ERA
european.law

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

FOCUS ON EXTRACTING EVIDENCE FROM MOBILE DEVICES

Online, 10-11 May 2021
10 May 2021 - 13:00-17:45 CEST
11 May 2021 - 09:15-13:00 CEST

UP GRADE
YOUR LEGAL EXPERTISE

Criminal Law

Professional Training (CPD)
www.era.int

Speakers

Steven David Brown, International Cybercrime Consultant, Vienna

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

Maria Chassirtzoglou, Director, Civil-Criminal Course, Hellenic School of Judges, Thessaloniki

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

Muthupandi Ganesan, Barrister at Law & Partner, Aliant Law, London

Paul Johnstone, Member of the European Judicial Cybercrime Network (EJCN), The Hague; Detective Sergeant, Garda National Cyber Crime Bureau, Dublin

Sapfo Katsanaki, Prosecutor, Prosecutor's Office, Athens

Eneli Laurits, District Prosecutor, Department for Juvenile Crimes, Estonian Prosecutor's Office, Tallinn

Jordy Mullers, Part-time Judge at Zeeland-West Brabant District Court, Legal Advisor at the Criminal Investigations Division of the Dutch National Police, Regional Unit Limburg

Dennis Pielken, Lecturer, Cybercrime & Digital Investigations, Rhineland-Palatinate Police University

Remco Sprooten, Senior Security Consultant, Team Leader, Security Operation Center, ENGIE NL, Amsterdam

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

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
321DT33e

Organisers
ERA (Laviero Buono) in cooperation with the Hellenic National School of the Judiciary

ΕΣΔΙ
NATIONAL SCHOOL OF THE JUDICIARY

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

Monday, 10 May 2021

13:00 Connecting to the videoconference platform and getting familiar with it

13:15 **Welcome and introduction to the programme**
Maria Chassirtzoglou and Laviero Buono

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

Chair: Laviero Buono

13:20 **Internet searches and computer forensics in criminal cases: using open-source intelligence to gather evidence online**
- World Wide Web (WWW) vs. the Internet
- Understanding Internet protocols (http, https, ftp)
- Internet cache – deleting and retrieving
- Surface search vs deep web search
- Meta search engines
- Proxy servers

Dennis Pielken

14:00 Discussion

14:15 **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

Remco Sprooten

14:45 Discussion

15:00 Short break

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

Chair: Laviero Buono

15:15 **Mobile phones: swipe right for evidence**
- Challenges posed by the type and volume of evidence found on a smartphone
- Legal and practical issues surrounding increasing use of Self-Service Kiosks by law enforcement for abstracting phone data
- Comparing and contrasting cell site analysis with GPS systems for locating a phone
- IMSI (International Mobile Subscriber Identity) catchers: their use and concerns about their deployment

Steven David Brown

16:00 Discussion

16:15 **Special investigation techniques when mobile devices are involved**
- Handling mobile devices as sources of evidence
- Common procedures for handling evidence on mobile devices
- Legal issues related to the collection of traffic/subscriber data and its admissibility in court

Paul Johnstone

16:45 Discussion

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 "Obtaining e-evidence when investigating and prosecuting crimes". It consists of six seminars to take place in Dublin, Thessaloniki, Prague, Trier, Cracow and Vilnius.

Who should attend?

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

Interactive online seminar

The online seminar will be hosted on ERA's own online platform. You will be able to interact immediately and directly with our top-level speakers and other participants. We will make the most of the technical tools available to deliver an intensive, interactive experience. As the platform is hosted on our own server, the highest security settings will be applied to ensure that you can participate safely in this high-quality online conference.

CPD

ERA's programmes meet the standard requirements for recognition as Continuing Professional Development (CPD). This event corresponds to **7.5 CPD hours**.

Your contact persons

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

Liz Greenwood
Assistant
Tel.: +49(0)651 9 37 37 322
E-Mail: Egreenwood@era.int

17:00 **The proposed European Production Order (EPO) and its effectiveness in collecting evidence (including evidence stored on mobile devices)**
- Legal framework and problems regarding traditional MLA in the digital age
- The EPO in the online context
- Specificities and challenges of criminal cases where anonymous networks and encrypted files are involved

Jordy Mullers

17:30 Discussion

17:45 End of the first day

Tuesday, 11 May 2021

09:15 Connecting to the videoconference platform

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

09:30 **Special investigation techniques on mobile phones: a new evidentiary frontier for prosecutors**
- Challenges posed by mobile phones
- Proving the authenticity of the data
- Ensuring that the data has not been altered
- Case studies

Rainer Franosch

10:15 Discussion

10:30 **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

Muthupandi Ganesan

11:00 Discussion

11:15 Short break

11:30 **Capturing evidence from the internet and the specificities of dark web investigations**
- Capturing evidence from the internet: open-source and covert
- The importance of the chain of custody in handling the evidence
- Trial considerations: methods of presentation and admissibility tests

