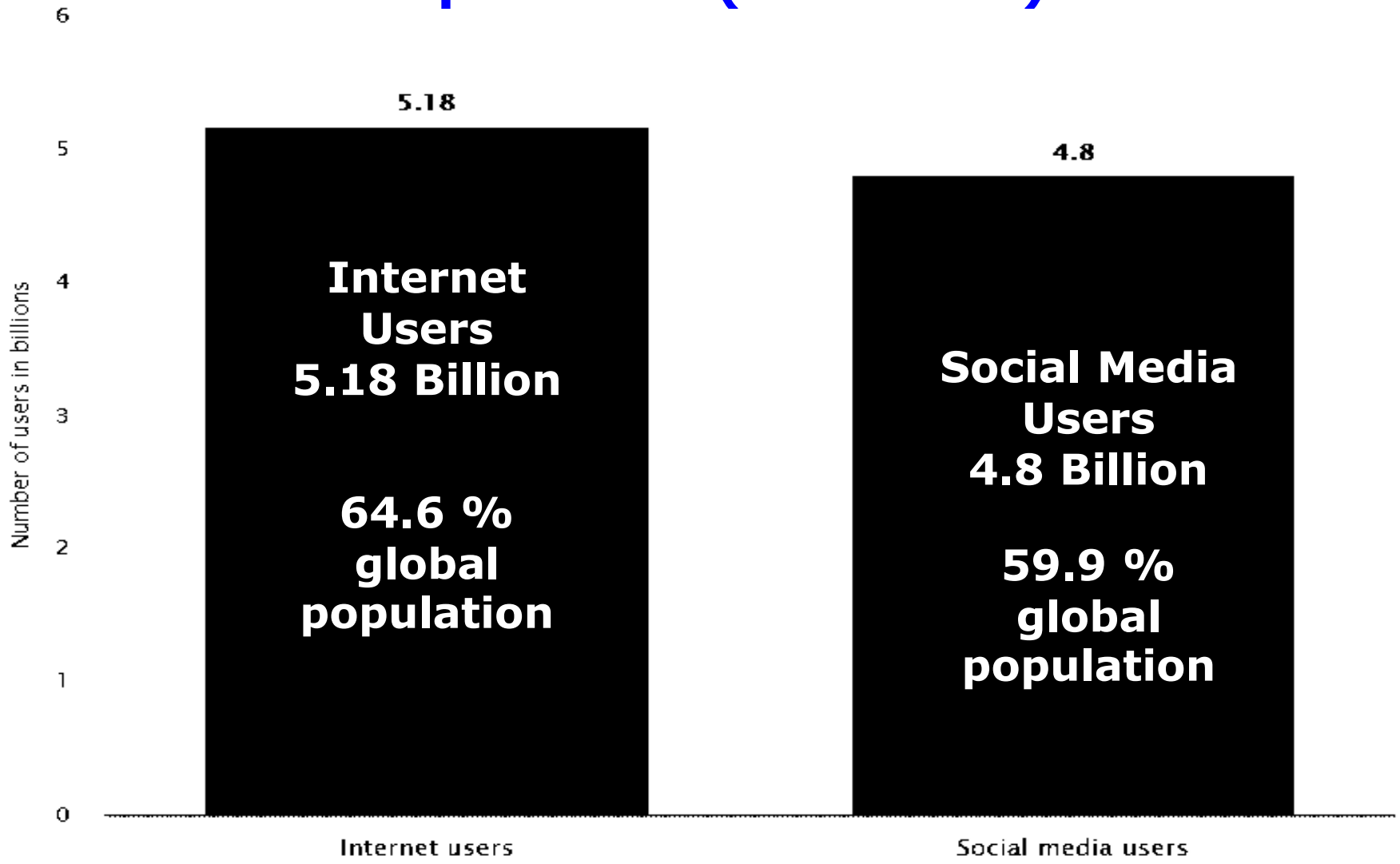


Deep Web 90%

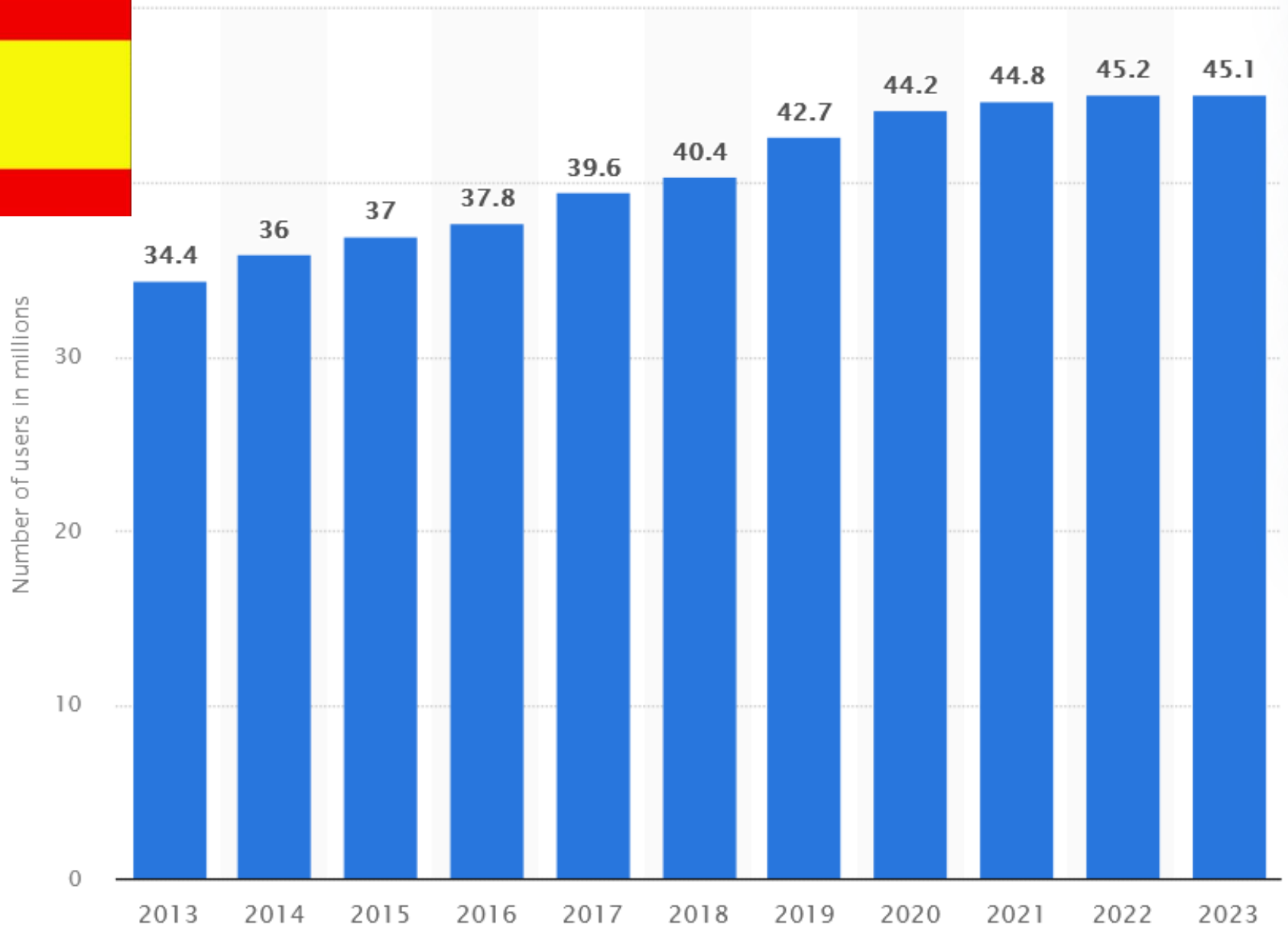
InZeit
Excellence in Acuity

**Conseil européen pour la recherche nucléaire*

Number of internet and social media users worldwide as of April 2023 (in billions)



Source: Statista May 22, 2023
https://www.statista.com/statistics/617136/digital-population-worldwide/



Source: Statista Nov 23, 2023
https://www.statista.com/statistics/1306497/internet-users-spain/

US DARPA
"ARPANET"
29 Oct 1969

Sir Tim Berners-Lee
CERN* 1989

*European Organization for Nuclear Research

The Internet

Insecure by design

InZeit
Excellence in Acuity

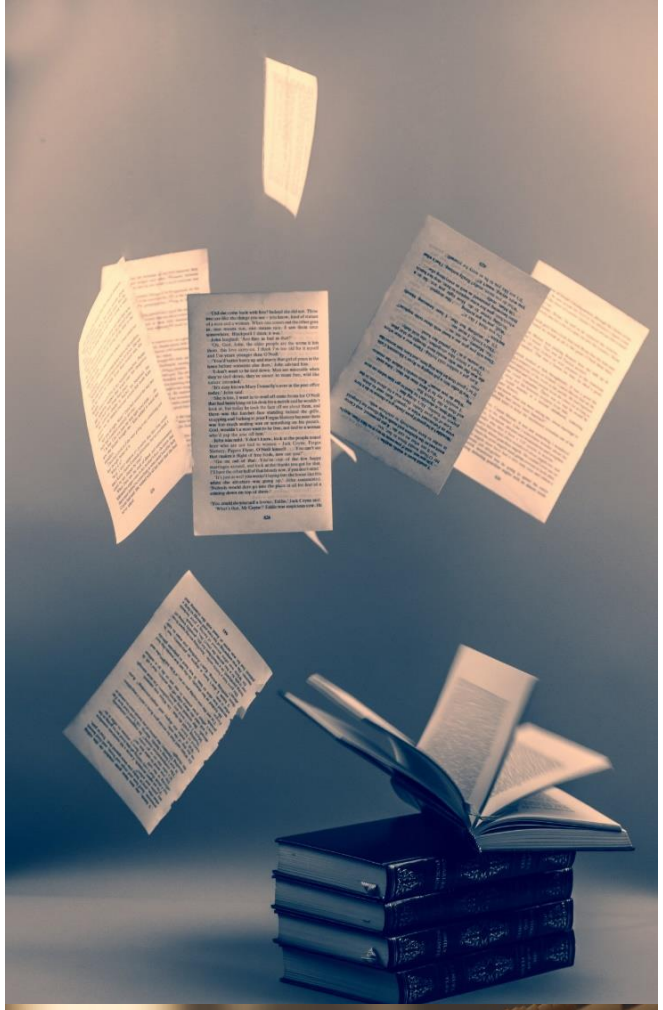
HTTP & HTTPS
(Hyper Text Transfer Protocol (Secure))

Indexed 'pages'

Collection of pages = Website

Unique Resource Locators (URLs)
= the website address in words
(linked to IP Address)

Domain Name
= the name you remember + the domain extension
(e.g. era.int)



InZeit
Excellence in Acuity

http://www.era.int

Protocol

http://www.era.int

Protocol

http://www.era.int

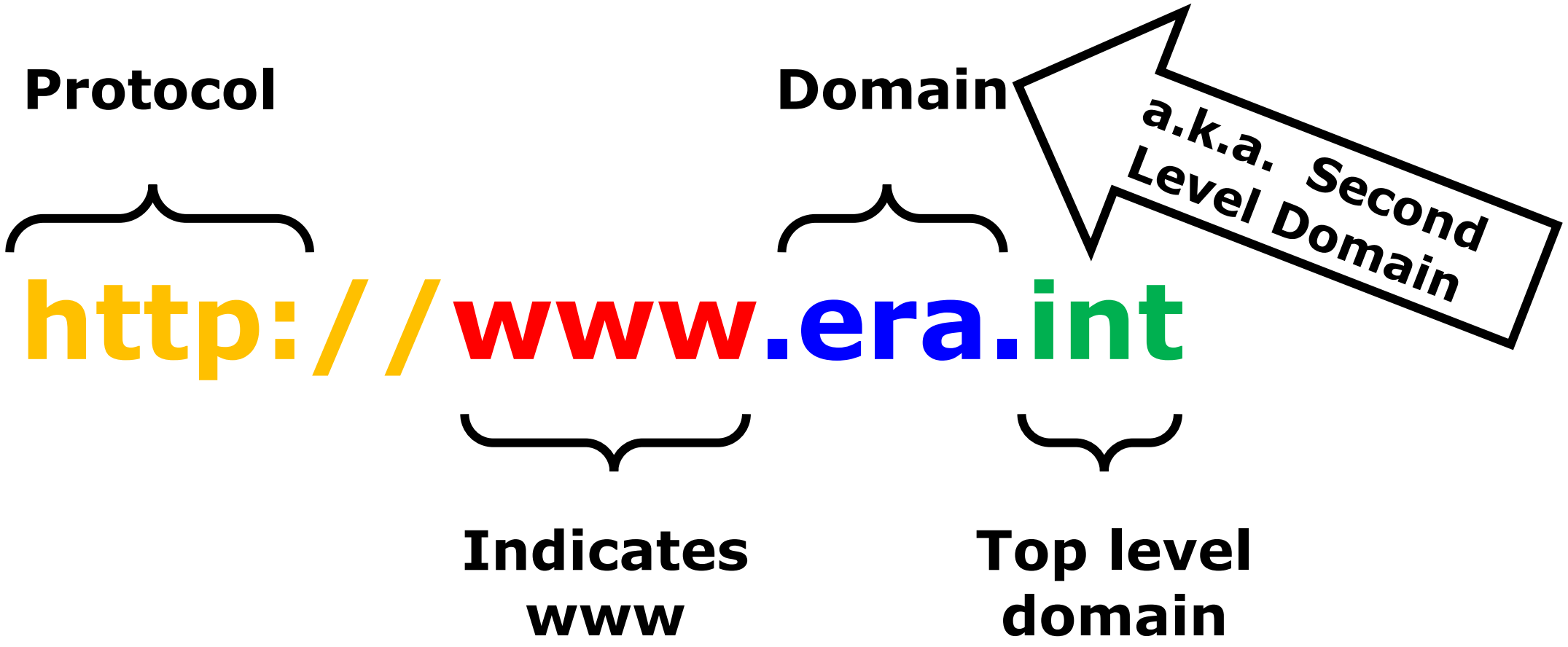
Indicates www

Protocol

Domain

http://www.era.int

Indicates www



.gov .com .edu .org .net .co.uk .de .fr

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Whois

Register of Internet domain name ‘owners’

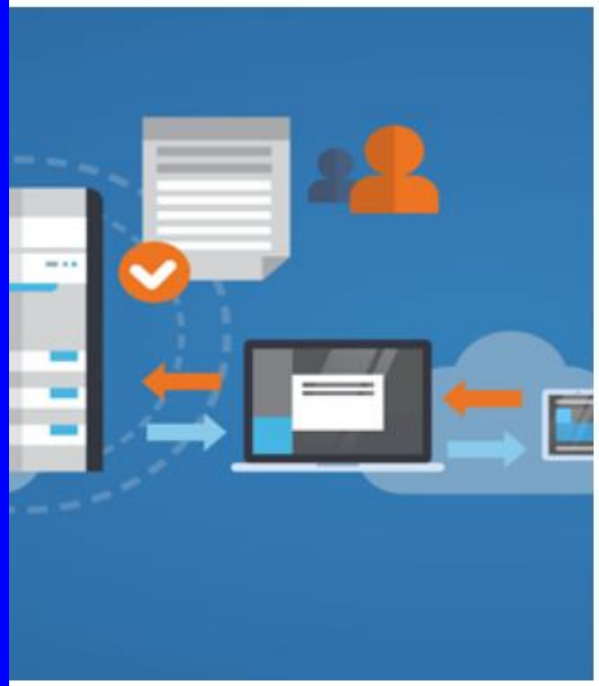
- Registrant data may be false
- Hidden behind a registration service
- Place to start search
- EU GDPR Rules – Whois blocked

(Authorised groups still have access)

r 2023

"The service will be used by participating ICANN-accredited registrars and requestors seeking nonpublic gTLD registration data. **It is intended for use by individuals and entities** with a legitimate interest for access to **nonpublic** gTLD registration data **like law enforcement, government agencies, intellectual property attorneys, cybersecurity professionals, and others**. Participation in the service by ICANN-accredited registrars will be voluntary

ata



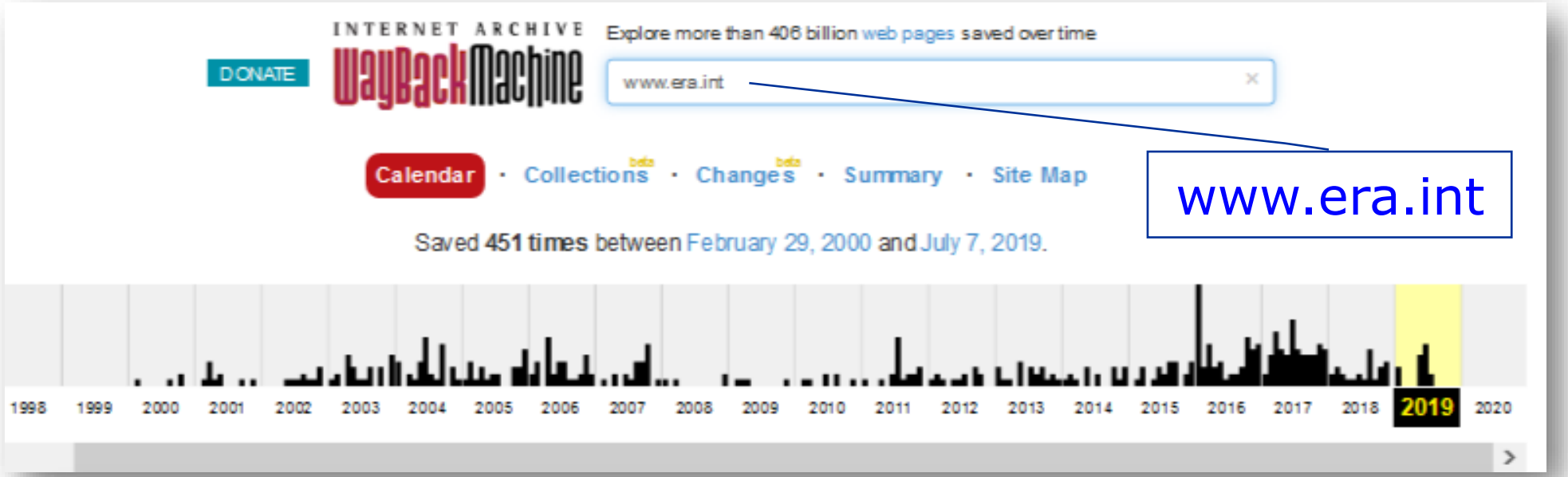
To submit a request for nonpublic
nt (new or existing) to access the

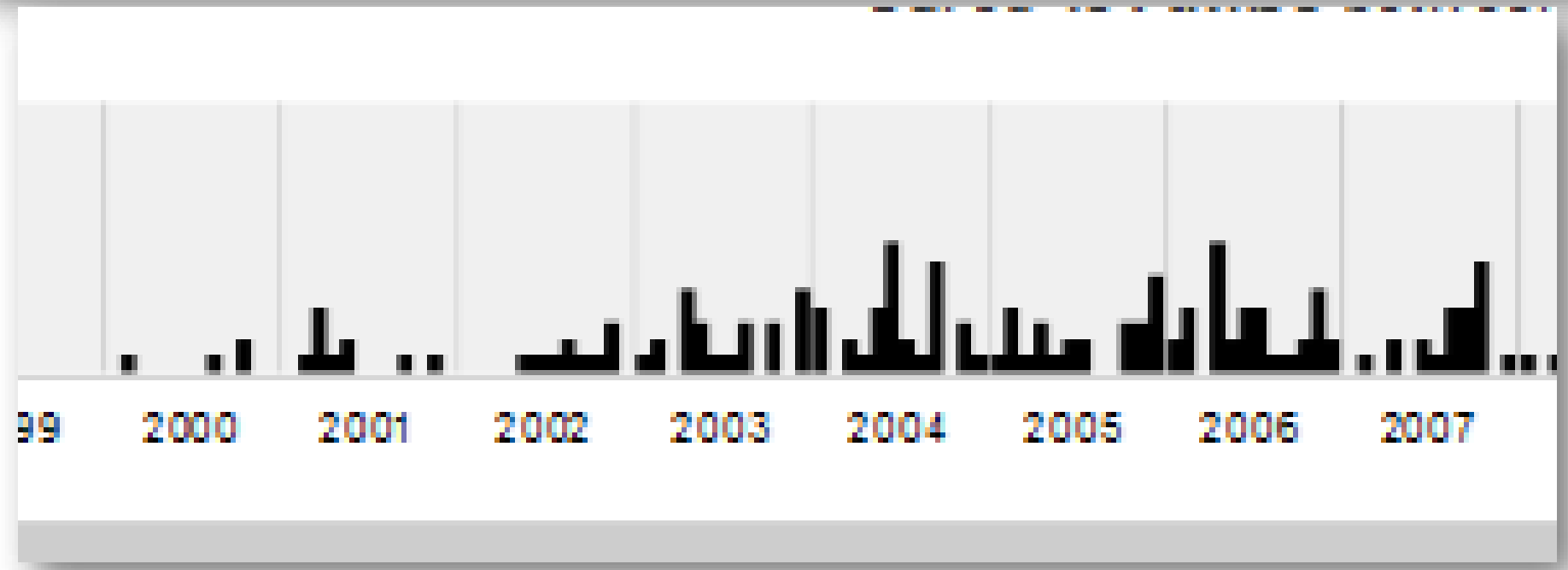
https://www.icann.org/rdrs-en

InZeit
Excellence in Acuity

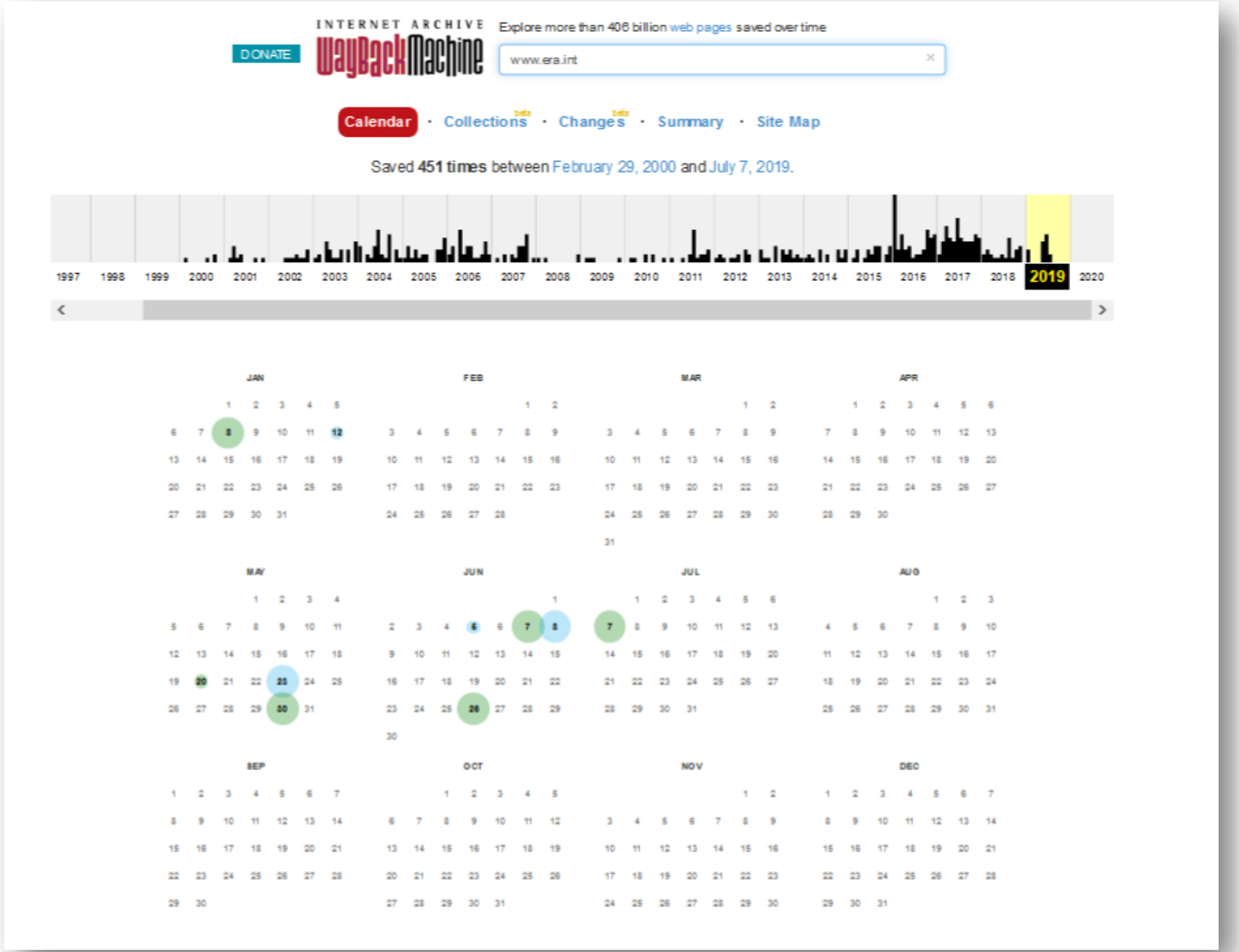
When websites change:

(http://web.archive.org)

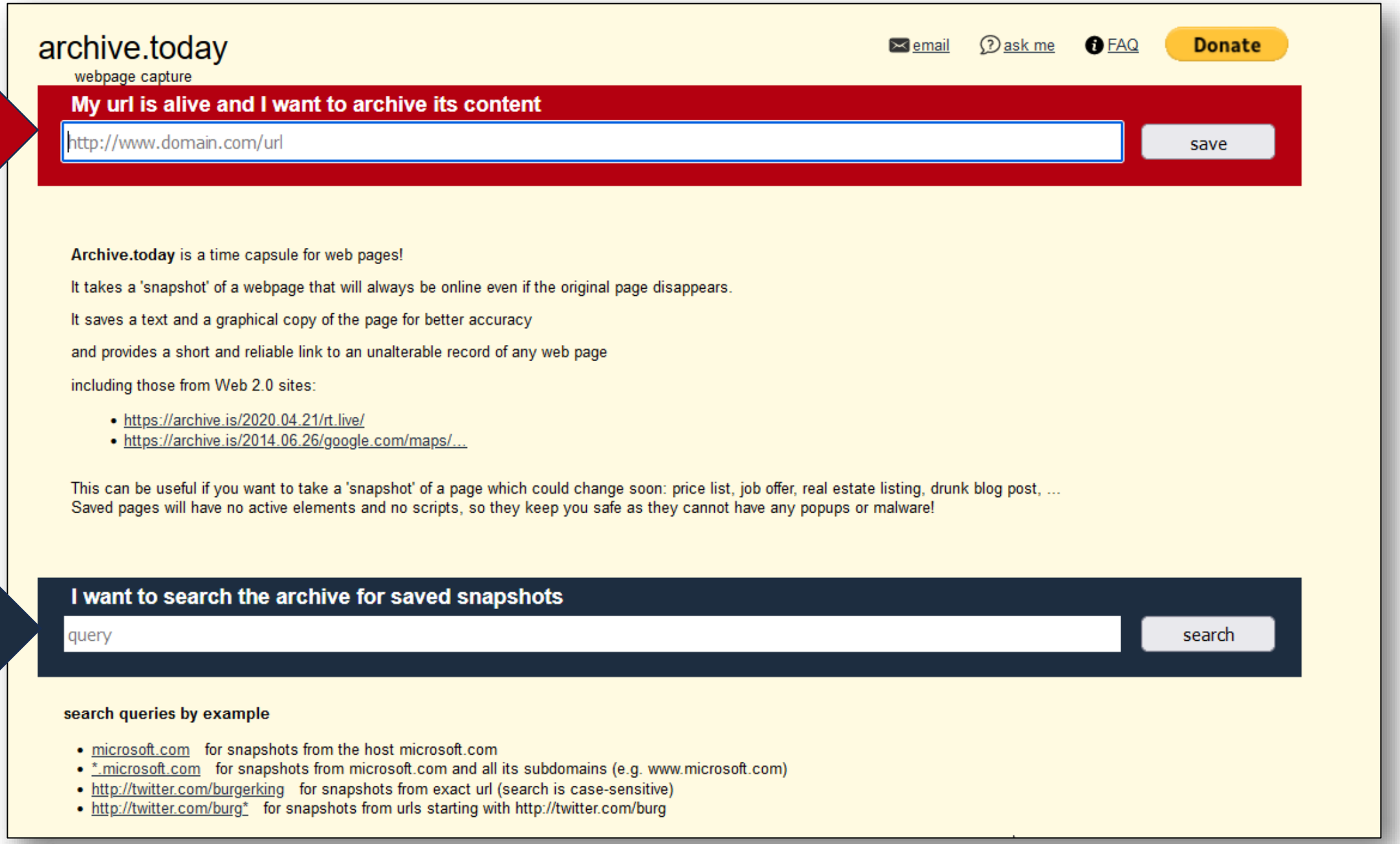




InZeit
Excellence in Acuity



Website from 23 June 2000



InZeit Excellence in Acuity

archive.is/archive.today

Normally:
First step is to l
the IP A

Can be faked, hidden or 'borrowed'

An Internet ess is the unique number generated Service Provider and assigned to a connec to identify the source & destination of messages across the Internet (like a postal address).

Example: tracking a Russian Money Launderer

2014 Tokyo Bitcoin Exchange went bankrupt

Hacked:

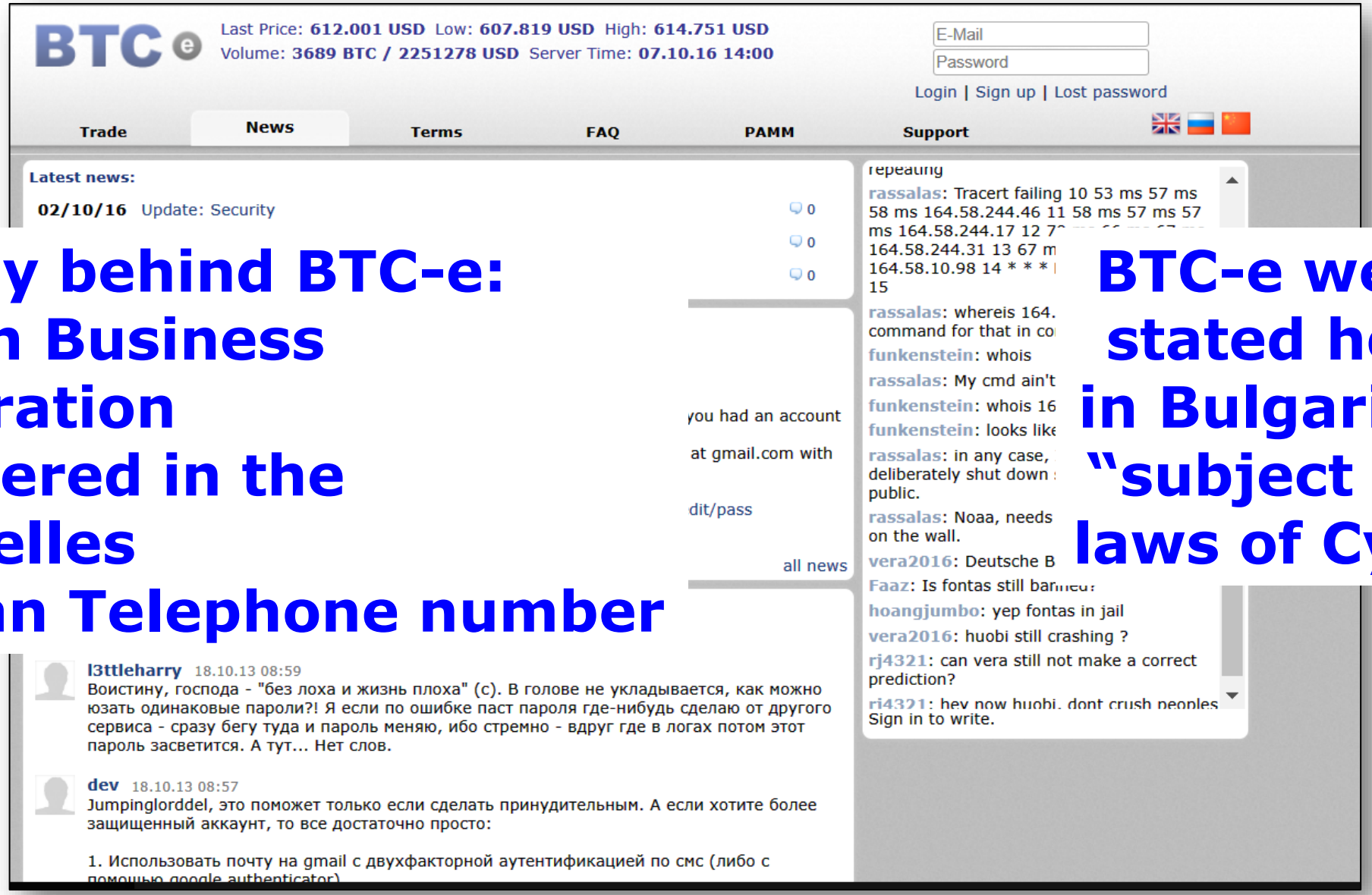
750,000 BTC users
100,000 BTC own
(7% of all BTC in existence)

“Loss: $530million”

Stolen BTC tracked by Chainalysis

Eventually ended up at BTC-e Exchange

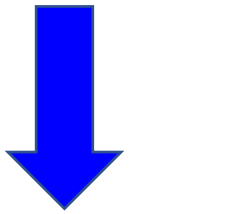
BTC-e ownership and location unknown

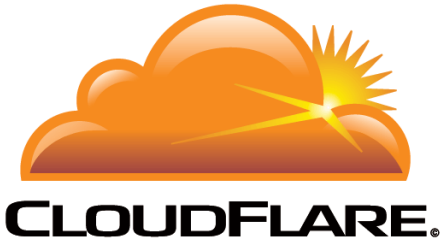


Company behind BTC-e:

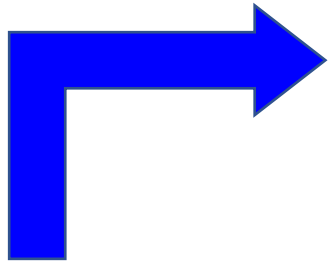
- **Canton Business Corporation**
- **Registered in the Seychelles**
- **Russian Telephone number**

BTC-e website stated hosted in Bulgaria, but "subject to the laws of Cyprus"

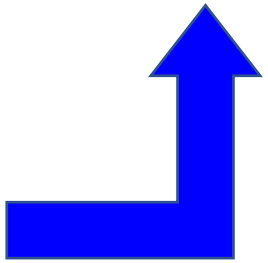




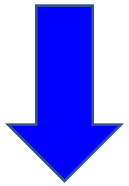
Protected BTC-e IP Addresses



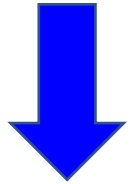
Legal Process served



BTC-e hosted on Server in Northern Virginia



Investigators covertly copied ('imaged') BTC-e's files



Logs showed 3 administrators (i.e. persons who managed the system)

BTC-e Admins

Posts written in Russian

Protected IPs

Bitcointalk Forum Admin used Username: "WME"

(Username linked to known carder)

Email account on wm-exchanger.com

Web Money Exchanger

Dispute with CryptXchange (Australia)

2012 Posted Lawyer's letter headed "Demand for the release of Alexander Vinnik's funds"

InZeit
Excellence in Acuity

WME
Jr. Member

Activity: 54

Re: Scam Report Against CryptoXchange $100k USD

July 18, 2012, 06:47:03 AM

#163

http://archive.is/6cFcY

DEUTSCH MILLER

53 MARTIN PLACE
SYDNEY NSW 2000

TEL: +61 2 9210 7777
FAX: +61 2 9210 7799
EMAIL: info@deutschmiller.com
WEB: www.deutschmiller.com

16 July 2012

Kenseycol Pty Ltd
T/as Crypto X Change
14 Sale Street
ORANGE NSW 2800

By post and email: support@cryptoxchange.com; legal@cryptoxchange.com

Responsible Partner: Zoe Hillman
Associate: Chris Stevens
Direct Tel: +61 2 9210 7771
Email: chris.stevens@deutschmiller.com
Our ref: 09268

Dear Sirs

Demand for the release of Alexander Vinnik's funds

We have still not had any response from you to our letters dated 11 April, 23 April and 4 May 2012.

InZeit
Excellence in Acuity

User WME = Alexander Vinnik

July 2017 Arrested in Thessaloniki

France, Russia, USA sought Extradition

2020 extradited to France

Vinnik's accounts monitored

Mid-2016 he logged into one of accounts using unmasked IP

IP of luxury hotel outside Russia

Hotel Chain HQ in USA

Subpoena for Passport

Sentenced to 5 years, deported to Greece 2022

5 August 2022 extradited to USA

Next hearing USA Feb 2024

InZeit Excellence in Acuity

Further Reading : "Tracers in the Dark" (2022) Andy Greenberg

Internet Protocol (IP) Addresses

Two types:

- **Static** (always the same)
- **Dynamic** (only lasts as long as connected)

Two versions:

IPv4

(4.3 billion - not enough numbers for everyone)

IPv6

What's yours? www.ipchicken.com

InZeit
Excellence in Acuity

Every website (every connection to Internet) has an associated IP address:

www.era.int

IPv4:

195.243.153.54

IPv6:

0:0:0:0:0:ffff:c3f3:9936

IP Address:

- Geo-specific
- Identifies:
  - ❖ The country
  - ❖ The ISP

ISP holds records of usage

Be careful what you ask for …

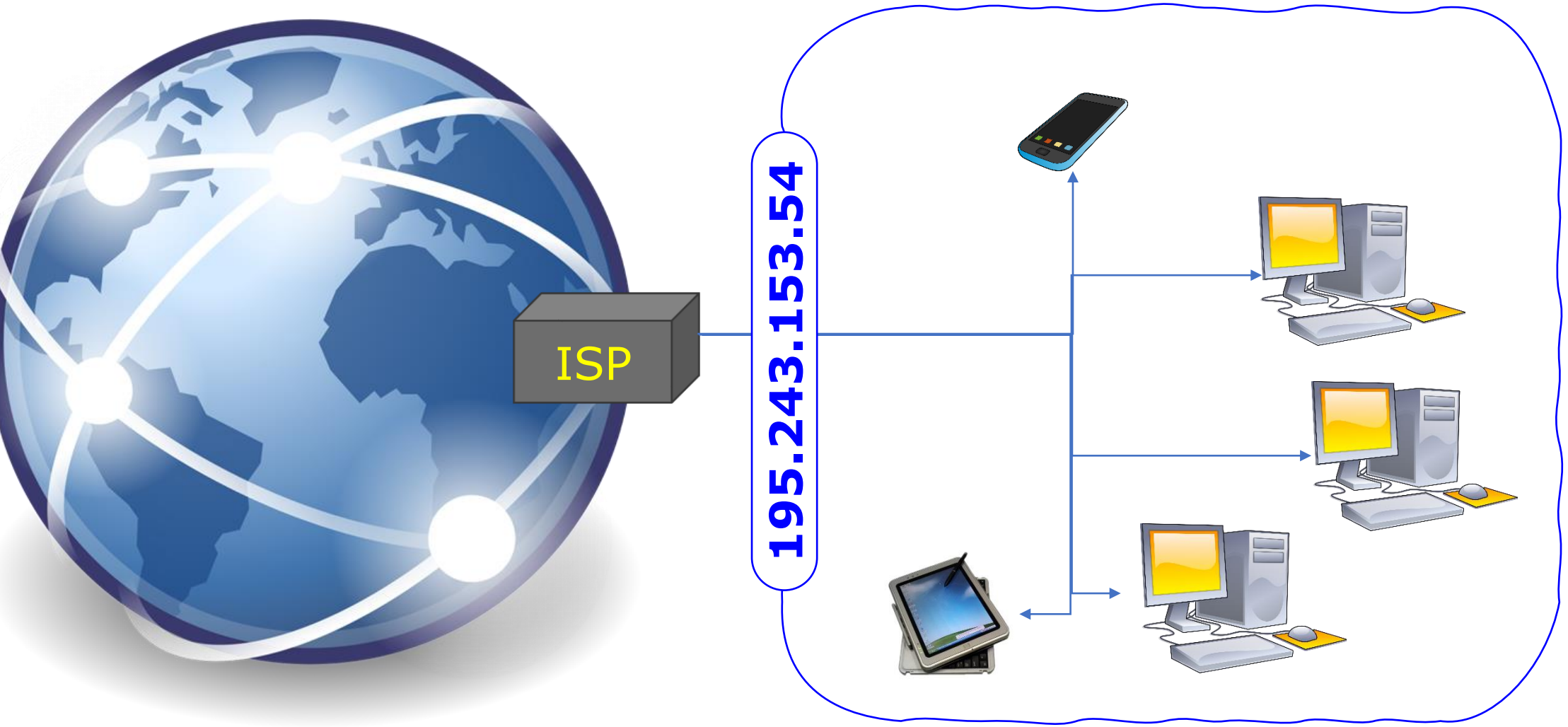
IP Address:
Needs to be carefully recorded
Time stamped to the second

Dynamic IP Addresses

Time Zones (UTC)

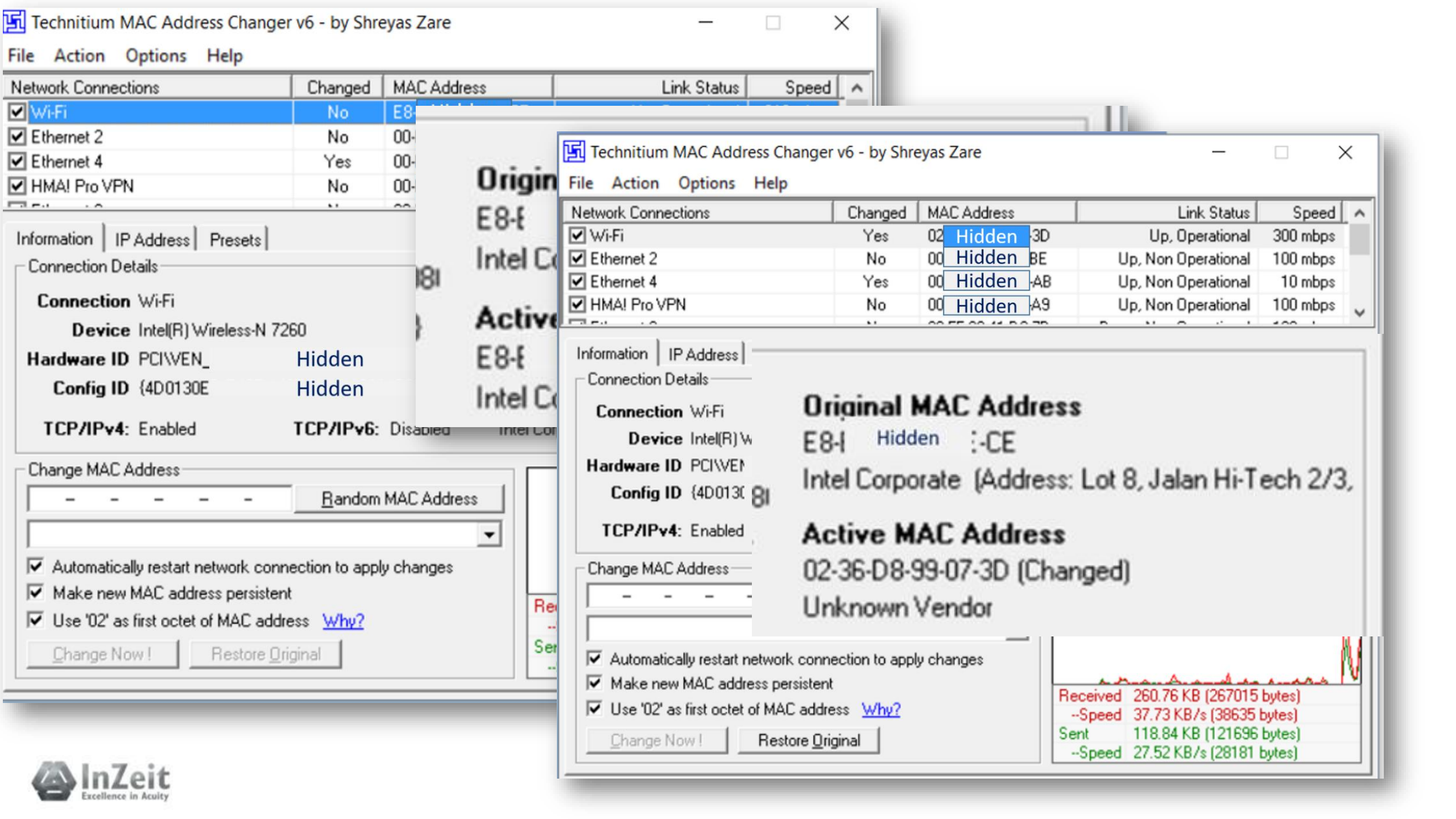
Date conventions: (dd/mm/yyyy) (mm/dd/yyyy)

MAC Address:
(Media Access Control or Physical Address)



MAC Address:
(Media Access Control or Physical Address)

- Identifies the device on the network
- Built into the device by manufacturer
- (normally) not broadcast beyond network
- But can ‘leak’ (e.g. some IPv6 versions)



InZeit
Excellence in Acuity

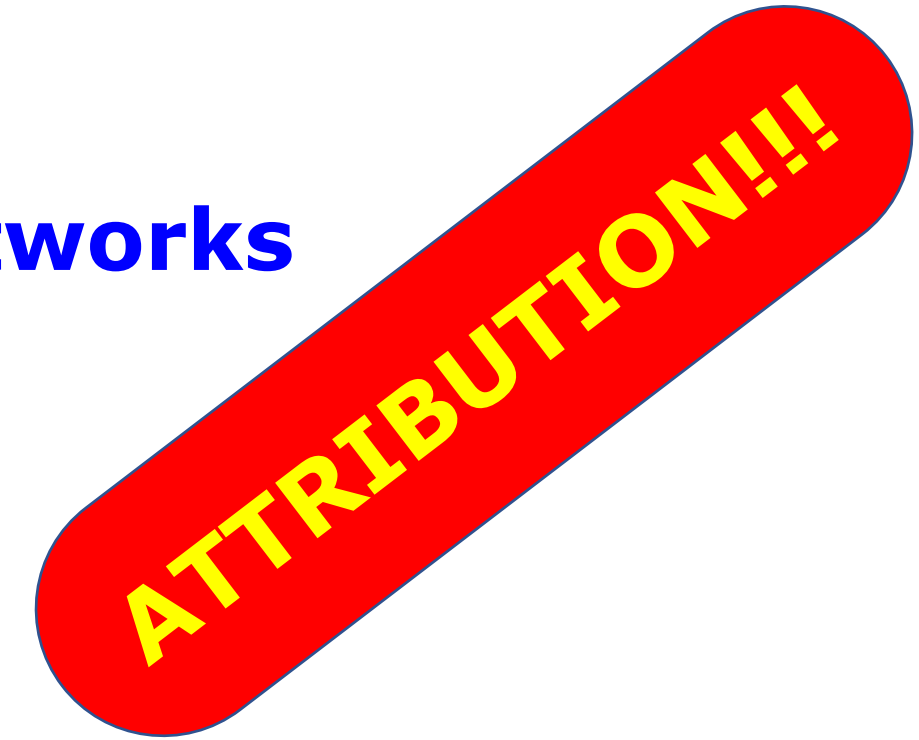
Phones - IMEI

International Mobile Equipment Identity

- Also MEID (Mobile Equipment Identifier)
- Hardcoded into mobile device by manufacturer (make and model can be traced)
- Identifies the device to the Cell Network
- Get IMEI Number key in: *#06#

Hiding an IP

- Public Access Points
- Piggybacking
- Compromised devices
- Proxy servers
- Virtual Private Networks
- Anonymisers
- Carriergrade NAT

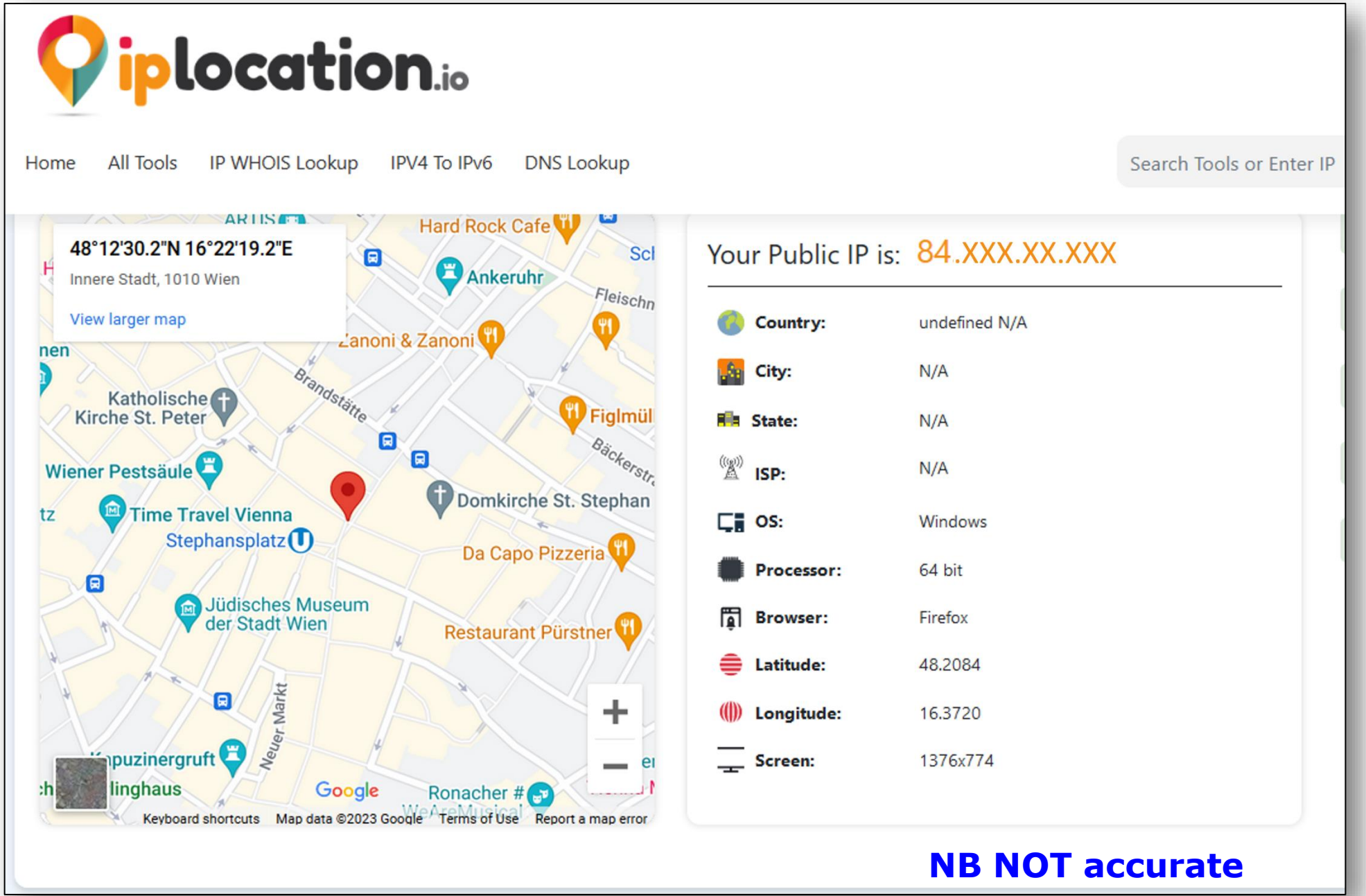


4 March 2015, California

- Home burgled
- 65-inch Smart TV (with Netflix) stolen
- Victim realised someone using her Netflix account

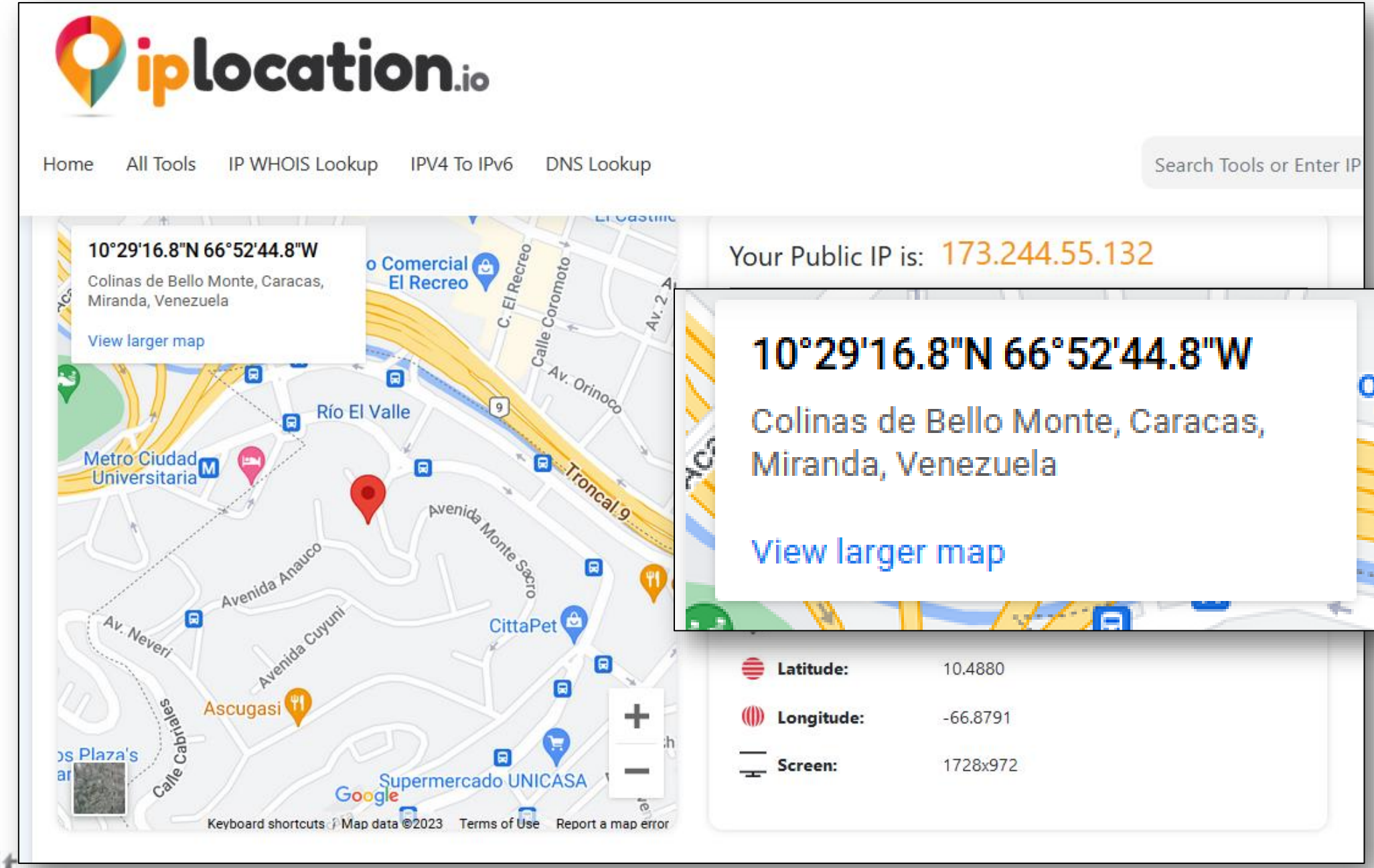
Bobby Alexander

- Police obtained IP address
- Raided the given address
- Came up with nothing
- Owners explained neighbour used their wifi account



NB NOT accurate

InZeit
Excellence in Acuity



Virtual Private Networks (VPNs)

VPNs enable access to the Internet through a remote computer/server using encrypted communication channel/tunnel

VPNs can be used by criminals to hide their location

VPN Providers often cooperate with legal process … some don't!

China	Banned (unless licenced)
Turkey	Banned
Iraq	Banned
Russia	Banned
Belarus	Banned
North Korea	Banned
Turkmenistan	Banned
UAE	Only approved VPNs
Iran	Only approved VPNs
Oman	Not for personal use
India	Data reporting requirement
Myanmar	Only approved VPNs
Pakistan	Only if user registers

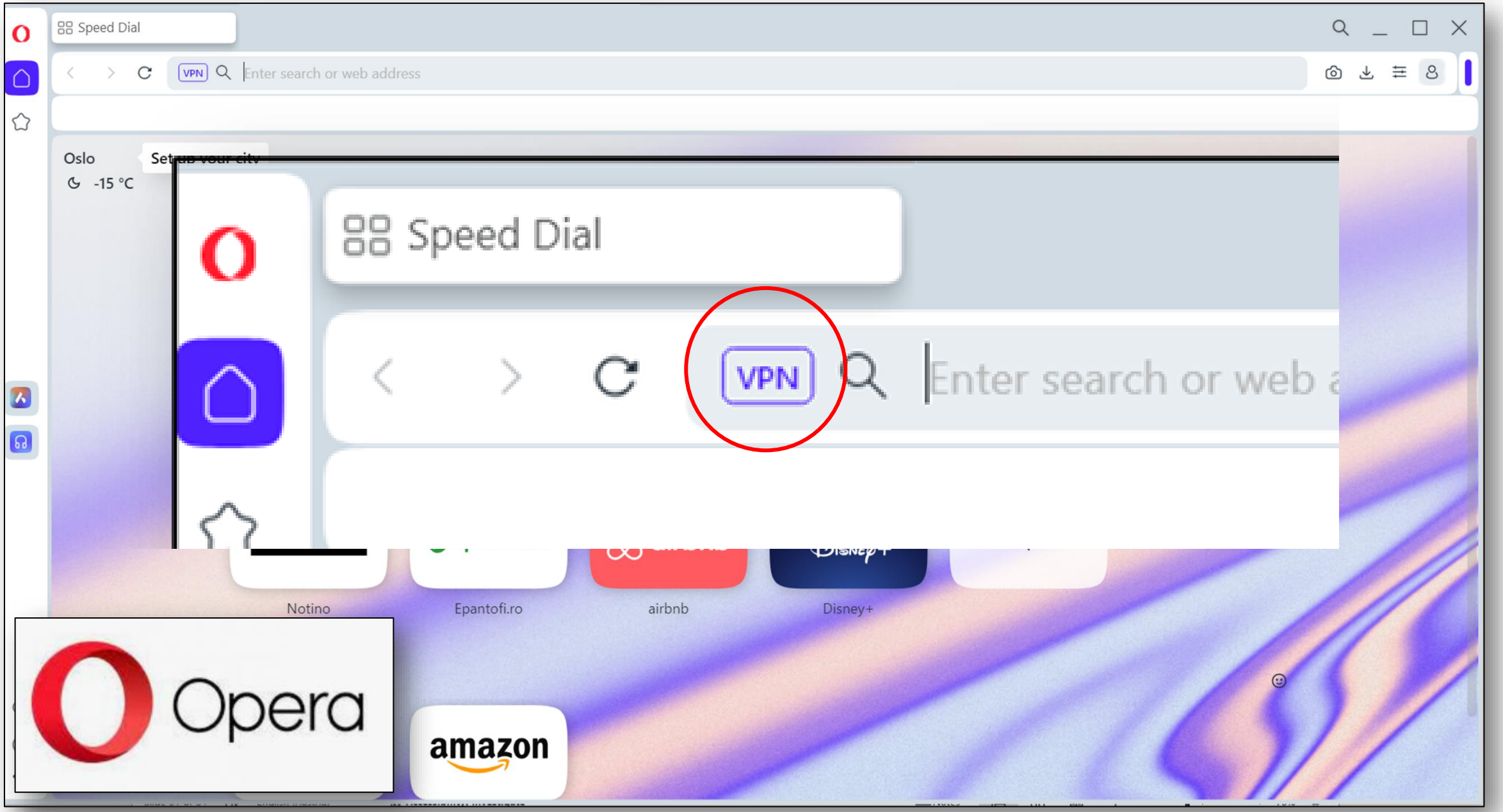
N.B. VPNs are controlled in some countries
(check local law before use)

https://www.comparitech.com/vpn/where-are-vpns-legal-banned/

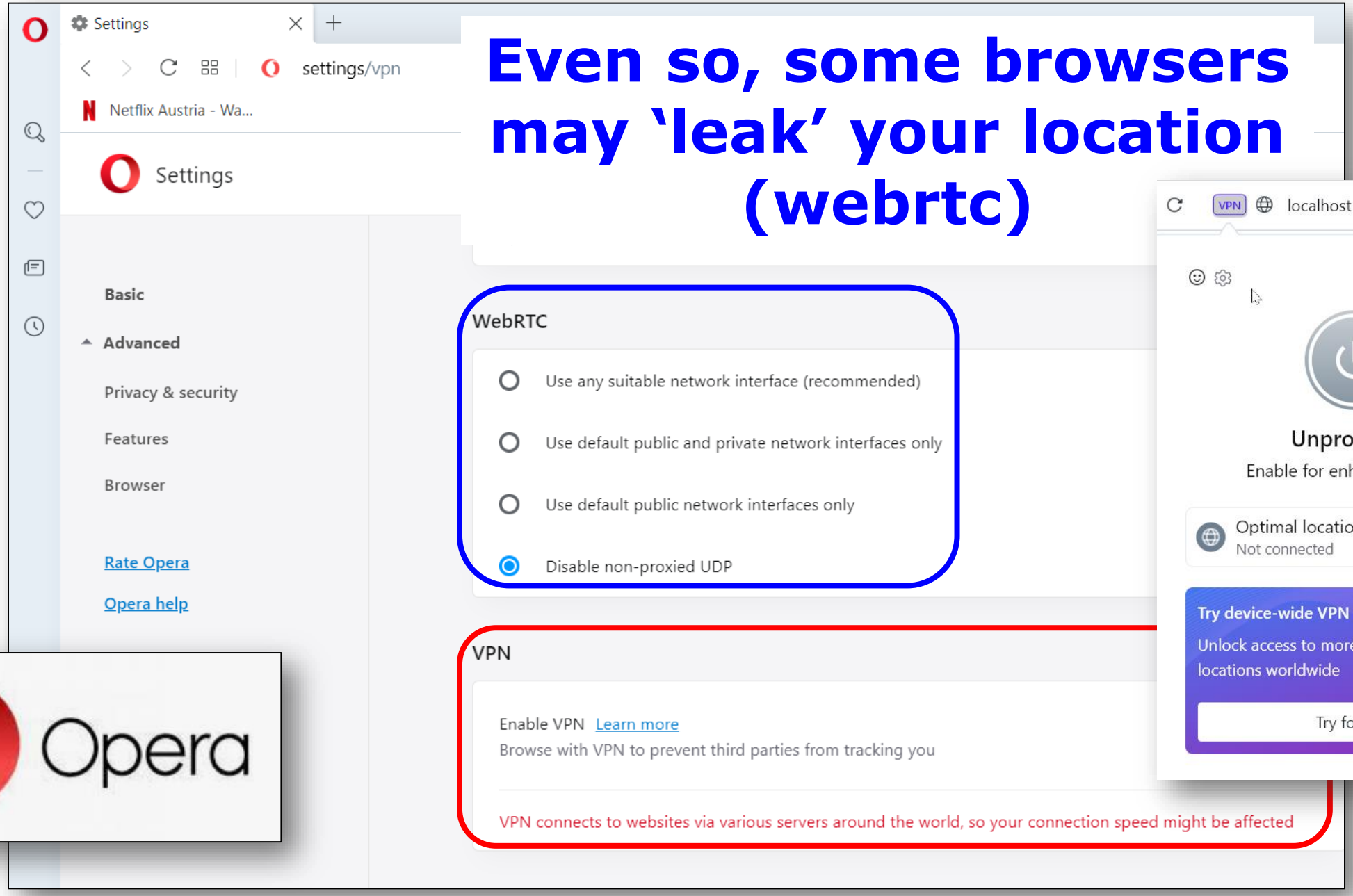
Well known VPN providers:

ExpressVPN
NordVPN
Hidemyass
CyberGhost VPN
Proton VPN

Also included in some anti-virus/internet security packages
And some browsers



Even so, some browsers may 'leak' your location (webrtc)



Opera

InZeit Excellence in Acuity

Settings/Advanced/Privacy & security/

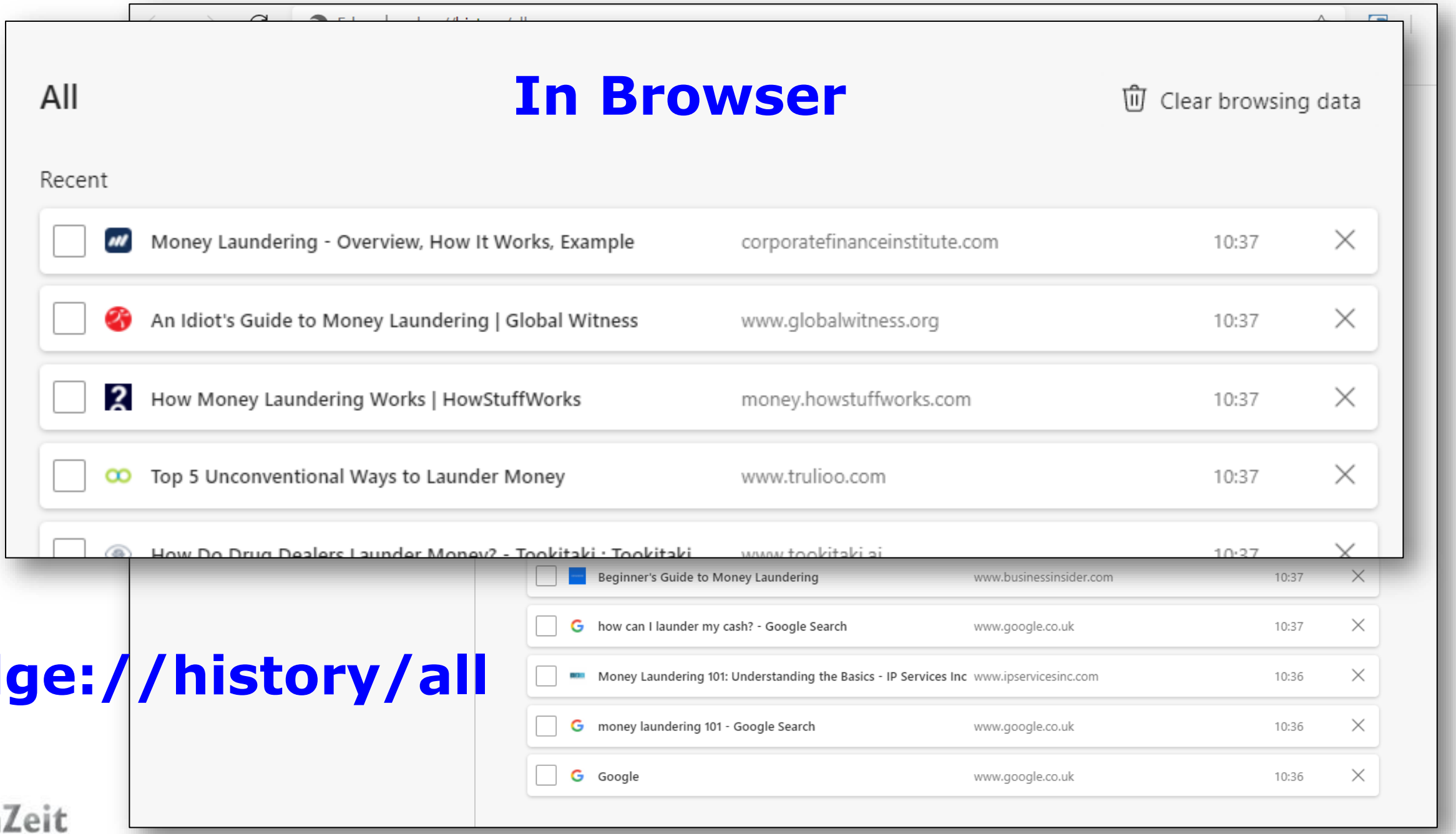
All you need is logs

… the automatically produced and time-stamped documentation of events relevant to a particular system

(source:www.techtarget.com)

LOGS

- Originally created for tracing bugs & improving performance
- Billing/maintenance records
- Generated automatically
- On the device
- On servers in the network
- Service providers
- Record meta-, traffic-data



edge://history/all

InZeit
Excellence in Acuity

edge://settings/siteData

InZeit Excellence in Acuity

Logs

A log, in a computing context, is the automatically produced and time-stamped documentation of events relevant to a particular system.

https://www.techtarget.com/whatis/definition/log-log-file

Server Logs

(Reminder: Server is a computer that provides services to other computers)

Can show:

Source and Destination IP Address
Date and Time of connection
User login details
What was accessed
Uploading/Downloading
Operating system on connecting device
What kind of browser used (and in what language)

Mohammed Ammer Ali –Computer Programmer
Father of two, Bolton, UK
2015 ordered enough ricin on Dark Web to kill 700 - 1,400 people

Username weirdos 0000

500 mg for 2.1849 BTC
(then = GBP320 those were the days!!!!!)

Encrypted chats discussed with seller:

- **the price of a lethal dose,**
- **discounts for bulk orders and repeat purchases**
- **ricin's shelf life**

Asked: "How do I test this ricin?"
Reply:"You must test it on a rodent."

Investigators found on Ali's Computer notepad:
To do "paid ricin guy" and "get pet to murder"

Searches for chinchillas, animal rescue centres, rabbits and "pocket-sized pets"

Google searches:

"abrin v ricin"
"home made cyanide and ricin"
"hydrogen peroxide"

On LG Nexus smartphone searched Yahoo for:

"what poison kills you quick, is foolproof, easily found/made, easily concealed and hard to detect post mortem"

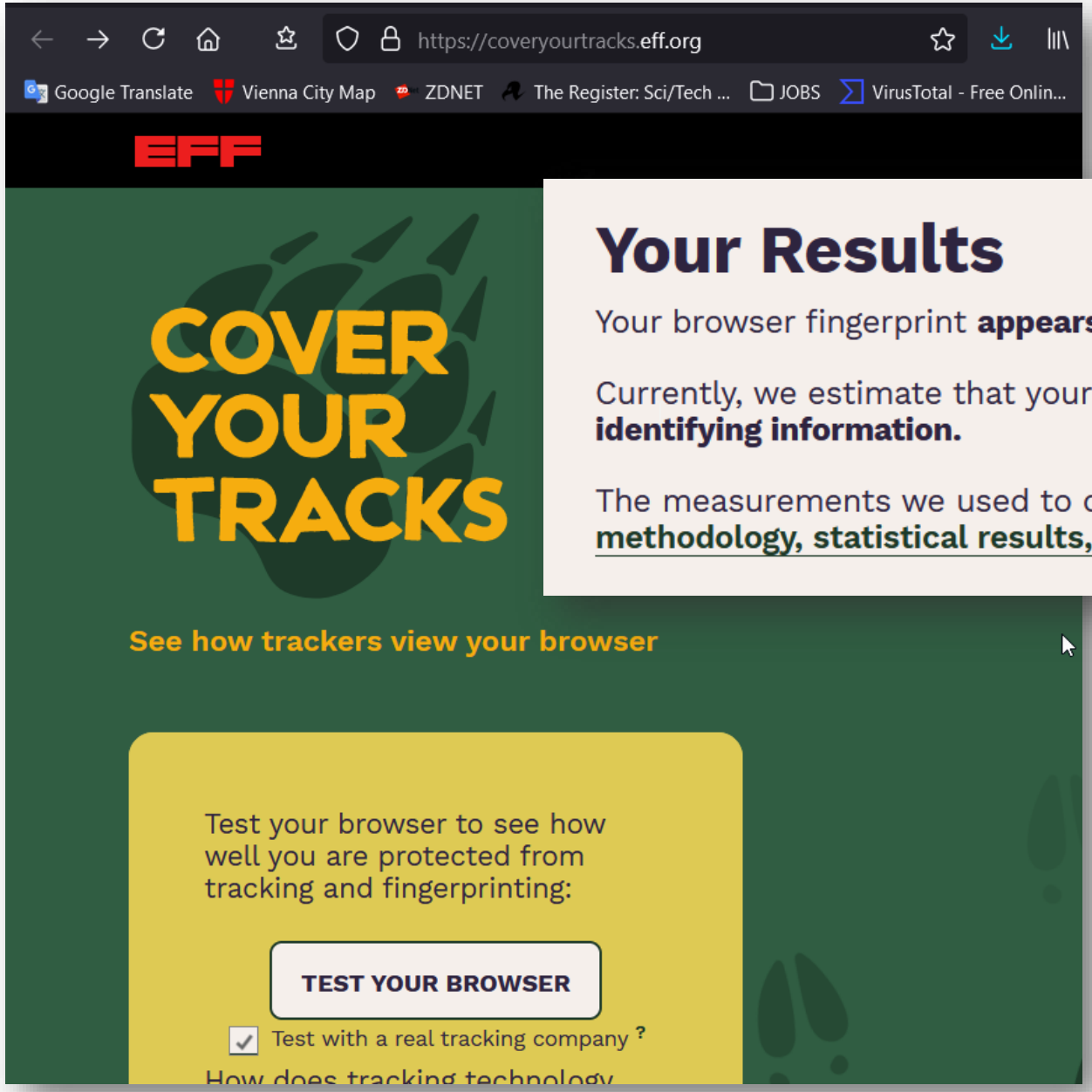
InZeit
Excellence in Acuity

https://www.theguardian.com/uk-news/2015/sep/18/breaking-bad-fan-jailed-over-ricin-plot
https://www.bbc.com/news/uk-england-merseyside-36483593

Cookies, search history and device configuration create a characteristic ‘browser fingerprint’

Try this out:

https://webkay.robinlinus.com/



Your Results

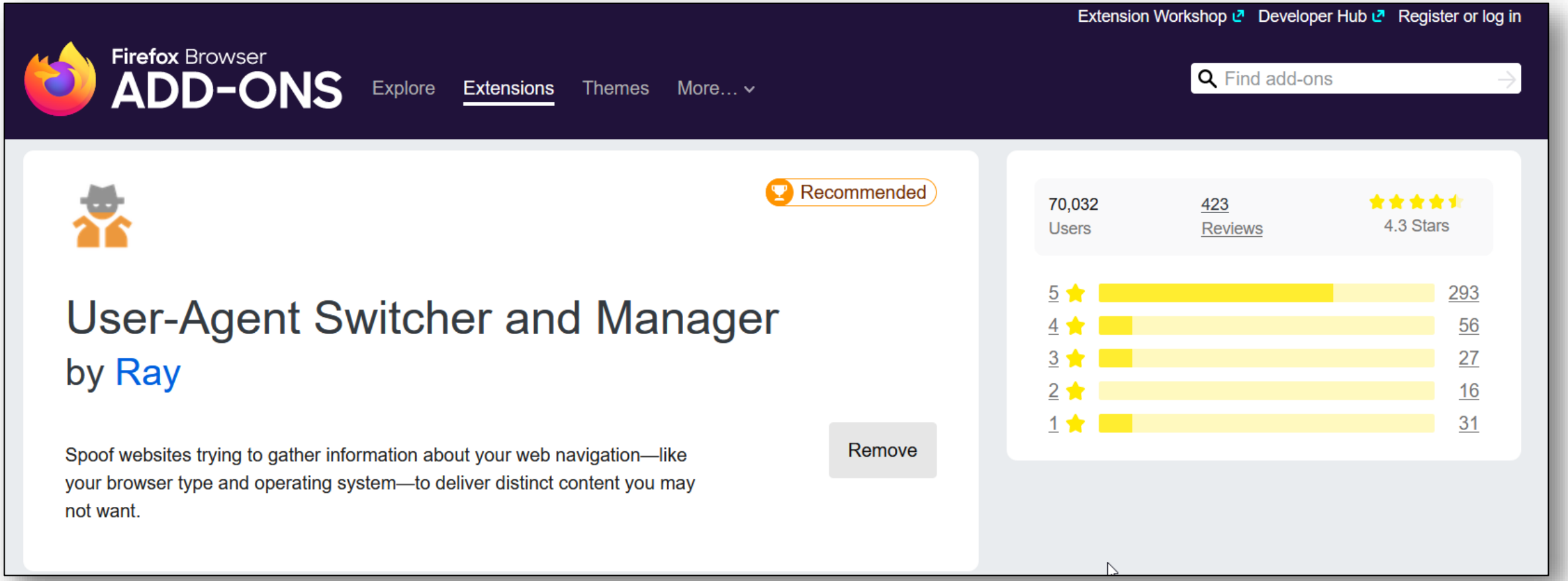
Your browser fingerprint **appears to be unique** among the 250,064 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.93 bits of identifying information.**

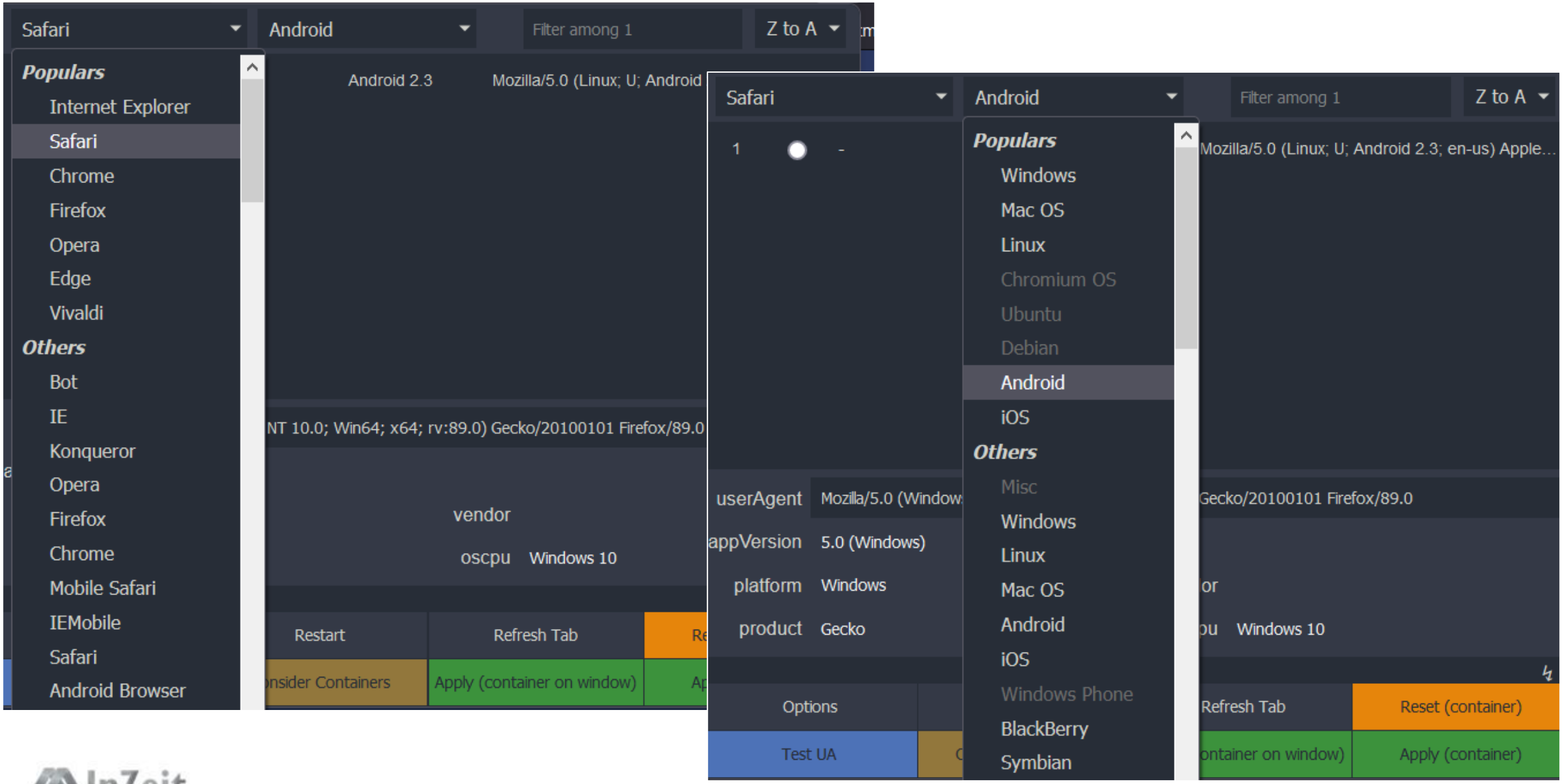
The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

Browser Fingerprinting
https://coveryourtracks.eff.org/

Browser fingerprint can also be faked:



Browser fingerprint can also be faked:

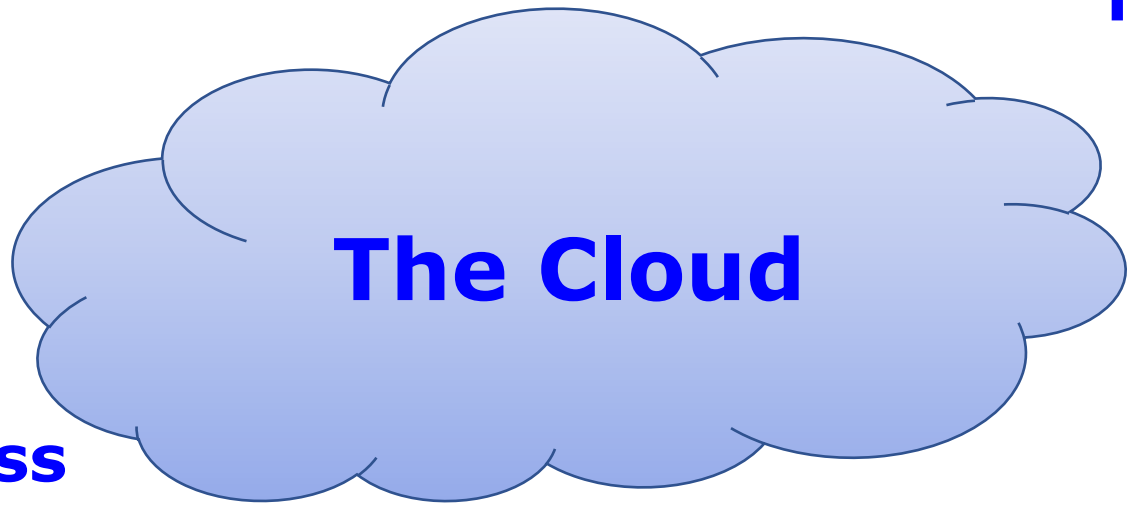


InZeit
Excellence in Acuity

Your data stored & processed somewhere else

gmail, outlook, yahoo mail, yandex mail , icloud, facebook

Your data may be spread across servers in multiple jurisdictions



Outsourcing: Iaas, Paas, Saas

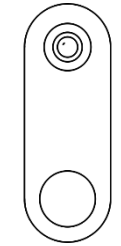
Relocated for business reasons (like load or electricity prices)

Even Cloud provider may not know where it is

Problems getting evidence:

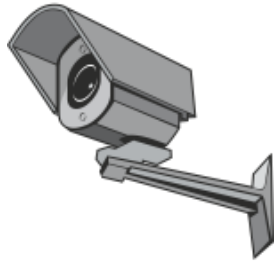
- No control
- One of 1000s of requests
- Have to trust the provider's standards
- Slow

InZeit
Excellence in Acuity



IOT

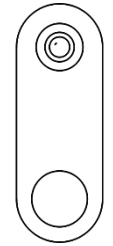
Estimated 22 billion - 50 billion devices



All connected

All generating & logging data

InZeit
Excellence in Acuity



IOT

How secure are they?

Default passwords

Most lack effective security

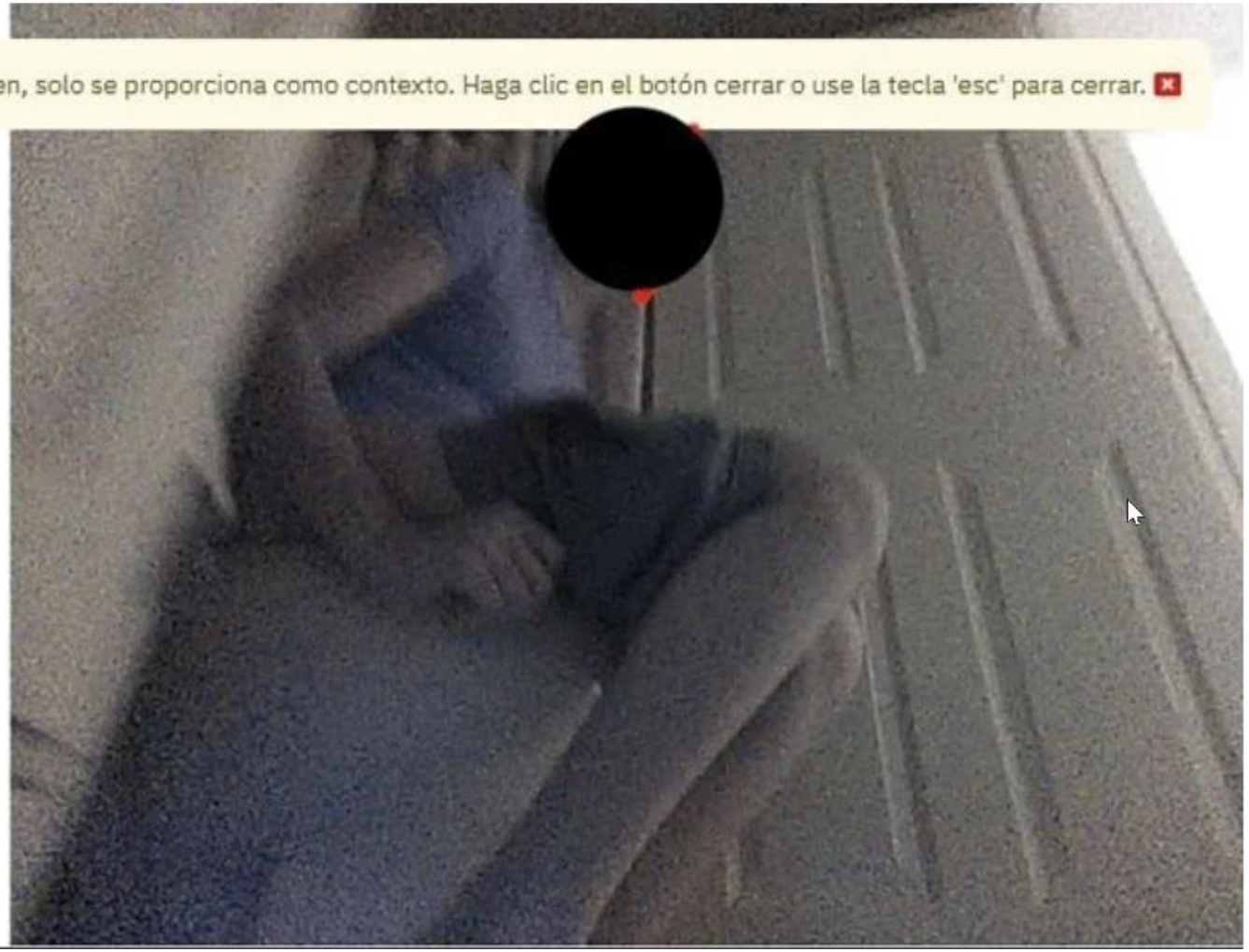
https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/

InZeit
Excellence in Acuity

Posted to Facebook

iRobot's Roomba J7 series robot vacuum

"special development robots with hardware and software modifications that are not and never were present on iRobot consumer products for purchase"



https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

InZeit
Excellence in Acuity

Posted

iRobot'
series

"specia
robots w
software
are not
prese
consum
p

Reuters 6 April 2023

Special Report: Tesla workers shared sensitive images recorded by customer cars

Naked man approaching car
Child knocked off bike
Doing laundry
'Really intimate things'
'certain sexual wellness items'
People walking by

(Banned in some places in China!)

https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

https://www.techn
l-intelligence-training-data-privacy/

InZeit
Excellence in Acuity

No central control

All websites end with .onion

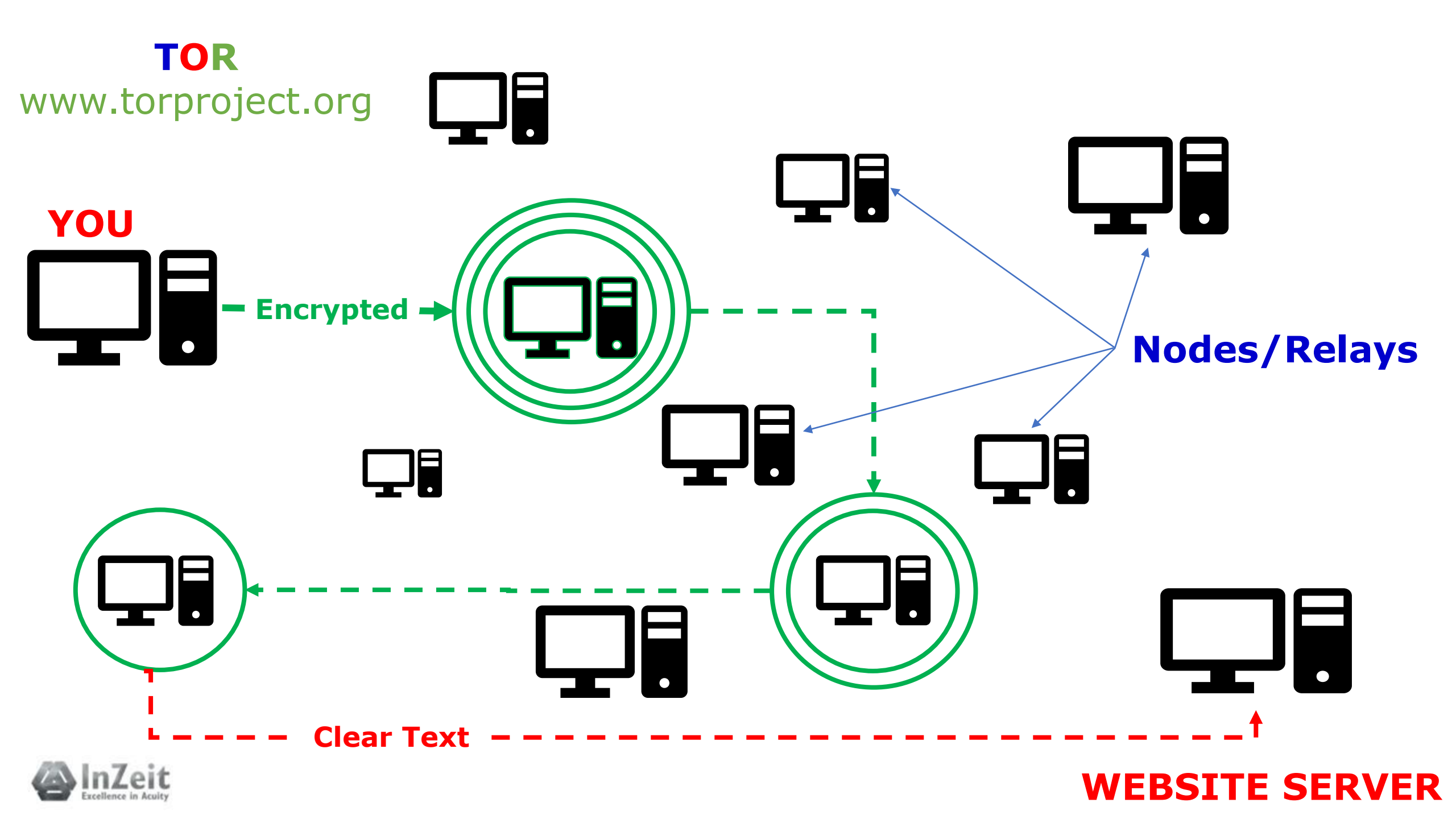
Can be used to access DarkNet

TOR
The Onion Router

Peer to Peer Network (people volunteer part of their hard drive)

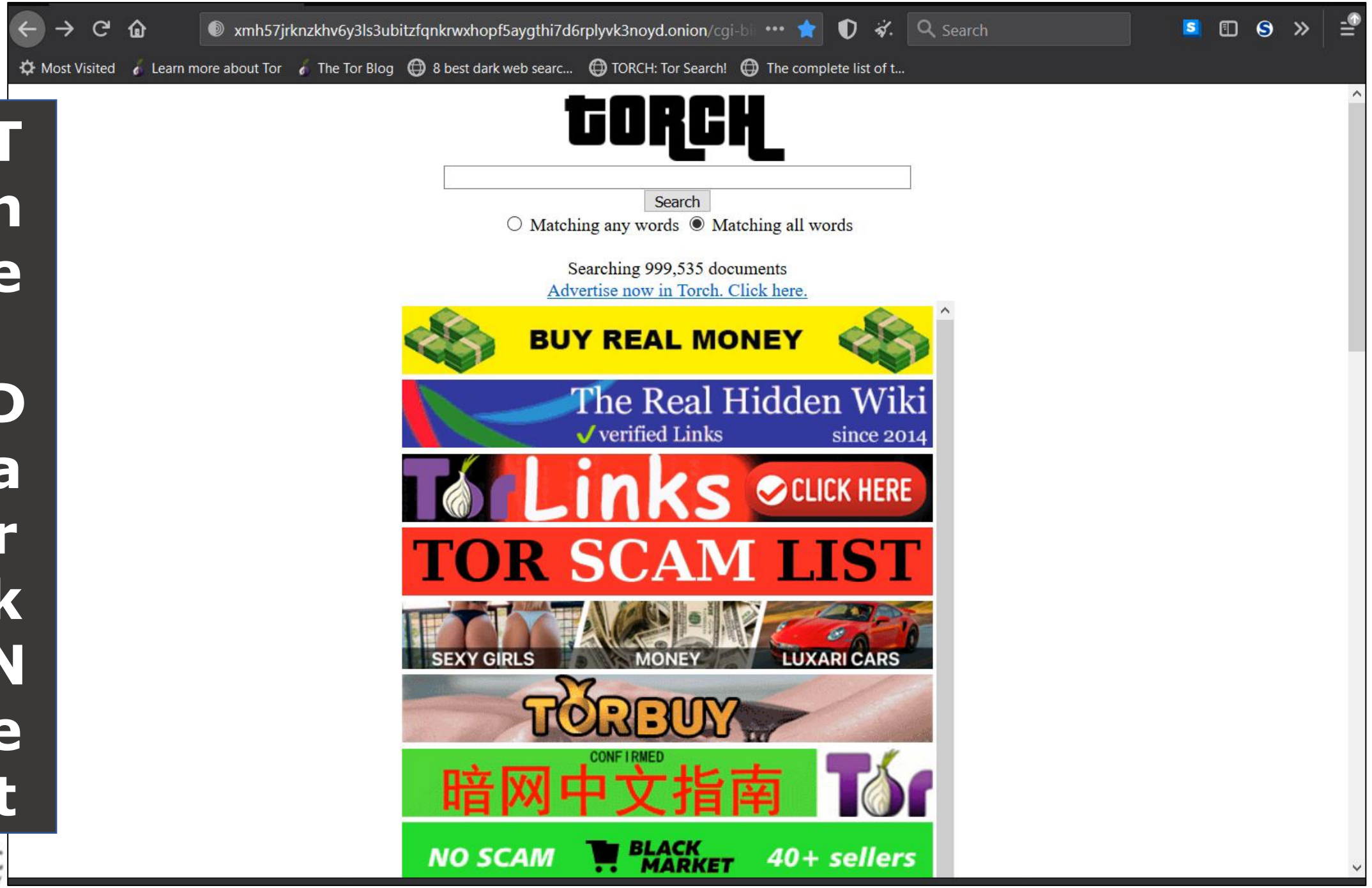
'Anonymising technology' (there are others)

InZeit
Excellence in Acuity

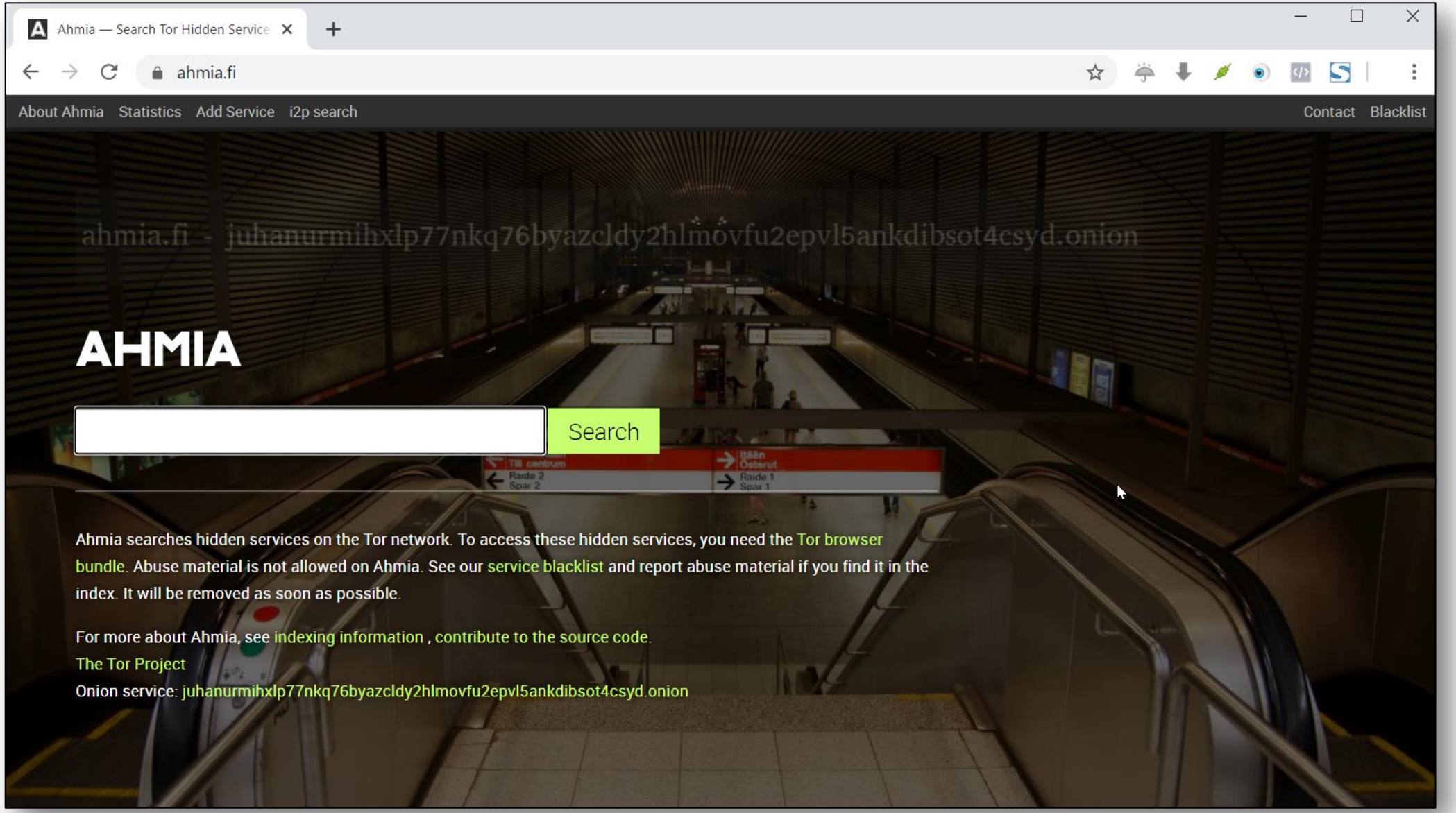

TOR
www.torproject.org
YOU
Encrypted
Nodes/Relays
Clear Text
WEBSITE SERVER
InZeit
Excellence in Acuity

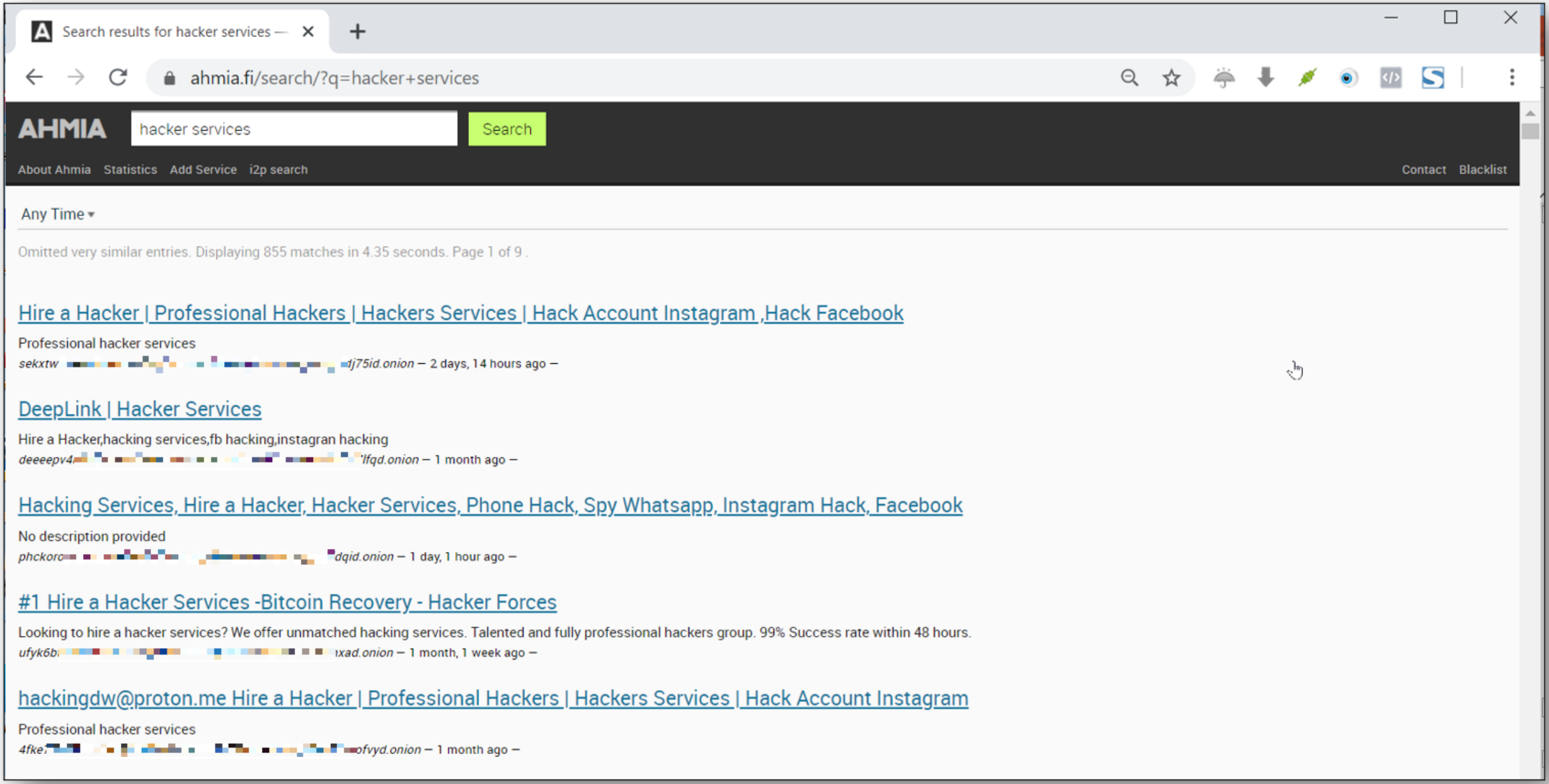
TOR

The DarkNet



InZeit
Excellence in Acuity





sekxtw7wkv67omxsltfwgisrnoovdjdu

sekxtw7wkv[redacted]hhgc7dj75id.onion

Tor

VPN

Google Translate

Neeva - Ad-free, priv...

Other bookmarks

sekxtw7wkv[redacted]vhhgc7dj75id.onion is blocked

This page has been blocked by Brave

ERR_BLOCKED_BY_CLIENT

Reload

Brave

Web browser

Hire a Hacker | Professional Hackers

sekxtw7wkv67 [redacted] hgc7dj75id.onion

Tor

Google Translate Neeva - Ad-free, priv

Other bookmarks

Use a VPN

HIRE A HACKER

Meet some of our Hackers services

WHATSAPP HACKING SERVICE

Do you want to know everything your husband, wife, children do on WhatsAPP and you don't have access to the device, just the cell phone number? See how we do it and

HACKING CELL

Need to monitor an Android phone or Iphone? See how to hire this cell phone monitoring service with android system and iphone system in a few minutes.

HACKING INSTAGRAM

Hire a Hacker for Instagram see how it works to hire a Hacker for Instagram, what it takes to hire and how Hacker for Instagram works answer all your questions.


Bad Idea!
tor2web.org
Tor2web: Browse the Tor Onion Services
What's Tor2web
Tor is a software project that lets you anonymously browse the Internet. Tor2web is a project to let Internet users access Tor Onion Services without using Tor Browser.
Getting started
Whenever you see a URL like http://duskgytldkxiuqc6.onion/, that's a Tor Onion service. Just replace .onion with .onion.to or .onion.city or .onion.cab or .onion.direct or any other domain made available by volounteers Tor2web operators Example:
https://duskgytldkxiuqc6.onion.to/
Make http:// .....Add .ly
This connects you with Tor2web, which then talks to the onion service via Tor and relays the response back to you.
WARNING: Tor2web only protects publishers, not readers. As a reader installing Tor Browser will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.

Bad Idea!

ahmia.fi/search/?q=whistleblower

AHMIA

whistleblower

Search

About Ahmia Statistics Add

Any Time

Omitted very similar entries.

Log in | Whistleblow

No description provided

kogbxf4ysay2qzozmg7ar45ijqm

Share and accept do

SecureDrop is an open-sourc

from anonymous sources. It

sdolvtfhatvsysc6l34d65ymdwx

20130401 Whistlebl

Für Freiheitsrechte, gegen Ma

a6pdp5vmmw4zm5tifrc3qo2pyz

Not secure | sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion.ly

List of SecureDrops Overview News Contribute D

White cube with keyhole (Securedrop logo)

SECUREDROP

Share and accept documents securely.

SecureDrop is an open source whistleblower submission system that media organizations and NGOs can install to securely accept documents from anonymous sources. SecureDrop is available in **21 languages**.

Get SecureDrop at your organization >

InZeit Excellence in Acuity

Bad Idea!

ahmia.fi/search/?q=passport

AHMIA

passport

Search

About Ahmia

Any Time

Omitted very s

EzPass - I

buy real passp

7a

Buy UK Pa

Buy UK Passp

gdct2ac

Not secure | gdct2ac6gse24s ebnthyd onion.ly

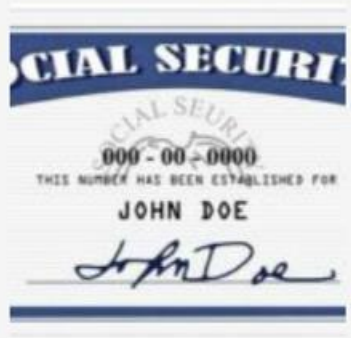
General Documents Center

Buy Documents Online, Passport, Driver's License, ID Card, SSN, Diplomat, Degree, Resident Permit

General Documents Center Blog Contact Us

About Us

Welcome To General Documents Center



Buy Passports online

InZeit
Excellence in Acuity

Summary

WWW = just another Internet Service

Identifiers:

URLs, Domain Names & WHOIS

IP Addresses (IPv4, IPv6, Dynamic, Static)

MAC Addresses (IMEI)

Can be blocked, masked or spoofed

Wayback Internet Archive

VPNs

Logs

Browser Fingerprints (history, cookies)

Cloud

Darknet & IoT

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

Inter ternot

Resources and further reading

Definition
https://www.britannica.com/technology/Internet
https://www.britannica.com/topic/World-Wide-Web

Data Estimation
https://www.statista.com/statistics/617136/digital-population-worldwide/
https://www.worldwidewebsize.com/
https://www.the-next-tech.com/blockchain-technology/how-much-data-is-produced-every-day-2019/

Protocols
Gross,M. (updated) 12 common network protocols and their functions explained
https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained

Wayback Machine (for old website versions)
http://web.archive.org

Find your IP address
www.ipchicken.com
http://www.privateinternetaccess.com/pages/whats-my-ip

Bitcoin Transactions
Greenberg, A. (2022) *Tracers in the Dark*, Doubleday Publishing

Vinnik Case Study
Identifying Post On Bitcointalk Forum http://archive.is/6cFcY

Changes in cybercrime trends during Pandemic:
https://rm.coe.int/presentation-fernando-miro-llinares-the-impact-of-covid-19-on-cybercri/1680a1e42f
https://aag-it.com/the-latest-cyber-crime-statistics/
https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/

UK Information Commissioner's Report 2016
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/670219/IOCCO_annual_report_2016_2.PDF p74

Technicum MAC Address Changer
https://technitium.com/tmac/

VPN bans
O'Driscoll,A. (2022) *Where are VPNs legal and where are they banned?*
https://www.comparitech.com/vpn/where-are-vpns-legal-banned/

WebRTC leaks
Vigderman,A. Turner,G. (2021) *WebRTC Leaks: A Complete Guide* https://www.security.org/vpn/webrtc-leak/

Your Browser Logs
(Enter in address bar of browser)

Google Chrome:

chrome://history/
(try this software utility:
https://www.nirsoft.net/utils/chrome_cache_view.html)

Microsoft Edge:

edge://history/all
edge://settings/siteData

Mozilla Firefox:

about:cache
about:cache?storage=memory

Ricin Dark Net case

Press Association (2015) *Breaking Bad fan jailed for trying to buy ricin* https://www.theguardian.com/uk-news/2015/sep/18/breaking-bad-fan-jailed-over-ricin-plot
BBC (2016) *Mohammed Ali: Breaking Bad ricin plotter's appeal turned down* https://www.bbc.com/news/uk-england-merseyside-36483593

Browser Fingerprinting

https://webkay.robinlinus.com/
https://coveryourtracks.eff.org/

Data Brokers

https://www.databroker.global/community/people

Rafter,D. (2021) *How data brokers find and sell your personal info* https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html

Internet of Things

Palmer,D. (2021) *Your insecure Internet of Things devices are putting everyone at risk of attack*
https://www.zdnet.com/article/your-insecure-internet-of-things-devices-are-putting-everyone-at-risk-of-attack/

Guo,E. (2022*) A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?*
https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/

Stecklow, S. Cunningham, W. Jin, H. (2023) *Special Report: Tesla workers shared sensitive images recorded by customer cars*
https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/

Meta-Search Engines

- Dogpile.com
- Metacrawler.com
- Wolframalpha.com
- Metager.com
- Ahmia.fi (also for .onion sites)

At your own risk:

- Torproject.prg

PROSEARCH

Open-source tools, computer forensics on mobile devices and in the Cloud

Encryption, privacy and the acquisition of mobile and cloud data

Damir Kahvedžić, PhD.

Co-funded by the European Union

Who am I?

Damir Kahvedžić

Senior Global Data Services Manager | ProSearch

Table of Contents

Topic

Story Time

Boris Johnson's Phone

Covid Response Inquiry

Examining the UK's response to and impact of the Covid-19 pandemic

The Inquiry asked for diaries, notebooks and WhatsApp messages by Johnson.

Messages from one mobile were given

An older phone was also found but it was locked and the password was unknown

Boris Johnson's Phone

What's the problem?

Mobiles are often locked and without a password

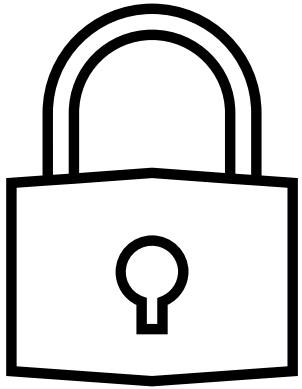
Why can't we access this device and hack into it.

Encryption

- What is it?
- Can we overcome and if not, what can we do?

Encryption

Encryption



Encryption

- The process of scrambling or hiding the true clear contents of a files.
- It converts something that is readable by humans to incomprehensible text and numbers.

Clear Text: a term given to unencrypted data

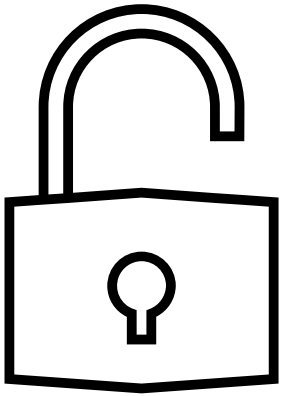
Cipher Text: a term given to the encrypted version of the data

Key: the unique value used by the algorithm to make the cipher text

Decryption

Encryption

- The process of descrambling the encrypted data from the Cipher Text to Clear text.
- Require the Key used at encryption time to authenticate and authorize you to access the data



Keys are made by providing

- Something you know (**password**)
- Something you are (**biometrics**)
- Something you have (**2FA**)

Example: Ceaser Cipher

Clear Text	Key	Cipher Text
Hi, how are you? I'm looking to talk to you about the PPI contract. Let me know when you are free to discuss. We need to get moving on it as soon as possible..	10	*Rs, ryg kbo iye? S'w vyyusxq dy dkvu dy iye klyed dro ZZS myxdbkmd. Vod wo uxyg grox iye kbo pboo dy nscmecc. Go xoon dy qod wyfsxq yx sd kc cyyx kc zyccslvo.*

All letters are shifted by a predetermined number of characters forward in the alphabet

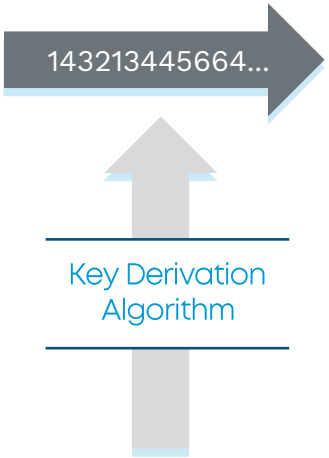
Shift the letters back to decrypt

Shifting mechanism = algorithm
Number of shifts = key

Simple to break, all you have to do is try **26** combinations. This is a **Brute Force** attack.

Example: AES 256 Cipher

Clear Text	Key	Cipher Text
Hi, how are you? I'm looking to talk to you about the PPI contract. Let me know when you are free to discuss. We need to get moving on it as soon as possible..	143213445664...	*QEP+G5dXvPqxP0TjNQI/UlWesiehHUnSnw7mgDCT/2oEMbox7rThr8Y1nWE9+LWFxM/FGHgMgXoEWVhBTTcKO1SeHYsGoSJ/uNYjspUQZO6Jgx9bWm67pqlrzRCi01WXJUWx+guhS2NlvaxmfY0BfeVt*



Newer algorithms use a much longer keys. Common ones are **AES**, **RSA**

Keys can be derived from easier to remember sources (PIN, biometrics, etc).

The number of possible combinations in an AES 256-bit key is **78** digits long.

To crack a single 256-bit key would take **trillions** of years

Attack

Attack

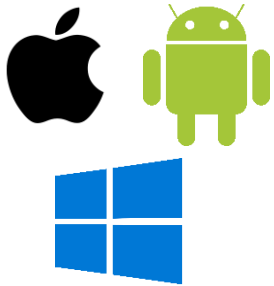
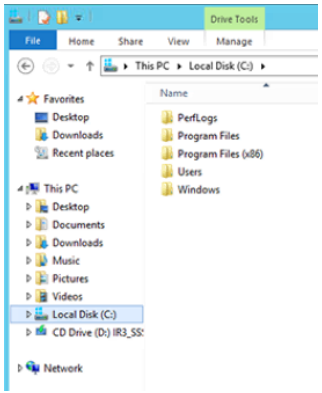
- Methods to decrypt data without authorization.
- Can vary from guessing the password to backward engineering the Cypher and deconstruct the way data was encrypted

Attacks include:

- **Brute Force Attack:** guess all possible passwords
- **Dictionary Attack:** guess passwords from a known list of passwords

As computing power gets bigger, the attacks get stronger.

Password vs Encryption

Key	Security Authorization	Device
Password		
PIN		
Biometric		
Pattern		

Password =/= Encryption

Passwords prevent access to resources

Authorisation made by the OS

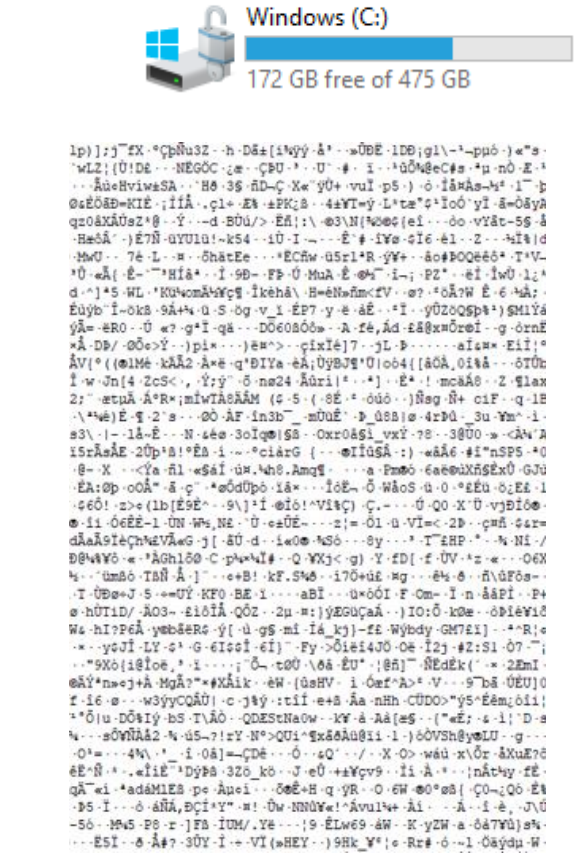
The resources may not have their text scrambled.

You are just prevented from accessing it by software. The data on the device is in clear text

Encryption Locations

Data can be encrypted at several locations during its lifetime. Different locations allows us to try different techniques and can give access to more or less information.

- **Operating System \ Hardware**
- **Application** Software running on the devices
- **Files** Individual file are encrypted by the application that made it.
- **Cloud** For backups and syncing
- Other **external** locations



Encryption Level - Disc

Full Disk Encryption is process of securing data at the hardware level by encrypting everything on a disk drive.

Data is encrypted and decrypted by the OS

Without the OS the data is not accessible

Examples include

- BitLocker on Windows Machines
- FileVault on Mac
- iOS 4 in 2011

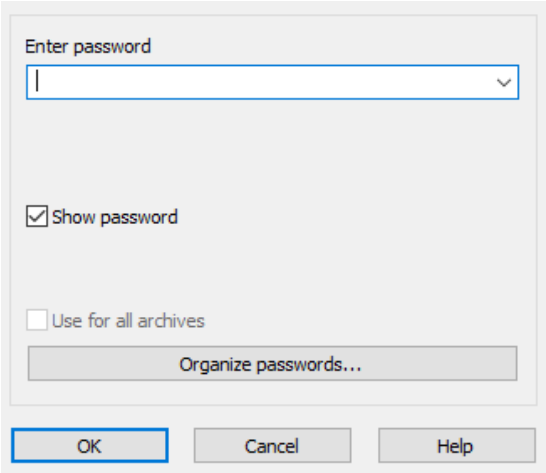
Encryption Level - Application

Application Specific Encryption

- Every application controls its own data and databases.
- Increasingly application encrypt the data while using it

- End to end encryption (E2EE): the data is encrypted on the sender device, in transit and at rest.

Encryption Level - File



Affects one file at a time

Most larger software suites allow passwords to lock a file

Password protection on essential documents limits access to who can read them and prevents unauthorized access.

Open to cracking and is probably the easiest to access of the three Encryption levels.

Encryption Attacks

Simple Attacks

Brute Force Attack: Basic attacks that try every combination of letters, number and characters including Upper and lower case.

Difficulty and time depend on the length of the password

- 10 digit passcode: 10,000,000,000 combinations. Cracked in 0.19 hrs
- 5 lower chars + 5 digits: 1,188,137,600,000 combinations. Cracked in 23.05hrs
- 5 lower chars, 5 upper chars, 5 digits: 14,116,709,565,337,600,000 combinations. Cracked in 11,412,508 days
- f16QL~!>5mX#9dgj”+2. Cracked in 22×1018 years. Age of universe is 13.8×109 years

The more complicated the password the longer it takes to crack

More successful attacks

Dictionary Attacks: Rather than guessing randomly. Generate a list of potential words and try them instead first. Dictionaries can be created using

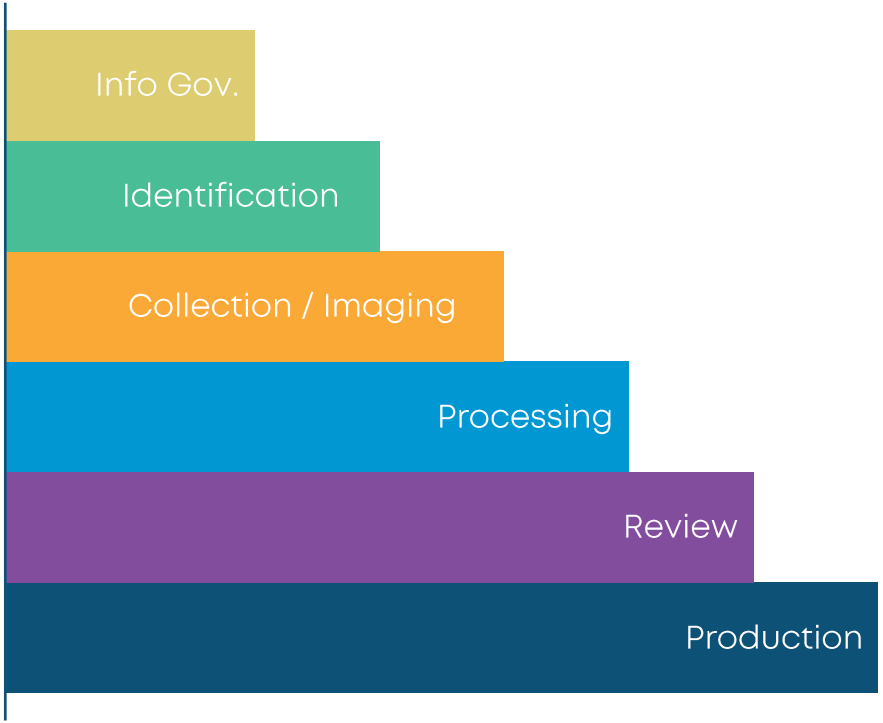
- previously known passwords
- known password databases
- list of all words found in any device belonging to a user. All words in any emails, hard drives or environment

Modifier Attack: modify each word in the dictionary with the likely substitute characters and try those words as well. For example:

- a get changed to @
- l gets changed to 1
- o changed to 0

Mobile Phones

Forensics \ eDiscovery Stages



Forensics and eDiscovery matters follow a well-established set of stages for almost all matters

The job of the digital forensics \ eDiscovery expert is to guide the legal practitioners in identifying, extracting and reviewing all necessary relevant information.

Encryption is a problem that makes this process more difficult in several stages.

Mobile Device

Rules

Data acquisitions from phones and tablets follow the same rules as any other device.

1. Be comprehensive
2. Minimise disruption
3. Note everything

However, they are much more difficult.
Collection depends on the OS, manufacturer, versions etc.

Dictated by the security and extent of encryption

Development of security features follows market forces

Mobile Device Acquisitions

Physically

Access the addressable storage space directly
Copy the data without the need for the OS
No OS security restrictions, no OS help
Increasingly not possible to due to physical and hardware restrictions

Pros:

- Collect all information regardless of where it sits and how
- Retrieve information that the OS does not know about or has forgotten
- Complete access allows us to ensure that nothing has changed

Cons:

- No help from the OS. We must understand the data ourselves, where it is stored, how and why
- NO HELP from the OS at all. Any encrypted volumes stay encrypted.
- NO HELP from the OS, so hardware and software security features need to be overcome

Mobile Device Acquisitions

Logically

Logical imaging is taking a copy of the data from the device with the help of the OS

Device is turned on and we use software to communicate with the OS and request data from it.

Pros:

- We work with the OS to gather the data.
- Communication protocols ensure we get a comprehensive data including apps, chats etc
- Easier to parse and understand.
- No encryption problems

Cons:

- OS only gives us what it knows about
- OS refuses to give any secure data
- Working with the OS is subject to the manufacturer's security. It may wipe the data if you try and fail too much.

Mobile Device Peripherals

Peripherals

Removable storage devices can be taken out of the phone and imaged separately

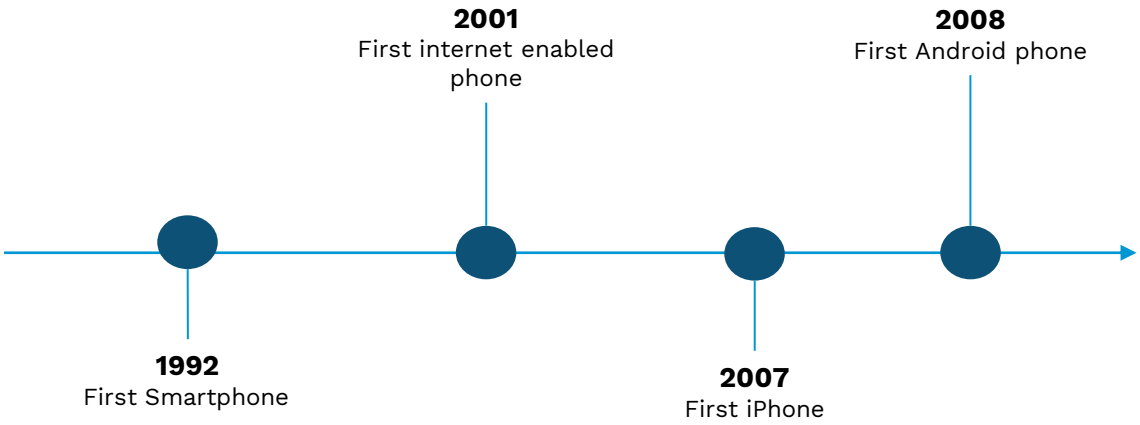
Some users may store their data on the SD Card.

You might get lucky, and the SD Card is not encrypted

Once removed from the device, manufacturer's security processes no longer applies

Free to hack into the SD Card

Smart Phone Development



Which acquisition method depends on the security features of the phone

Early editions did not have great security

No encryption.

Too demanding for the early OS

iPhone PIN was only 4 digits (if there were any)

Developments follows market forces and high-profile incidents

iPhone 4 Released

iPhone 4

- Released in 2010
- iOS devices have hardware encryption
- Uses AES-256, which is what banks use for transactions.
- The key is generated and stored on-device

San Bernardino 2015

San Bernardino Attack

Shooting in California left 14 people dead

One of the shooters left behind an iPhone 5C

Security meant that more than 10 tries on the phone would wipe the data

The US government wanted Apple to build a backdoor into the device so that they can access it

Apple worked with the US government up to a point. It did not want to develop any custom back doors

The aftermath of the case forced Apple to tighten security even further

Sutherland Springs 2017

Sutherland Springs (2017)

Shooter Devin Kelley killed 26 people in Texas

Left behind an iPhone SE

US Government subpoenaed Apple

Increased pressure for Apple to work with the authorities

Pensacola (2019-2020)

A gunman killed three people in Pensacola, Florida while in the possession of two iPhones.

Apple handed over all data they had associated with the devices, but the FBI wanted more

FBI reconstructed the phones and got into the phone without Apple's help.

Pegasus (2021)

The exploit jailbreaks an iPhone then installs malware tools to allow remote access to the device

Apple Developments Overview

Summary

- Apple has not developed a backdoor into the physical device
- It has recently developed end-to-end encrypted cloud data.
- It proposes the use of the iCloud

1. Get the phone to create a new iCloud backup
2. Apple will then be able to collect and decrypt it

In each of the previous cases the police made errors in handling the iPhone

This is in effect a Logical Acquisition. No deep forensic artefacts are preserved

Apple started educating law enforcement on what to do and how to handle devices.

The Cloud

iCloud Encryption

iCloud Details

- Released in 2011 to sync data between devices
- Used to store backups of the entire device
- Recently implemented the **Advanced Data Protection for iCloud.** Its an optional setting you must enable
- It creates an end-to-end encryption for 25 categories of data
- Keys are kept on trusted devices only
- Both iDevices must have ADP enabled for it to work
- If ADP is not used then the keys are stored by Apple and can be accessed

iCloud Encryption

Advanced Data Protection

iCloud Mail is not end to end encrypted because of the need to interoperate with the global email system

iCloud Backup:

- With ADP: the keys to your backups are secured in Apple data centers should you ever forget your password, PIN or lose your device
- Without ADP: iCloud Backup and everything inside it is end-to-end encrypted, including the Messages in iCloud encryption key

Some metadata about files is visible even with ADP. This is device information, list of apps, date and time of backups, when a file was created etc.

Category	Encryption	Key Stored By
iCloud Mail, Contacts Calendars	In transit & on server	Apple
iCloud Backup, iCloud Drive, Photos, Notes, Reminders, Bookmarks, Voice Memos, Wallet, Password, Health Data, Journal Data, Home Data, Messages, Maps...	End-to-end	Trusted devices

https://support.apple.com/en-us/102651

Other Locations

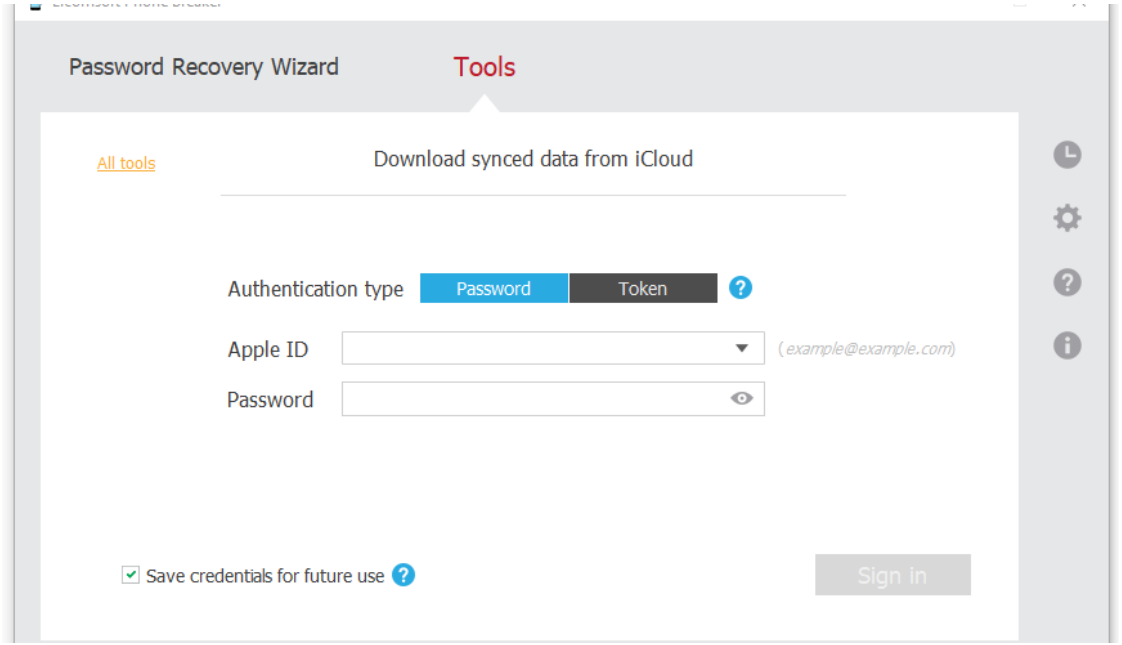
3rd Party Clouds

- You can choose to backup your data to other cloud providers
- **WhatsApp** defaults to Google Drive or iCloud
- Simply get a new phone and sync the data down

Local Backups

- You can still back up data locally to your Mac

ProSearch Way



Process

1. Coordinate with client to create a backup.
2. If privacy concerns are warranted a custom backup with specific information can be created.
3. Use Elcomsoft Phone Breaker to authenticate into their iCloud
4. Download the backup in iTunes format
5. The backup is an exact replica of the phone and can be further processed using normal forensic tools

Round up

Boris Johnson's Phone

What happened?

In the end the PIN was found on a piece of paper

Even if the PIN was not found it would have been a simple matter to get the backups

Or he could get a new phone and sync the old data do

Takeaways

Summary

- Mobile devices are getting harder to access
- Forensic tool are always a few steps behind encryption and newer security features. They will never be able to support all methods.
- However, mobile devices are never found in isolation.
- Look to the cloud for your data

PROSEARCH

Thank You

damir.Kahvedzic@prosearch.com

For more information visit www.prosearch.com

Handling electronic evidence in courts

Senior Public Prosecutor Chatrine Rudström

Co-funded by
the European Union

ÅKLAGARMYNDIGHETEN

Agenda

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

ÅKLAGARMYNDIGHETEN

About me

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

ÅKLAGARMYNDIGHETEN

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

- Eurojust, network of practitioners
- Established 2016
- Five observer states: Norway, Switzerland, Serbia, USA and Japan
- Plenary meetings, topical discussions
- Subgroups
- Training

Challenges

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

ÅKLAGARMYNDIGHETEN

ÅKLAGARMYNDIGHETEN

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

Jurisdiction

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

ÅKLAGARMYNDIGHETEN

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.”

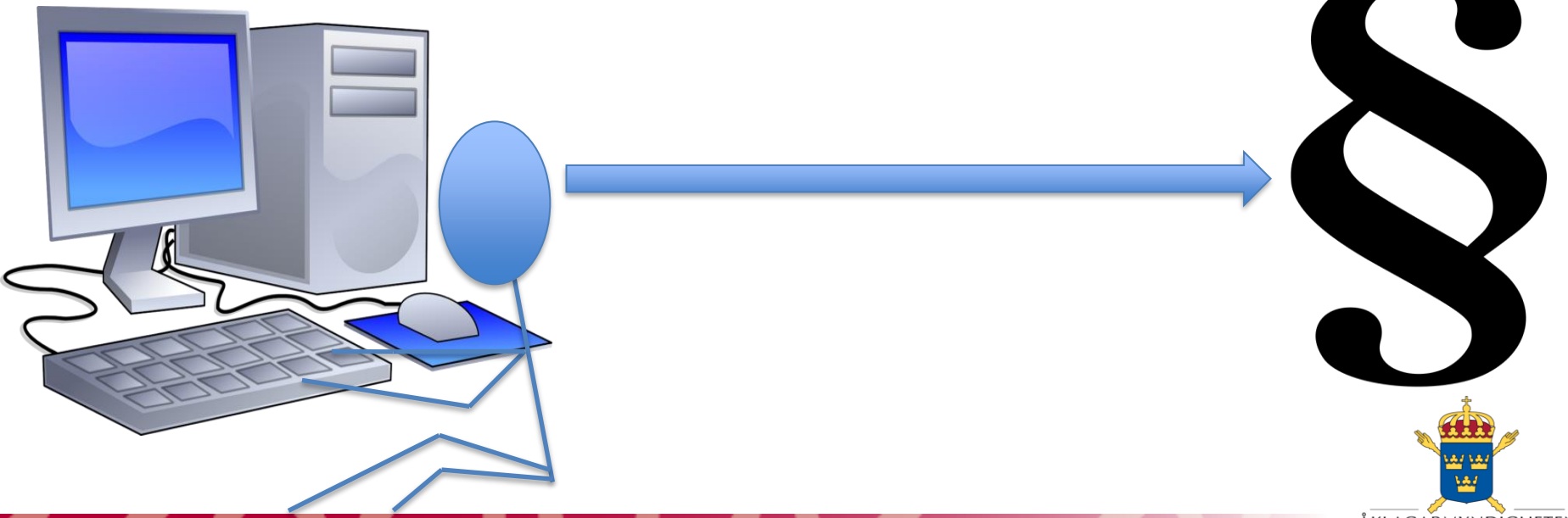
ÅKLAGARMYNDIGHETEN

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

Prosecutor as a “link”



Prosecutor as a “link”

Special demands on the “link”

- Knowledge

- Objectivity

- Presentation

ÅKLAGARMYNDIGHETEN

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

ÅKLAGARMYNDIGHETEN

Data categories

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

ÅKLAGARMYNDIGHETEN

Character of the investigative measure

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

Cross-border gathering

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

ÅKLAGARMYNDIGHETEN

Presenting digital evidence in court

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

ÅKLAGARMYNDIGHETEN

Contact information

Chatrine Rudström

Senior Public Prosecutor

chatrine.rudstrom@aklagare.se

+46 10 562 54 41

+46 70 346 35 57

ÅKLAGARMYNDIGHETEN

Bavarian State Ministry of Justice

POST-COVID CHALLENGES IN CRIMINAL JUSTICE

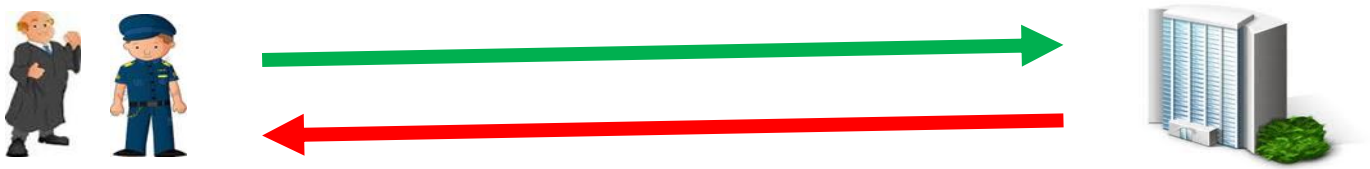
Barcelona, 22 February 2024 – 23 February 2024

Prosecuting Hate Speech and other criminal online content - Proactive cooperation by service providers

Co-funded by the European Union

Reactive vs. proactive cooperation

Reactive cooperation



Reactive vs. proactive cooperation

Proactive cooperation

Structure of presentation

- **Proactive vs. reactive** cooperation by service providers
- **Proactive cooperation by service providers** in the prosecution of **hate speech**
  - Obligations for service providers under **union law**
  - Additional obligations under **national law**?
  - **Voluntary cooperation** – codes of conduct

Advantages of proactive cooperation

- Investigation of otherwise unreported cases
- High efficiency - No need to issue production orders

Important tool in the prosecution of **mass phernomena** with **large numbers of unreported cases**: e.g. child sexual abuse, cyber crime, **hate speech**

Hate speech - harmonisation within the EU

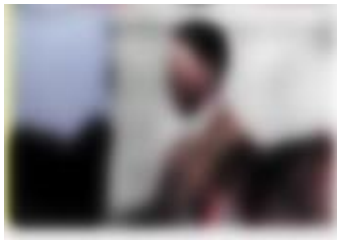
- Framework decision 2008/913/JHA of 28 November 2008 on combating racism and xenophobia (art. 1 par. 1):

  publicly inciting to violence or hatred, incl. by
  publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes

- COM proposal of 2021 to extend the list of EU crimes to hate speech and hate crime:

  - bias motivation
  - element of hatred

Hate speech - examples



Legal basis under Union law

Regulation (EU) 2021/784 of 29 April 2021 on Terrorist Content Online

- Directly applicable since 07.06.2022
- Applies to hosting service providers offering services in the Union
- art. 14 par. 5: terrorist content involving an imminent threat to life:

  obligation to inform authorities competent for the investigation and prosecution of criminal offences

Legal basis under Union law

Regulation (EU) 2022/2065 of 19 October 2022 Digital Services Act (DSA)

- Applies to **all intermedieary service providers offering services to recipients in the Union**, incl. hosting service providers (art. 2 par. 1 DSA) since 17.02.2024 (25.08.2023 for Very Large Online Platforms)

- **Limits liability** for illegal content

- Constitutes **due diligence and transparency obligations**, such as:
  - Legal representatives in the EU (art. 13 DSA)
  - Transparency reports (art. 15 DSA)
  - Notice and action mechanism (art. 16 DSA)

Legal basis under Union law

art. 18 DSA: Notification of criminal offences

What triggers the obligation to notify?
awareness *of "information giving rise to a suspicion that a **criminal offence involving a threat to the life or safety of a person or persons** has taken place, is taking place or is likely to take place"*

Applicability to **offences against public order**?

- Incitement of masses (sec. 130 of German Criminal Code= art. 1 COUNCIL FRAMEWORK DECISION 2008/913/JHA of 28 November 2008 on combating racism and xenophobia)
- Use of symbols of unconstitutional and terrorist organisations (sec. 86a of German Criminal Code)

Legal basis under Union law

art. 18 DSA: Notification of criminal offences

- What information has to be notified?
  "*all relevant information available*" (s. recital 56)

- Who has to be notified?
  authorities of Member State concerned (if impossible to determine: Member State of establishment or Europol)

Legal basis under national law

Can **national law** further define "*criminal offence involving a threat to the life or safety of a person or persons"* and/or extend obligation under art. 18 DSA?

Obstacles:

- Exhaustive nature of the DSA (art. 1 DSA, recital 9)
- art. 3 par. 2 Directive 2000/31/EC (E-commerce Directive), s. ECJ C-376/22 Decision of 9 November 2023 (KommAustria)

Voluntary proactive cooperation

- The EU **Code of conduct** on countering illegal hate speech online (31. May 2016): no commitments to notify competent authorities of criminal offences

- **Individual Projects**, e.g. joint initiative of the Bavarian State Ministry of Justice and the Bavarian Regulatory Authority for New Media

Justiz & Medien
KONSEQUENT GEGEN HASS

Eine Initiative des Bayerischen Staatsministeriums der Justiz und der Bayerischen Landeszentrale für neue Medien

Bayerisches Staatsministerium der Justiz

BLM Bayerische Landeszentrale für neue Medien

Thank you for the attention!

Michael Rothärmel
Email: michael.rothaermel@stmj.bayern.de

Social Media as Digital Evidence

Concrete cases

Patricia Ayodeji
payodeji@icab.cat

Co-funded by the European Union

ABOGADO · ILUSTRE COL·LEGI DE L'ADVOCACIA DE BARCELONA

ADVOCADA · ILUSTRE COL·LEGI DE L'ADVOCACIA DE BARCELONA

The Law Society

Marina Grynykha in Unsplash

IN THE HIGH COURT OF SOUTH AFRICA

(WESTERN CAPE DIVISION, CAPE TOWN)

Case Number: **8271/2023**

In the matter between:

BONNY LEVI First Applicant

NURI SUSHI (PTY) LTD Second Applicant

and

MEHDI PAKDOUST Respondent

Coram: Bishop, AJ

Heard: 22 November 2023

Delivered: 24 November 2023

BISHOP, AJ

1. The First Applicant (**Levi**) and the Respondent (**Pakdoust**) were co-owners of a business called Nuri Sushi (Pty) Ltd. As the name suggests, it is a sushi restaurant. And, like sushi that had stood in the sun too long, their relationship went sour. The details are not before me, save for one. It concerns Facebook, and it has led to a Meta dispute spanning continents. In the end, it turned out it was all the fault of Zane the marketing manager.

2. Nuri Sushi had a Facebook Page. It used this Page to advertise its business. It was, at least on Levi's telling, an extremely valuable asset for the business, particularly because it had 11 000 hungry followers.

3. A Facebook Page – unlike a personal Facebook account – is run by an "administrator". The administrator must be a Facebook user. Mr Pakdoust was a Facebook user and while he and Levi were still working together, he was an administrator of the Nuri Sushi page. Mr Levi was not a personal Facebook user. But he also acted as an administrator of the Nuri Sushi page through another of his businesses that did have a Facebook account – Eastern Food Bazaar.

4. An administrator of a Facebook page has many powers. He can add content to the page. He can invite other Facebook users to become administrators of the page. And he has the awesome ability to remove existing administrators.

5. That is what Pakdoust did to Levi. On 26 April 2021, he removed Levi's agent – Eastern Food Bazaar – as an administrator of the Nuri Sushi Page. This

seems to be have been the culmination of the dispute between the parties about Nuri Sushi.

6. Fortunately, a month later, the parties were able to settle their disputes. Levi agreed to buy out Pakdoust's share in Nuri Sushi for R1.5 million. One of the clauses of that settlement agreement – clause 3.2 – related to Nuri Sushi's social media. It read:

> *Pakdoust agrees and undertakes to disengage from any social media platform relating to Nuri and / or St Georges Mall including all and any Facebook pages, Instagram and any other social media activity. In this regard, Pakdoust agrees and undertakes to do all things necessary to remove himself as the administrator, or the like and shall hand over to Levi all and any passwords and access information that may be required from time to time.*

7. This seems like a relatively simply clause – Pakdoust was required to transfer control of the Nuri Sushi Facebook Page to Levi. But it does not translate accurately into Facebook lingo. What Facebook required to transfer control was for Pakdoust to make Levi (or his agent) an administrator, and then remove himself as an administrator. It could not be achieved through the handing over of "passwords and access information". It took two experts and American lawyers to figure out how to actually achieve something that ought to have been easy.

8. Pakdoust claims that, shortly after the settlement agreement was concluded, he invited Eastern Food Bazaar to be an administrator, and then removed himself as administrator. From his perspective, his job was done. But Eastern Food Bazaar never received a notification from Facebook that it had been invited to be an administrator. And so it could not become an administrator.

If social media evidence was an ice cream

A bit of a perfect storm

An integral part of our daily lives
Easy to use

Instrument for the commission of crimes & sometimes the scene in which the crime is committed

Criminals always adapt

Spot their vulnerability

Create their own evidence against them

Risks of Using Social Media as Evidence

Data accuracy

must meet the same standards as other types of evidence to be admissible in court.

Privacy

collecting data in violation of GDPR

Ethical

the fairness of using such evidence, and the extent to which social media data should be used in legal cases.

Jaw dropping extraordinary evidence in social media

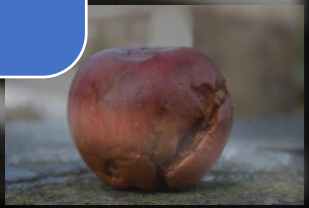
Most Social media platforms have become a crucial source of digital evidence, often used in court cases and investigations

Challenges in collecting and preserving social media evidence

Best practices

Essential to use the right tools and techniques to ensure admissibility

A rotten apple will spoil the whole barrel




Case Law


Case I
Facebook


designed by freepik.com

Audiencia Provincial Valencia,
Judgment 468/2020
19 Nov. 2020, Rec. 44/2020

Glorifying terrorism and incitement to hatred

No followers. No real or imminent danger. No consequences.


Case II
Facebook Live

Judgment TSJ Castilla y León de Valladolid 15 March 2021

A warm, fuzzy feeling

The company learnt through its Area Manager, in charge of services to their client that at ***08:31 on 1 March 2020,*** *one of its staff published on Facebook* ***whilst driving*** *a vehicle provided by the company,* ***at a speed close to 90 km/h (seen on the speedometer) and at the same time taking a photograph of the steering wheel and rear panel.***

In the disciplinary file it was not proven that the company encourages as common practice that its drivers take photographs **whilst driving** their heavy-duty trucks, and publish them in social media whilst in motion, even though some workers do it.


Case III
(previously Twitter)

King Emeritus Juan Carlos I of Spain

Tribunal Supremo
Judgment 135/2020 7 May 2020, Rec. 3344/2018

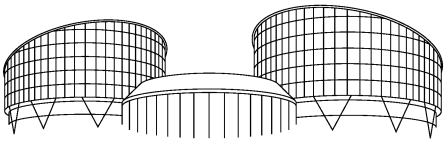
Pablo Hasel (Pablo Rivadulla Duró) Rapper and Poet
Public praise or justification of terrorism, insult and slander against the Spanish Crown and State Institutions (the police)...

64 incriminating **tweets** (2014-16) including support for convicted members of a terrorist group, posted **video** accusing King Emeritus of squandering public money, of murdering his brother, of spending money on "binges and whores, a mafia boss, comparing police to Nazis.... Offensive rap song about the Monarchy

More than 54,000 followers

Imprisoned since 15/02/2021

Image Bego Blanco



ECHR 10/23 Application no. 27925/21
Pablo RIVADULLA DURÓ –v-Spain

"The Court also observes that the applicant's messages were easily and freely available online and thus had the potential to reach a large number of people, including those of a young age.

Court declared Pablo Hasél's case inadmissible (9 November 2023)

Conviction for royal slander did not disproportionality impair his right to freedom of expression


Case IV YouTuber

Image Ana Ivanova

Instrument and “scene” of the crime

YouTuber

Social media influencer **€€**

Upload or create videos on YouTube

Typically post to their **personal** YouTube channel

Supreme Court Judgment 547/2022 Appeal Humiliation homeless Silvio

Cirilo Subscriber Dare –physical space remove cream and replace with toothpaste and give to general public – gave to homeless instead and 20€

Complaints subscribers and mentions on TV, newspapers, radio

Massive and indiscriminate diffusion

82 public videos
1.161,989 subscribers
124.410,846 visualizations of his content

Google Inc.

January 2017	**798,29€**
February 2017	**1.129,30€**
March 2017	**253,92€**

Close channel. Banned for 5 years (removed on appeal as took place on public streets and not YouTube)

15 months imprisonment

Cirilio pay Silvio 20K moral damages

Innovative tools for Digital Investigation

Blackbag Technologies

BlueBear

Magnet Forensics

Cellebrite

AccessData

Sumuri Forensics Simplified

Oxygen Forensics


e-pdp®
Thank you
All images : Zamorik Brothers except Ana Ivanova (slide 25) -Noun Project
Bego Blanco (slide 23) and Slide 14
https://e-pdp.eu/

Barbancho Legal / INTERNATIONAL DEFENSE IN SPAIN

HANDLING ELECTRONIC EVIDENCE ON MOBILE DEVICES IN COURTS: PERSPECTIVES OF THE DEFENCE

María Barbancho Saborit
Criminal Lawyer

Co-funded by the European Union

I. ACTUAL SITUATION

- Digital evidence increasingly relevant in criminal proceedings: UK Chief Police Council " over 90% of all crime is recognized to have a digital element"

- Challenge: establishing a set of rules to improve cross-border admissibility of electronic evidence and evidence itself. Nowadays admissibility of evidence is still on national basis.

- Convention on Cybercrime does not include any specific digital evidence, chain of custody or digital forensic standards. Neither do the European Production and Preservation Orders. Neither does any other mutual recognition and cooperation instrument of the EU.

II. ACTUAL SITUATION: CONTEXT OF ART 6 ECHR

¿ Are criminal proceeding sufficiently regulated in order to ensure accurate technology fact-finding and protection of suspection from adverse effects of the digital sustem and data?

¿Are suspects, accused and defendants granted the opportunity to effectively access and examine digital evidence or challenge forensic expertise?

II. ACTUAL SITUATION: CONTEXT OF ART 6 ECHR

In general: ECHR upheld the position that the admissibility, probative value and burden of proof must be given to the specific national legal systems. The Court does not act as fourth instance examining admissibility and exclusionary rules on evidence.

KHAN vs UK (Feb 2014) : intrusive surveillance techniques should be regulated by law and not by police guidelines, which are not sufficiently binding and do not meet requirements for foreseeability. Legal basis of the measure in view of fair trail safeguards are: a) surveillance to be based on presented facts, time limits, authorization and notification after termination.

II.EU POLICY- MAKING AND EVIDENCE ADMISSIBILITY:

Barbancho Legal / INTERNATIONAL DEFENSE IN SPAIN

- **The 2009 Green Paper and the European Investigation Order:** details the procedures for requesting and exchanging evidence between EU Member States but created no rules on evidence gathering and admissibility.

- **The European Public Prosecutor's Office (EPPO)**: e the power to gather and present evidence before national courts. The relevant legal framework does not set standards for gathering evidence.

- **The E-Evidence Package:** In response to the increasing demand for cross-border electronic information, in April 2018 the European Commission proposed an "E-evidence package" to create a tool for law enforcement agencies to obtain electronic data from other countries6. The texts of the proposed regulation7 and directive do not address common standards on gathering or admissibility of evidence.

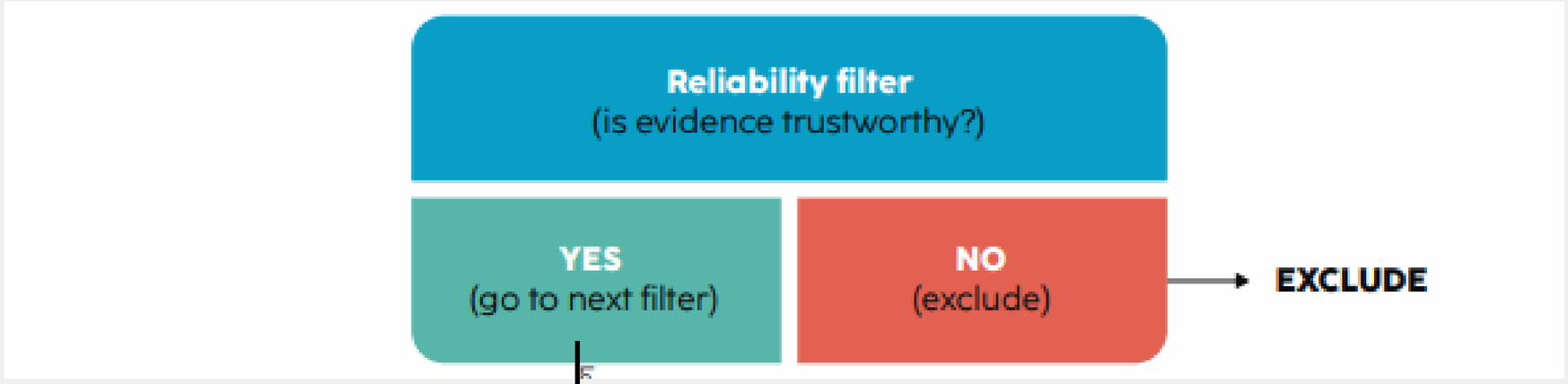
- **Procedural Rights Directives:** The question of evidence exclusion as a remedy for violation of these rights was a key issue during negotiations but none of the Directives provides clear provisions on this.

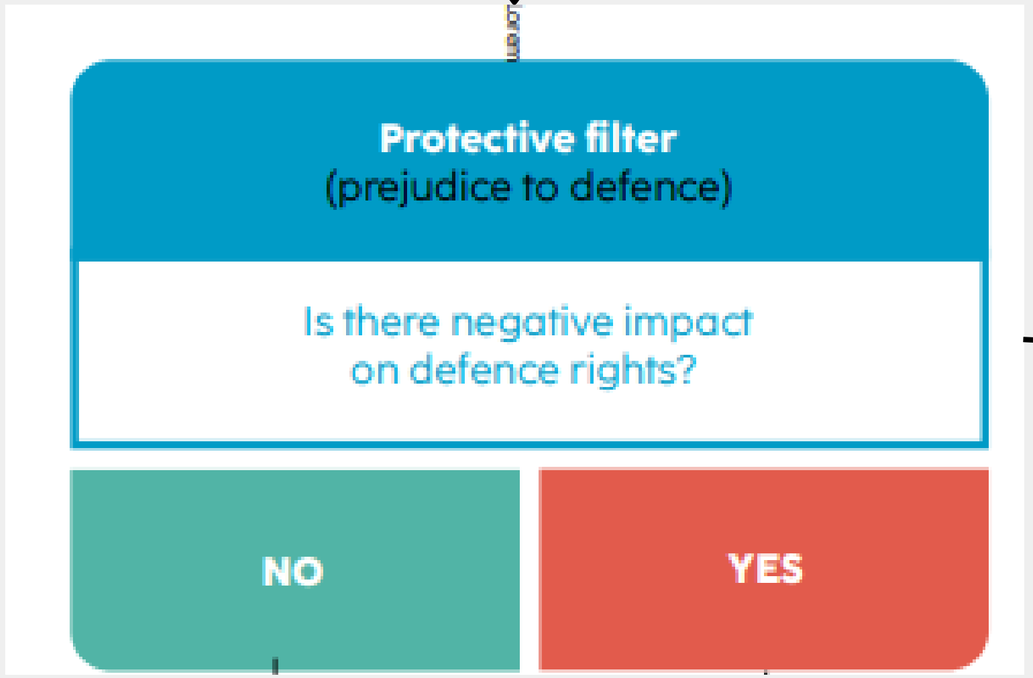
III. RECOGNIZED STANDARS TO ENSURE DATA SECURITY

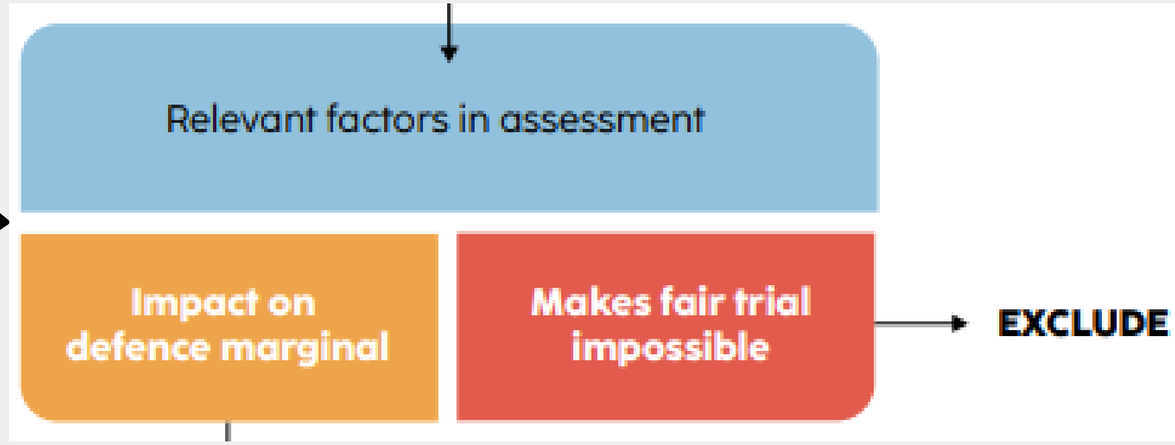
- Global Guidelines for Digital Forensics Laboratories (Interpol - Mai 2019)
- Best Practice Manual for the Forensic Examination of Digital Technology (ENFI, European Network of Forensic Science Institutes, 24 January 2024)
- The ISO/IEC STANDARD 21037 Guidelines for identificacion, collection, acquisition and preservation of digital evidence

ADMISSIBILITY TEST: RELIABILITY + PROTECTIVE FILTER

Barbancho Legal / INTERNATIONAL DEFENSE IN SPAIN







IV. ELI PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL ON MUTUAL ADMISSIBILITY OF EVIDENCE AND ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDING.

Article 7

Admissibility of electronic evidence

(1) Member States shall provide that electronic evidence is used in criminal proceedings only if it is ensured that:

(a) the evidence at the time of its use corresponds to the state in which it was obtained;

(b) the evidence at the time of its use corresponds to the full extent to the evidence at the time it was obtained;

(c) the evidence was sufficiently protected against falsification and manipulation in the period between its obtention and its use.

(2) Sufficient protection within the meaning of paragraph 1(c) shall in any event require that each access to the electronic evidence is adequately logged and that the storage medium is adequately protected against external interference.

(3) Member States shall ensure that electronic evidence is only used in criminal proceedings if there is sufficient evidence that it is not the result of manipulation or forgery prior to the time of production.

(4) The defendant has the right to access the full extent of the evidence, and to the report prepared by qualified IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions in the expert opinion. Member States shall ensure that qualified IT experts are involved, upon the request of the suspect or accused, in the assessment of the standards established in paragraphs 1 to 3.

(5) Member States shall consider granting the defendant the right to request the use of machine-learning technology or predictive coding when the full review or the keyword search of documents is not appropriate for an accurate assessment of the evidence.

Barbancho Legal / INTERNATIONAL DEFENSE IN SPAIN

CONCLUSIONS:

- **Chain of custody:** There are certain minimum standards that shoud be implemented by EU Member States such as the presence of an IT expert in acquisition phase of electronic data: ensures the integrity of data seized or for example the search and seizure of computer or any other access to electronic data should be carried out in presence of the defendant or the user of the device.

- **Admissibility:** general rules of admissibility of evidence should be implemented; principle of general admissibility of legally obtained evidence (lex loci) should only be broken if its use in the other Member State is against bis constitutional fundamental principles

Barbancho Legal / INTERNATIONAL DEFENSE IN SPAIN

THANK YOU
DANKE
GRACIAS
GRÀCIES

MBARBANCHO@BARBANCHO.LEGAL

University of Antwerp
Faculty of Law

Dealing with e-evidence in cross-border cases: best practices and possible new scenarios in light of the new EU legislation

Prof. dr. Joachim Meese

associate professor

attorney

Co-funded by the European Union

Introduction and background

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

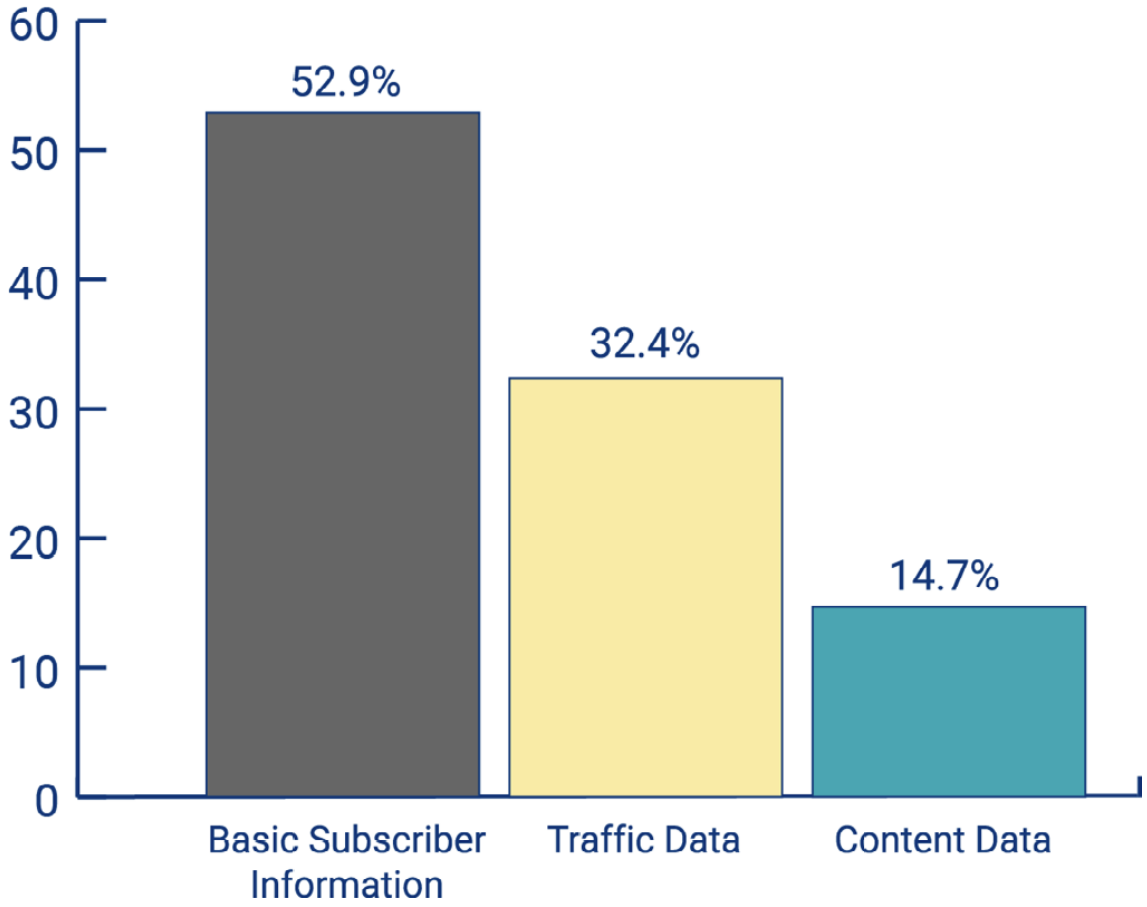
- historical background -

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, …

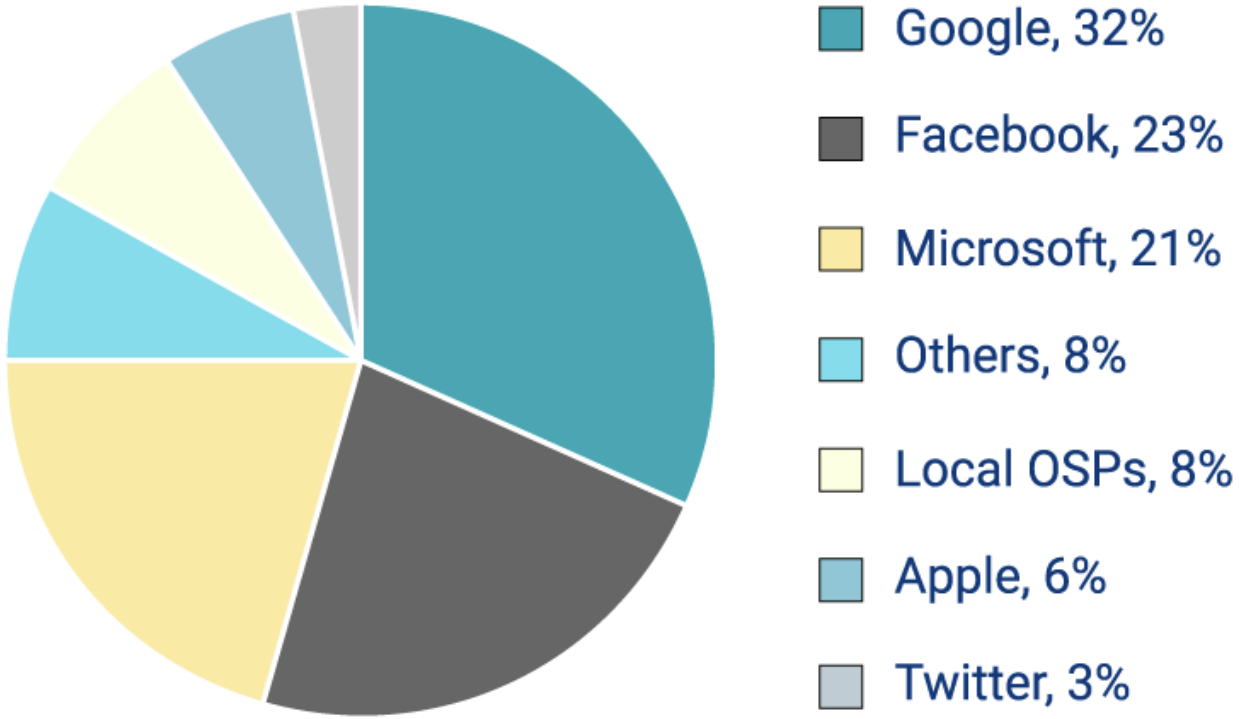
most common types of e-evidence

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



most common types of e-evidence

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



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

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)

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

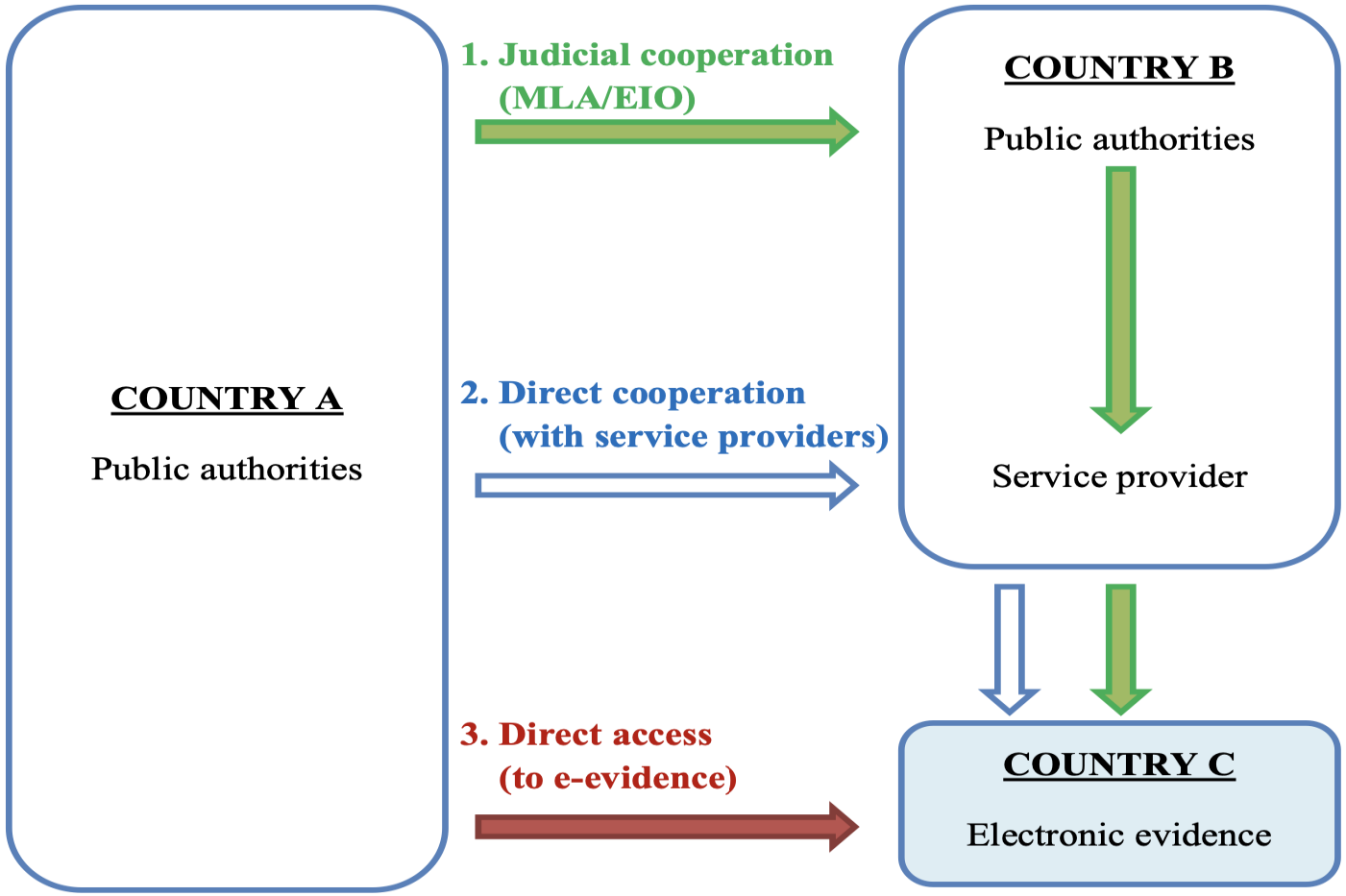
https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

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

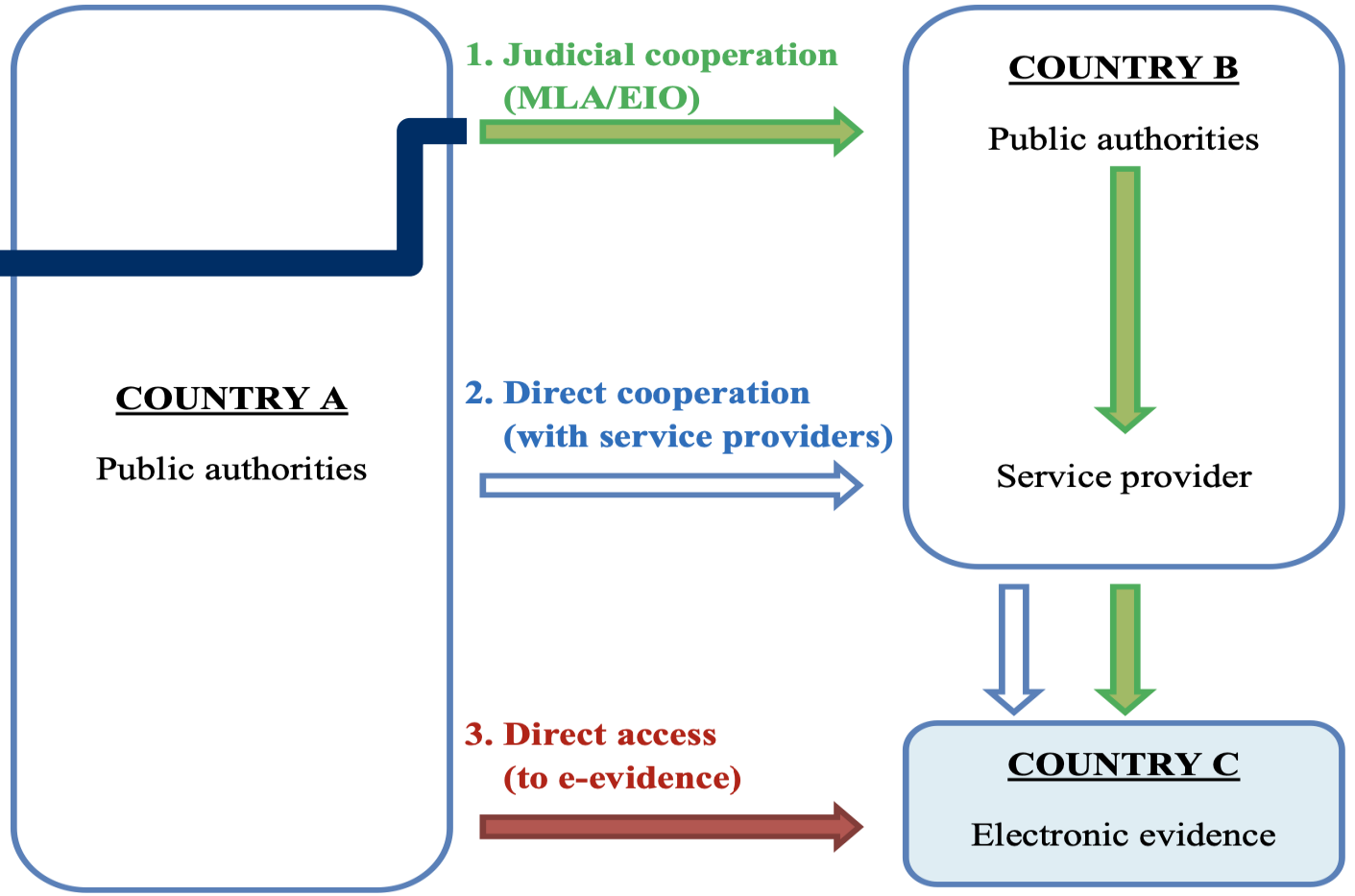
cross-border access to evidence

- **possible scenarios:**



cross-border access to evidence

- **possible scenarios:**



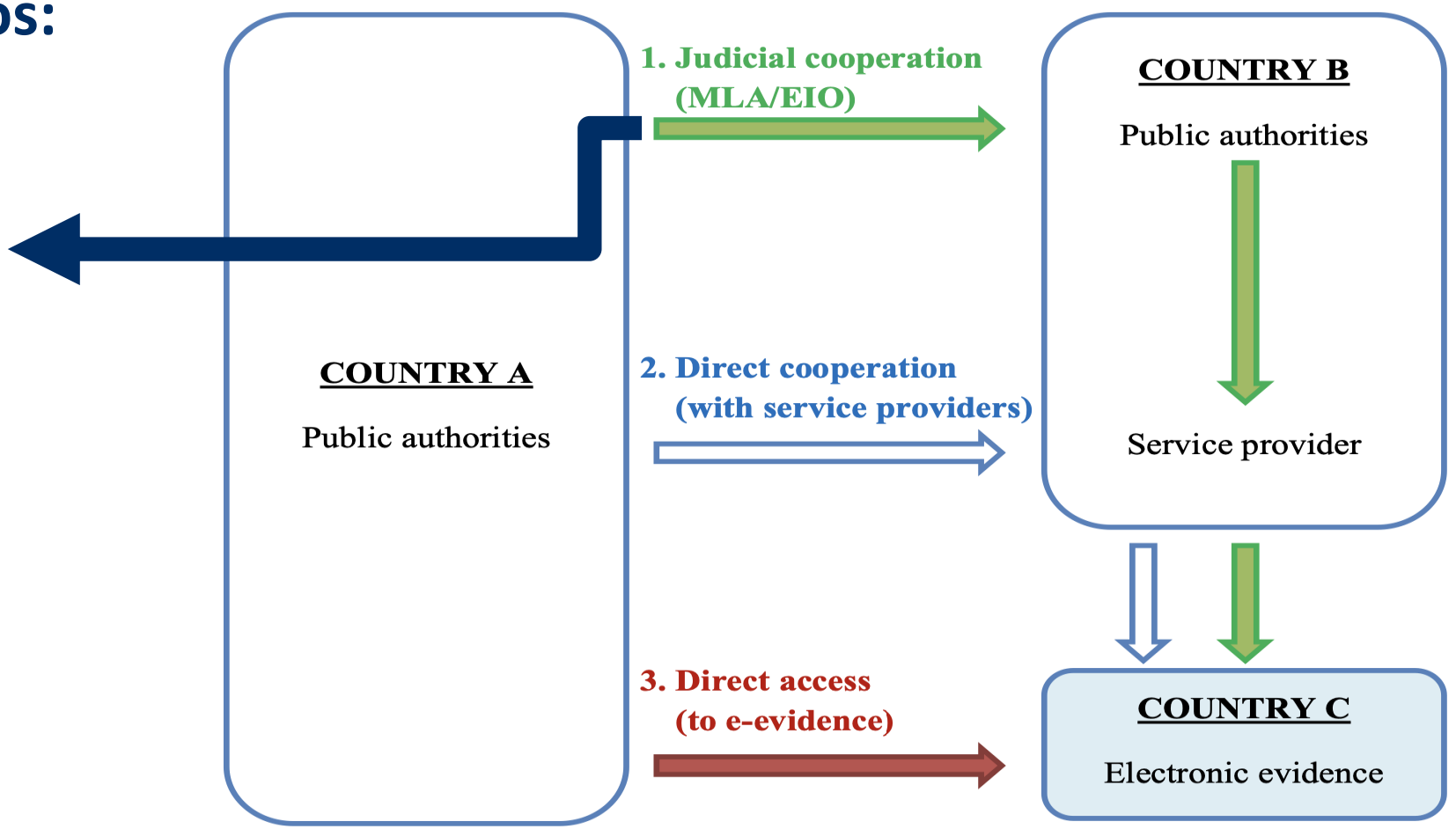
- ✓ within EU: EIO
- ✓ outside EU: international agreements
  - Budapest Convention on cybercrime
    - 2nd additional protocol can be signed by MS in the interest of the EU (Council decision of 5 April 2022)
      - ✓ improve international cooperation
      - ✓ enhance direct cooperation
      - ✓ emergency 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)

cross-border access to evidence

- **possible scenarios:**

number of requests per year on e-evidence:

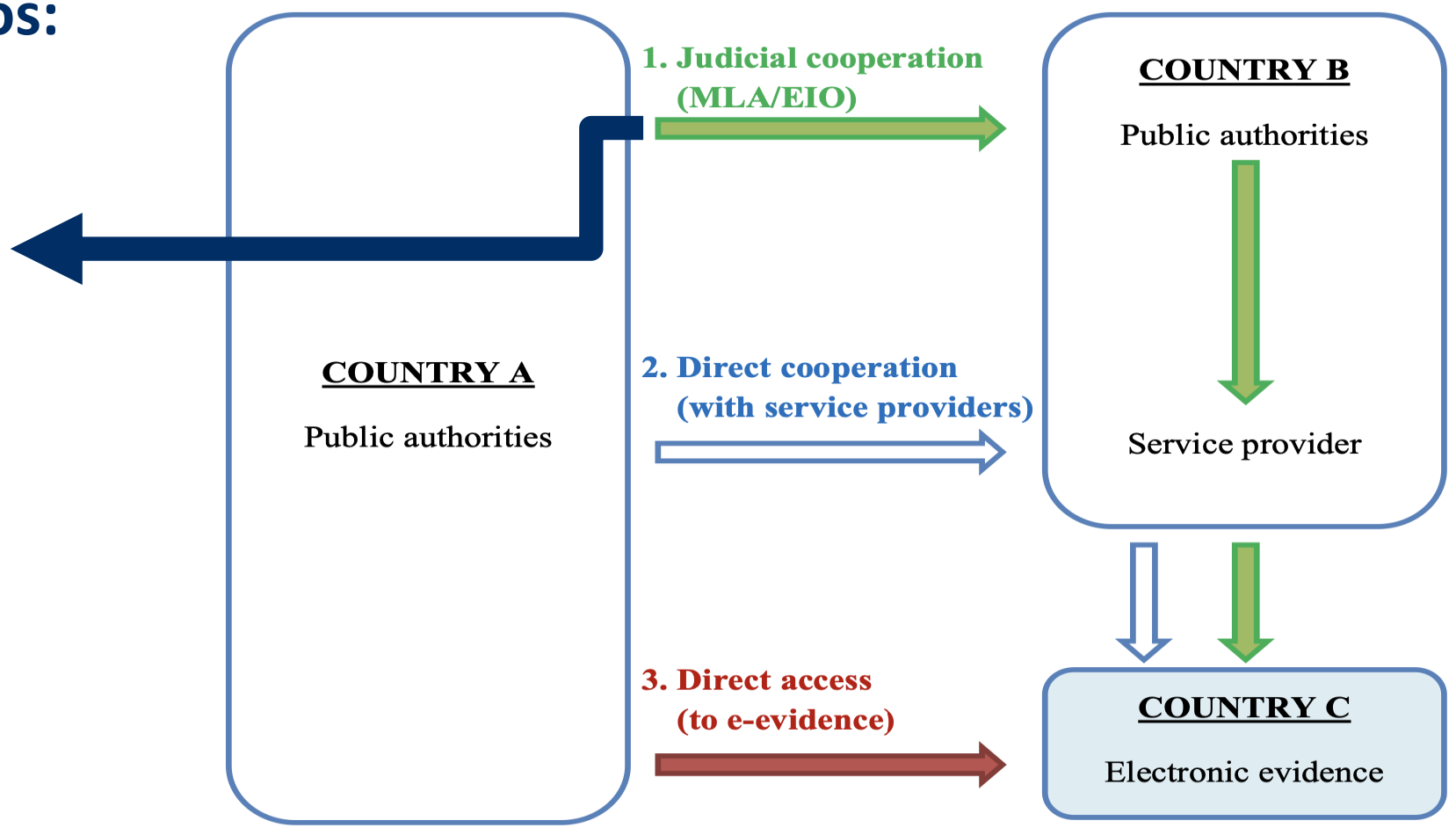
- ✓ between EU member States: 13.000
- ✓ EU MS to US: 1.300



cross-border access to evidence

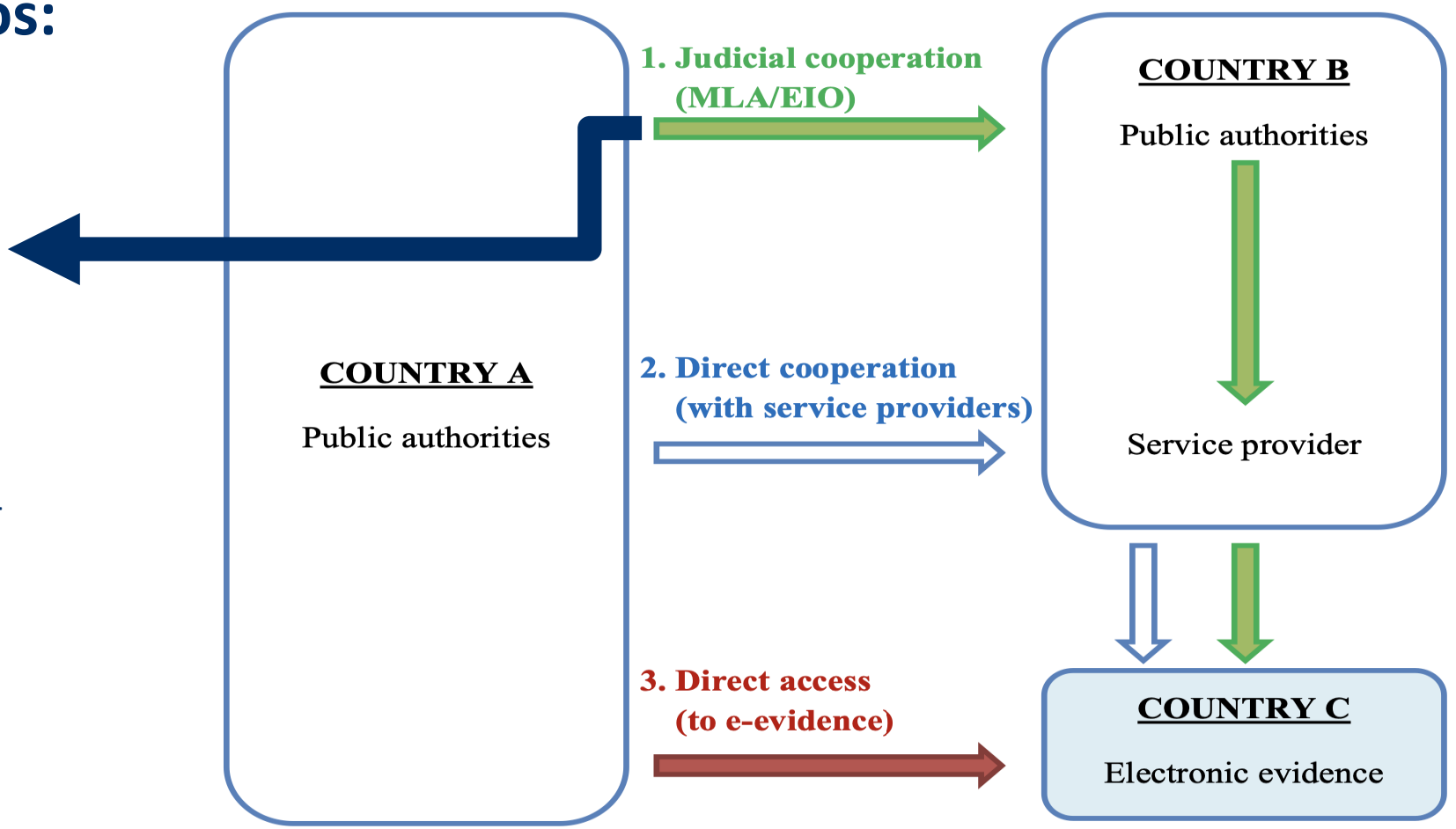
- **possible scenarios:**

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



cross-border access to evidence

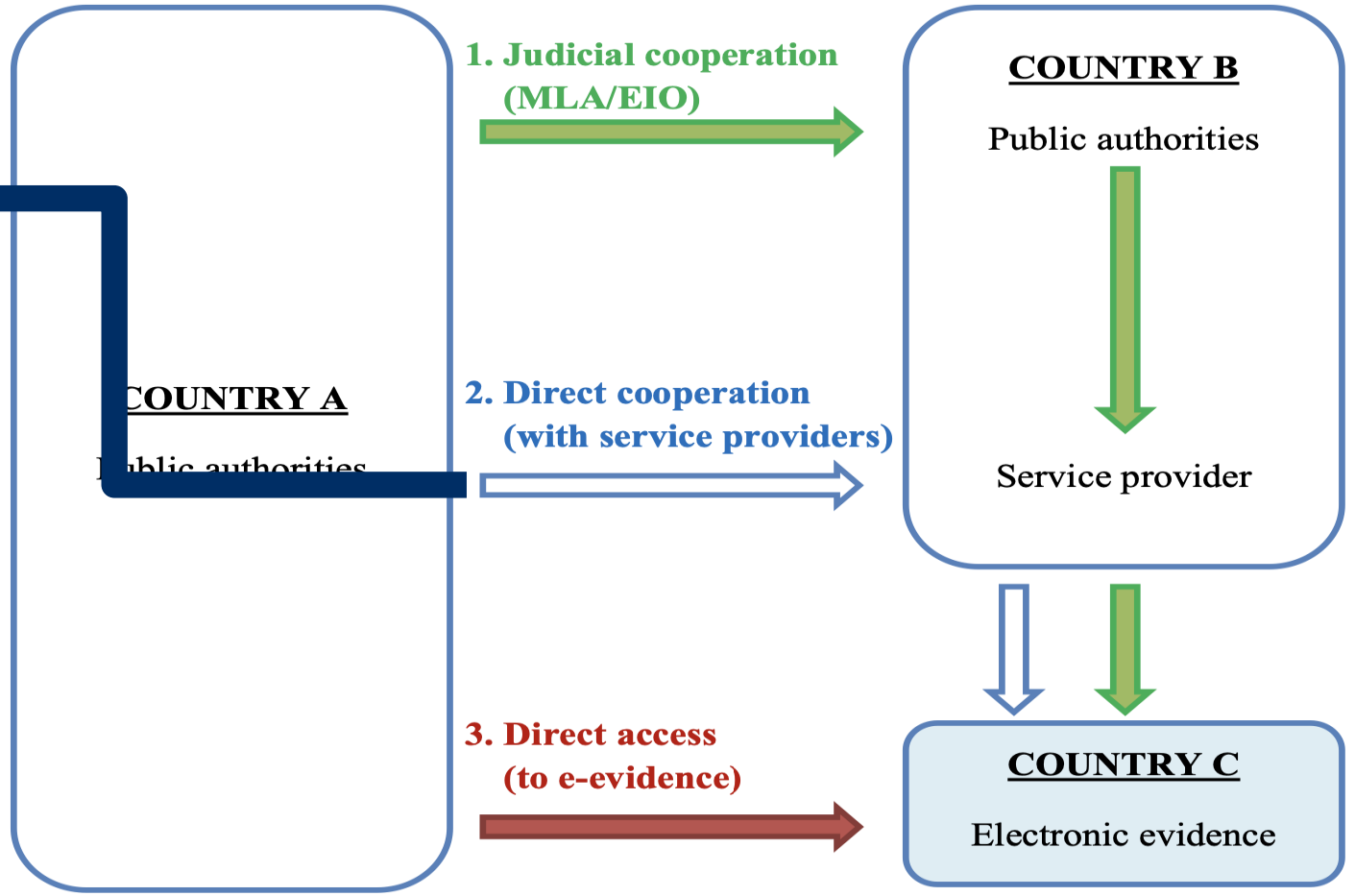
- **possible scenarios:**



✓ 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

cross-border access to evidence

- **possible scenarios:**



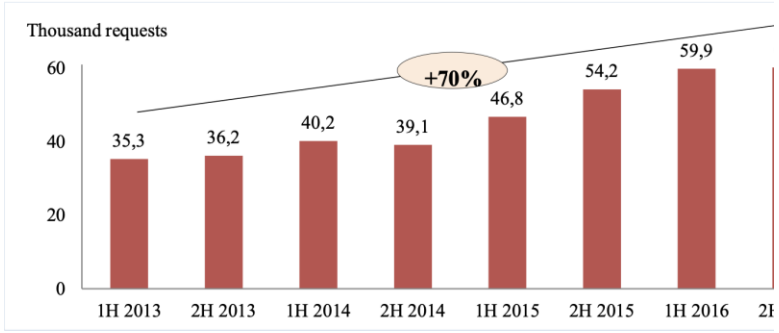
✓ non-content data
- service providers established in the US and, to a more limited extent, in Ireland, which reply directly to requests from EU member States law enforcement authorities on a voluntary basis

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

cross-border access to evidence

- **possible scenarios:**

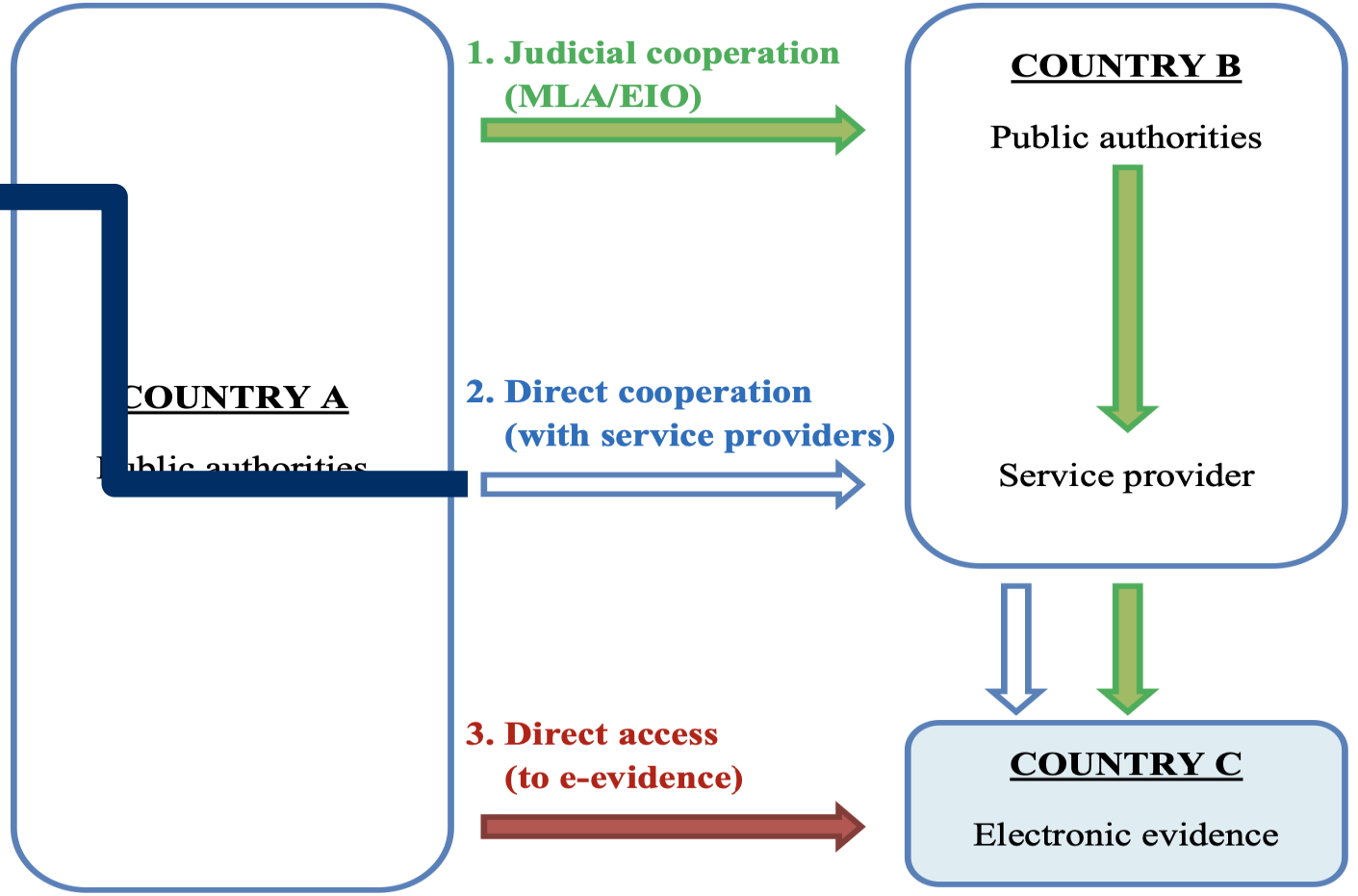
numbers:



→ in 2018, 3 member States account for > 75% of all requests from the entire EU

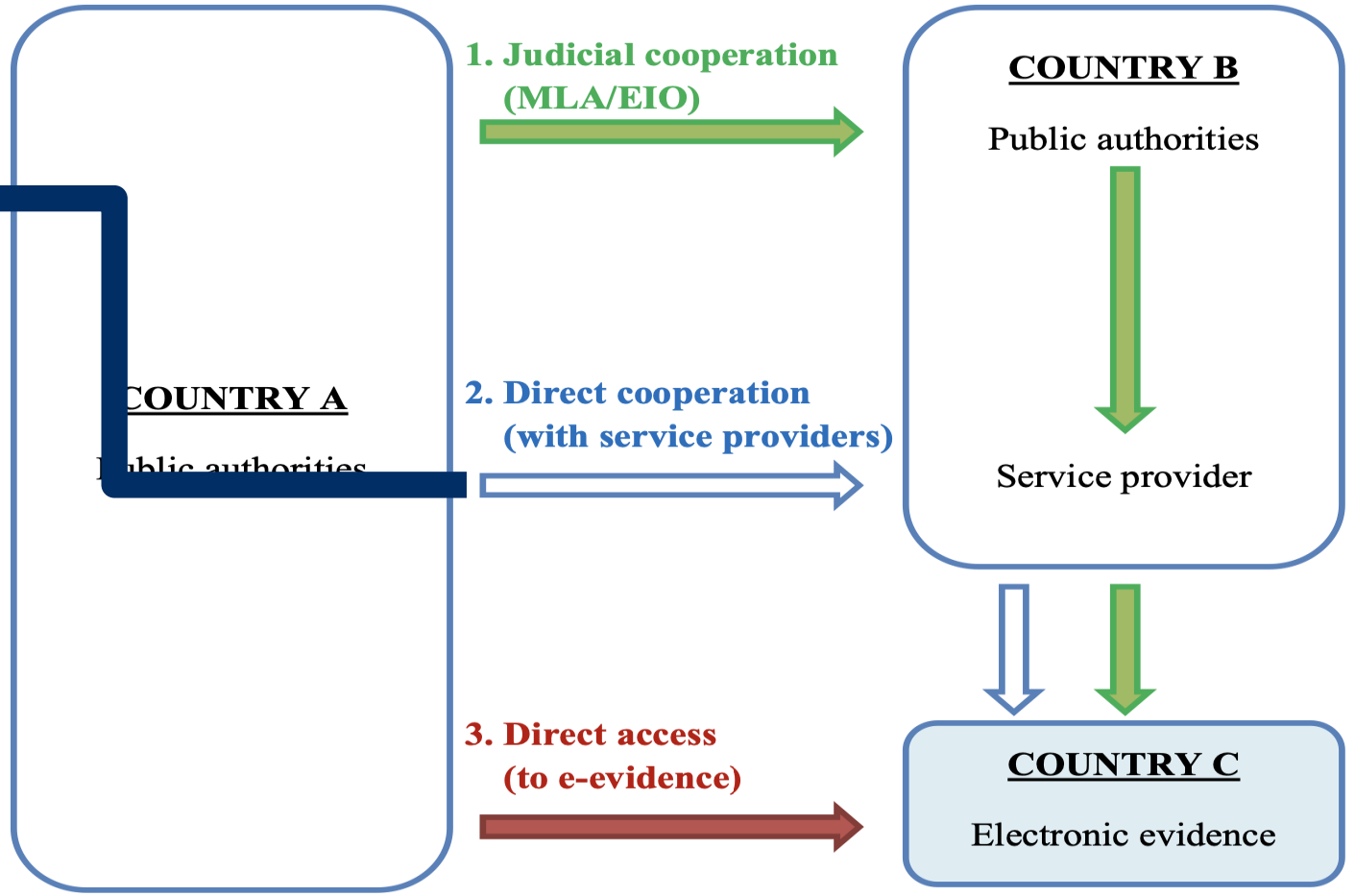
- Germany: 35.271
- UK: 28.598
- France: 27.268

→ Google & Facebook: 70% of total requests



cross-border access to evidence

- **possible scenarios:**



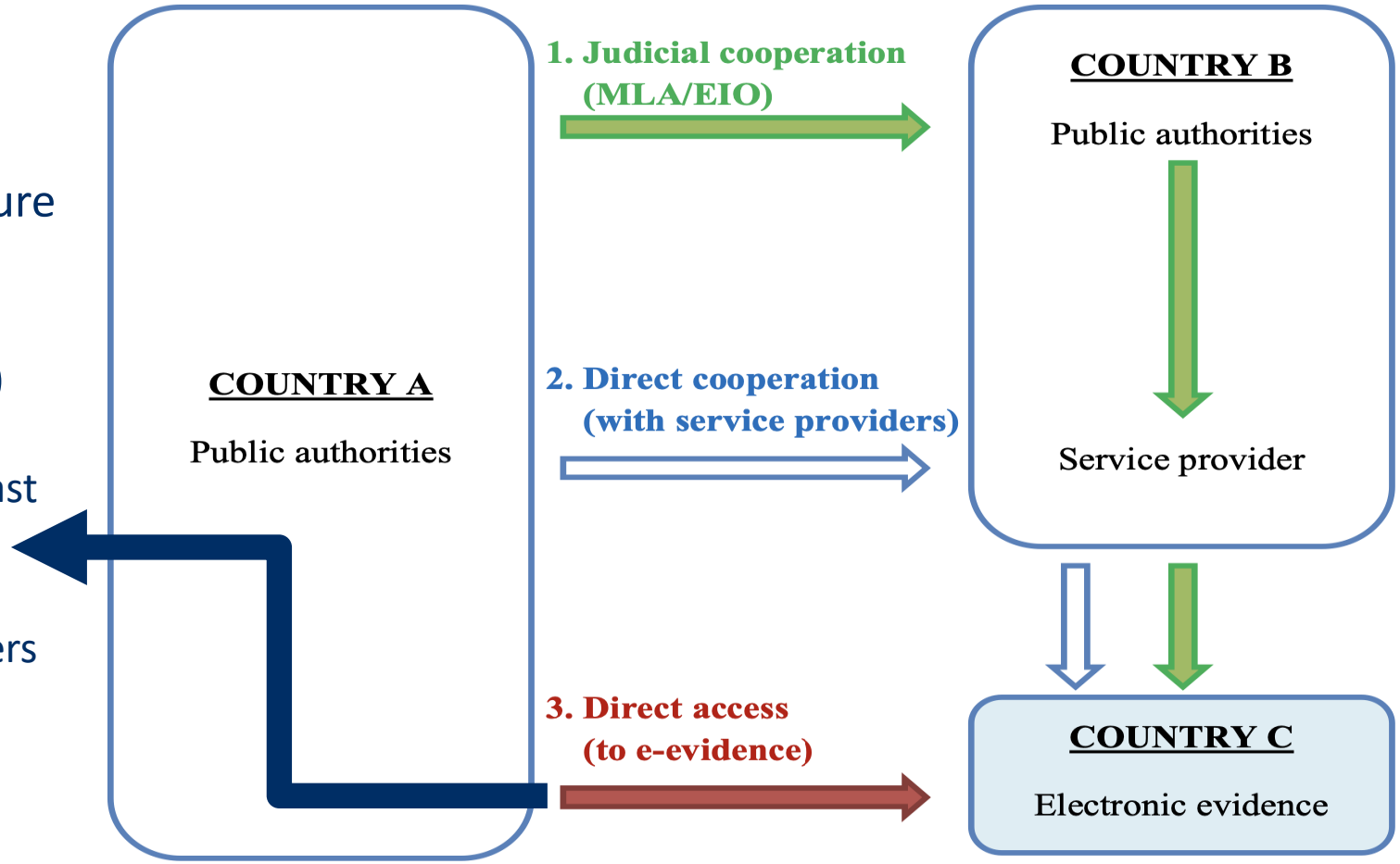
✓ challenges
- can be unreliable
- can take too long
- only possible with a limited number of service providers
- providers all apply different policies
- not transparent
- lacks accountability in case of non-compliance
  - see, however the Belgian case of YAHOO! (Cass. 1 December 2015, P.13.2082.N)

cross-border access to evidence

- **possible scenarios:**

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

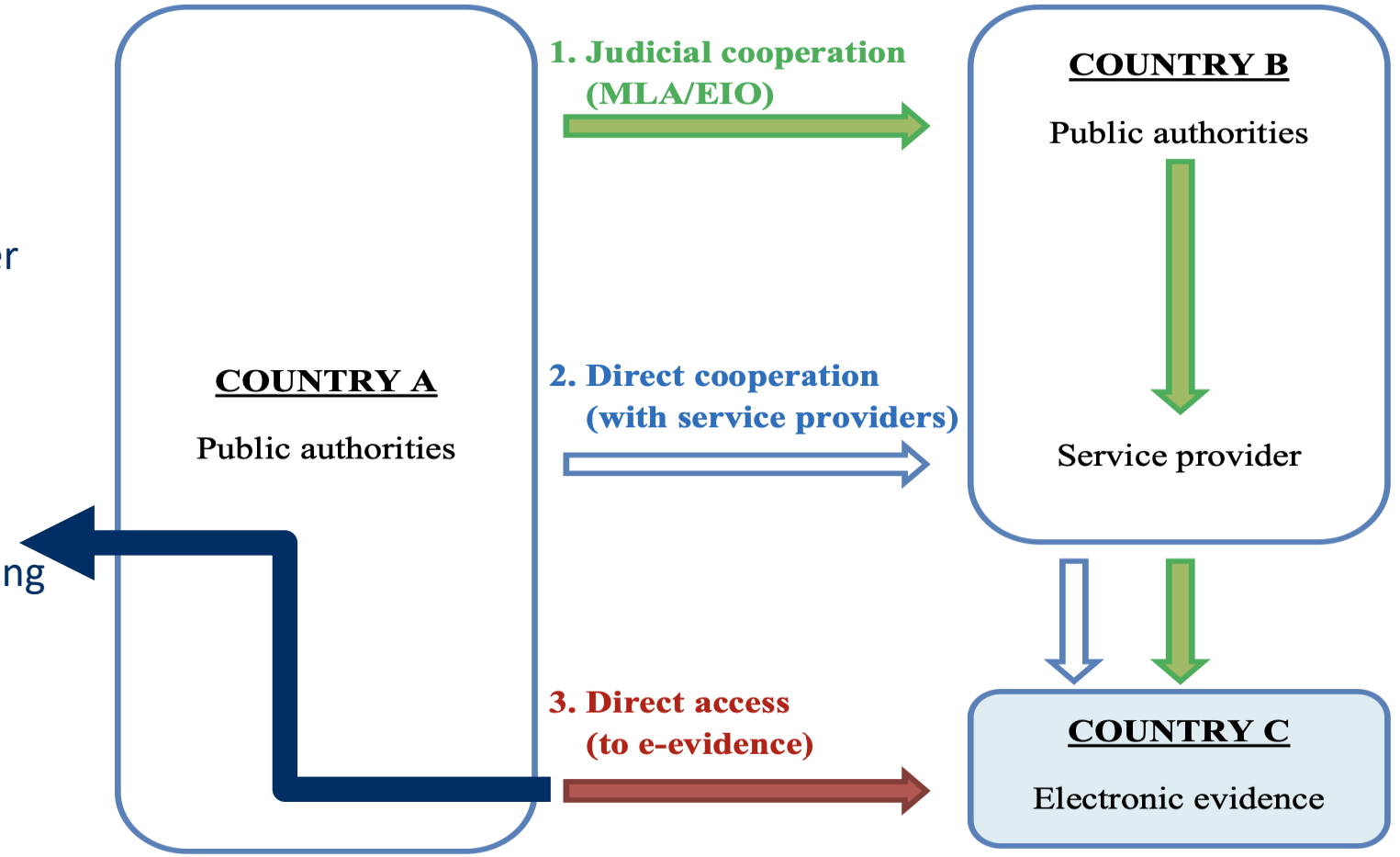
→ possible under national law of at least 20 member States
→ this tool becomes more relevant
  - data are regularly stored on servers in a different location
  - in case of loss of knowledge of location of data (e.g. Darknet)



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



cross-border access to evidence: what about EPO?

- **EPO**
  - Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings
    - http://data.europa.eu/eli/reg/2023/1543/oj
    - applies from **18 August 2026**
  - Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives of gathering electronic evidence in criminal proceedings
    - http://data.europa.eu/eli/dir/2023/1544/oj
    - must be transposed into national law by **18 February 2026**

cross-border access to evidence: what about EPO?

- **EPO**
  - what:
    - the Regulation: 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)
    - the Directive: rules on the designation of designated establishments and the appointment of legal representatives of certain service providers that offer services in the Union, for the receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States, for the purposes of gathering electronic evidence in criminal proceedings
  - 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

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

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!)

Comparative scheme: visual representation

More about EIO

- basic premise & scope -

- procedure -

- challenges and limitations -

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

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)

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

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)

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

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

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

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)

More about EPO

- key principles & main concepts -

- scope & procedure -

- conditions & grounds for refusal -

EPO – the Regulation

- **Scope (art. 2)**
  - criminal proceedings
    - both during pre-trial and trial phase
    - also against legal persons
  - execution of a custodial sentence or detention order of at least 4 months, imposed by a decision that was not rendered in absentia
  - only for data pertaining to services rendered by service providers

EPO – the Regulation

- **Definitions (art. 3)**
  - service provider: anyone providing one or more of the following categories of services (except for financial services):
    - electronic communication services, such as:
      - internet access services
      - interpersonal communications services (messaging services, email services, internet telephony services, …)
    - internet domain name and IP numbering services, such as IP address assignment, domain name registries, and related privacy and proxy services
    - other information society services which enable users to communicate with each other, or to store or otherwise process data, such as social networks, online marketplaces and other hosting service providers

EPO – the Regulation

- **Definitions (art. 3)**
  - offering services in the Union:
    - enabling natural or legal persons in a Member State to use the aforementioned services; and
    - having a *substantial connection*, based on specific factual criteria, to the Member State referred to in the first point; such a substantial connection is to be considered to exist where the service provider has an establishment in a Member State, or, in the absence of such an establishment, where there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States

EPO – the Regulation

- **Definitions (art. 3)**
  - data:
    - subscriber data: relating to the identity of the user, e.g. name, date of birth, billing and payment data, …
    - data requested for the sole purpose of identifying the user: IP addresses, logs and access numbers together with technical identifiers, …
    - traffic data: relating to the provision of a service, e.g. the geographic location of the device used, date, time, duration, …
      - more privacy-intrusive
      - under certain circumstances, IP addresses can be considered traffic data
    - content data: text, video, voice, images, sound, …

EPO – the Regulation

- **Definitions (art. 3)**
  - electronic evidence
    - subscriber data, traffic data, or content data lawfully stored by or on behalf of a service provider, in an electronic form, at the time of the receipt of an EPOC or EPOC-PR

EPO – the Regulation

- **Issuing authority (art. 4)**
  - EPOC
    - subscriber data & data for the sole purpose of identifying the user
      - a judge, a court, an investigating judge **or a public prosecuto**r competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC requires review in the issuing State, which can also be done by a **public prosecutor**
    - traffic & content data
      - a judge, a court, an investigating judge competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC requires **judicial** review in the issuing State (i.e. review by a judge, a court of an investigating judge)

EPO – the Regulation

- **Issuing authority (art. 4)**
  - EPOC-PR
    - all data categories
      - a judge, a court, an investigating judge or a public prosecutor competent in the case concerned, or
      - any other competent authority as defined by the issuing State which, in the case concerned, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law → such EPOC-PR requires review in the issuing State, which can also be done by a public prosecutor

EPO – the Regulation

- **Conditions for issuing**
  - EPOC (art. 5)
    - necessary and proportionate
      - the EPOC may only be issued if a similar order could have been issued under the same conditions in a similar domestic case
    - EPOC for subscriber data & data for the sole purpose of identifying the user
      - may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months
    - EPOC for traffic data or content data
      - requires a sentence of a max. of at least 3 years in the issuing State, or one of the offences as summed up in art. 5.4 (offences connected with cyber-crime, fraud relating to non-cash means of payment, terrorism and sexual abuse of children)
    - immunities and privileges: see art. 5.10

EPO – the Regulation

- **Conditions for issuing**
  - EPOC-PR (art. 6)
    - necessary and proportionate
      - the EPOC-PR may only be issued if a similar order could have been issued under the same conditions in a similar domestic case
    - may be issued for all criminal offences and for the execution of a custodial sentence or a detention order of at least 4 months

EPO – the Regulation

- **Legal representatives**
  - service providers shall designate or appoint at least one addressee for the receipt of, compliance with and enforcement of EPOC and EPOC-PR orders
  - those legal representatives:
    - must be staffed with the necessary powers and resources to comply with the orders
    - must **produce the data within the set deadlines**
    - are subject to possible sanctions in case of non-compliance
    - must ensure confidentiality, secrecy and integrity of the data produced and preserved

EPO – the Regulation

- **Execution timeframes**
  - EPOC (art. 10)
    - regular cases: within 10 days upon receipt
    - emergency cases : within 8 hours upon receipt
  - EPOC-PR (art. 11)
    - obligation to preserve the data for 60 days
    - can be extended by an additional 30 days

EPO – the Regulation

- **Grounds for refusal of EPOC orders (art. 8 and 12)**
  - **art. 8: situations in which enforcing States must be notified**
  - **art. 12: grounds for refusal by enforcing States: reasons related to**
    - immunities or privileges under the law of the enforcing State
    - freedom of press and freedom of expression
    - manifest breaches of fundamental rights “in exceptional situations”
    - ne bis in idem

EPO – the Regulation

- **Other provisions**
  - procedure for enforcement when service provider doesn't comply: art. 16
  - review procedure in case of conflicting obligations with third country law: art. 17
  - effective remedies: art. 18
  - art. 32: the use of EIOD or MLA for the gathering of electronic information is still allowed

EPO – the Regulation

- **Admissibility of evidence?**
  - former texts mentioned that evidence obtained in breach of the Regulation would not be admissible before a court
    - no longer mentioned in the Regulation
    - issues of admissibility will have to be solved according national law
- **Criticism of stakeholders**
  - see https://edri.org/wp-content/uploads/2023/06/Joint-Letter-Plenary-Vote-E-evidence-13-June-2023.pdf
    - toothless notification system?
    - poorly designed safeguards regarding professional secrecy and confidentiality?

Thank you!

Let’s connect:

@ joachim.meese@uantwerp.be

in www.linkedin.com/in/joachimmeese/

@JoachimMeese

Co-funded by
the European Union

Handling electronic evidence on mobile devices in court: experiences in Spain

November 23rd, 2024

Andreu Van den Eynde

Mobile Forensics

- Science of retrieving data from a mobile phone under forensically sound conditions
- Almost all digital forensic investigations include a phone
- Need to break encryption mechanisms
- Difficult to preserve original evidence from alteration
- Risk of accidental deletion

Pegasus spyware scandal becomes a ‘full-blown European Union affair’: Report

Edited By: Nishtha Badgamia

Brussels, Belgium • Updated: Nov 09, 2022, 10:19 PM(IST)

Reports suggest that the spyware developed by the Israeli-based company NSO Group, Pegasus, and its less sophisticated version, Predator are some of the most well-known brands in Europe. Photograph:(Reuters)

FOLLOW US

Topics

- Expert witnesses: Public vs. Private
- Private contractors assisting LEAs
- Forensic acquisition methods & secondary victimization
- Future perspectives

Expert witnesses: Public vs. Private

- *Private experts are not trustworthy. They are not impartial because they are paid by one party* (Huelva High Court 01/10/2009).
- *Courts must reason why they choose the public expert conclusions instead of the private expert conclusions. Lack of impartiality of private experts cannot be presumed* (Barcelona High Court 09/03/2016).

Expert witnesses: Public vs. Private

- Citizen Lab is not an admissible expert witness:
  - Lack of forensic standards
  - Protection of know-how
  - No equivalent European lab
- Private computer forensics
  - Not reliable

Expert witnesses

- Specialized
- Experienced and updated
- Using scientific methodology
- Clearly explained coherent conclusions
- Submission to critics and debate
- No conflict of interests

Daubert Standard

Supreme Court #232/2022, March 14th

LEAs and private contractors

- Strong dependency on private forensic tools
- Undisputed findings

Private contractors

- Use of Cellebrite's forensic devices

Forensic acquisition methods

- Manual acquisition
  - Data on screen
- Logical acquisition
  - Extraction of files and directories
- Physical acquisition
  - Bit-by-bit copy (Hex Dump)

Forensic acquisition methods

- Protection of victim’s privacy
- Secondary victimization
- Other fundamental rights involved (lawyer privilege, parliamentary immunities)

Future perspectives

- Need for independent tech labs
- Open-source forensic tools
- Collective dimension of privacy
- Admissibility and reliability judicial standards

Handling electronic evidence on mobile devices in court: experiences in Spain

Andreu Van den Eynde
www.eynde.es
andreu@icab.es
@eyndePenal