Eneli Laurits

12:00 Discussion

12:15 **Handling electronic evidence on mobile devices in court: case studies**
- Proving the authenticity of data resulting from dark web investigations
- Challenges posed by websites and social networks

Sapfo Katsanaki

12:45 Discussion

13:00 End of online seminar

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

Apply online for
"Obtaining e-evidence when investigating and prosecuting crimes":
www.era.int/?130482&en

Save the date

Data Protection and the Law Enforcement Directive
Online, 19-21 May 2021

Annual Conference on EU Border Management 2021
Online, 9-11 June 2021

Artificial Intelligence in Criminal Law and Law Enforcement
Online, 16-18 June 2021

Summer Course on European Criminal Justice
Online, 21-25 June 2021

Specialised e-Courses

Fighting Child Pornography Online: 10 Key Questions
Alisdair Gillespie

www.era.int/elearning

This programme has been produced with the financial support of the Justice Programme 2014-2020 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.

Academy of European Law

Online

10-11 May 2021

Steven David Brown

Swipe Right for Evidence

InZeit

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 Required March 2020 (Europe)

Albania
Andorra
Austria
Belgium
Bulgaria
Cyprus
France
Germany
Greece
Hungary
Italy
Kosovo
Luxembourg
Monaco
Montenegro
Norway
Poland
Russian Federation
San Marino
Slovakia
Spain
Switzerland
Ukraine
(Belarus pending)

InZeit
Excellence in Acuity

https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf

SIM Registration NOT Required March 2020 (Europe)

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

InZeit Excellence in Acuity

https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf

155 Countries globally
… not UK

Heathrow 2019

Two (main) mobile phone systems:

- GSM (Global System for Mobile Technology)
- CDMA (Code Division Multiple Access) – mainly USA

Telecoms companies share their networks (= 'roaming')

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#**)

SIM Card

Authorises phone number on a telecoms network.

May contain

- call history
- contacts and
- received texts

SIM can be switched between different phones

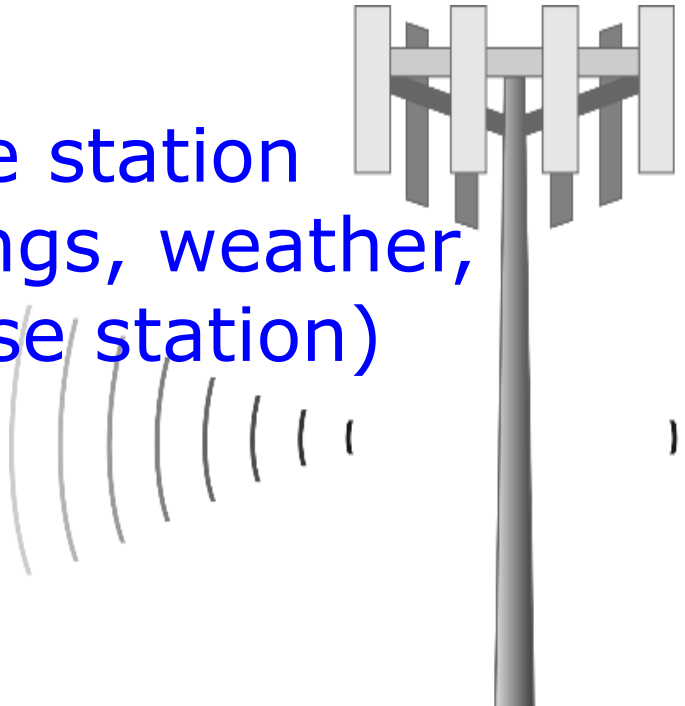
Some modern SIM cards have Secure Element that stores credit card details to allow use as payment device

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

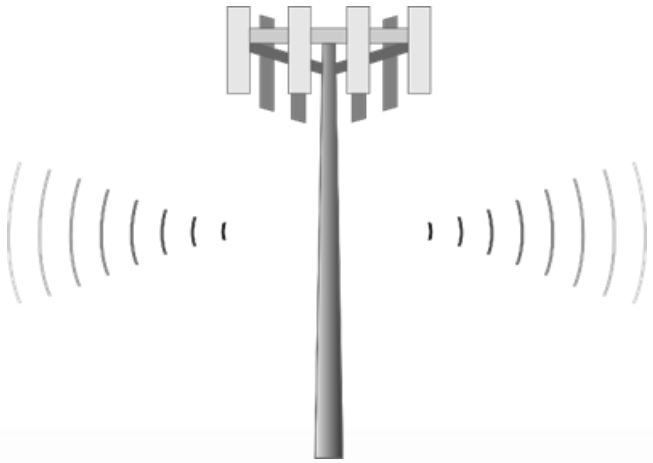
It selects the most powerful base station signal

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.

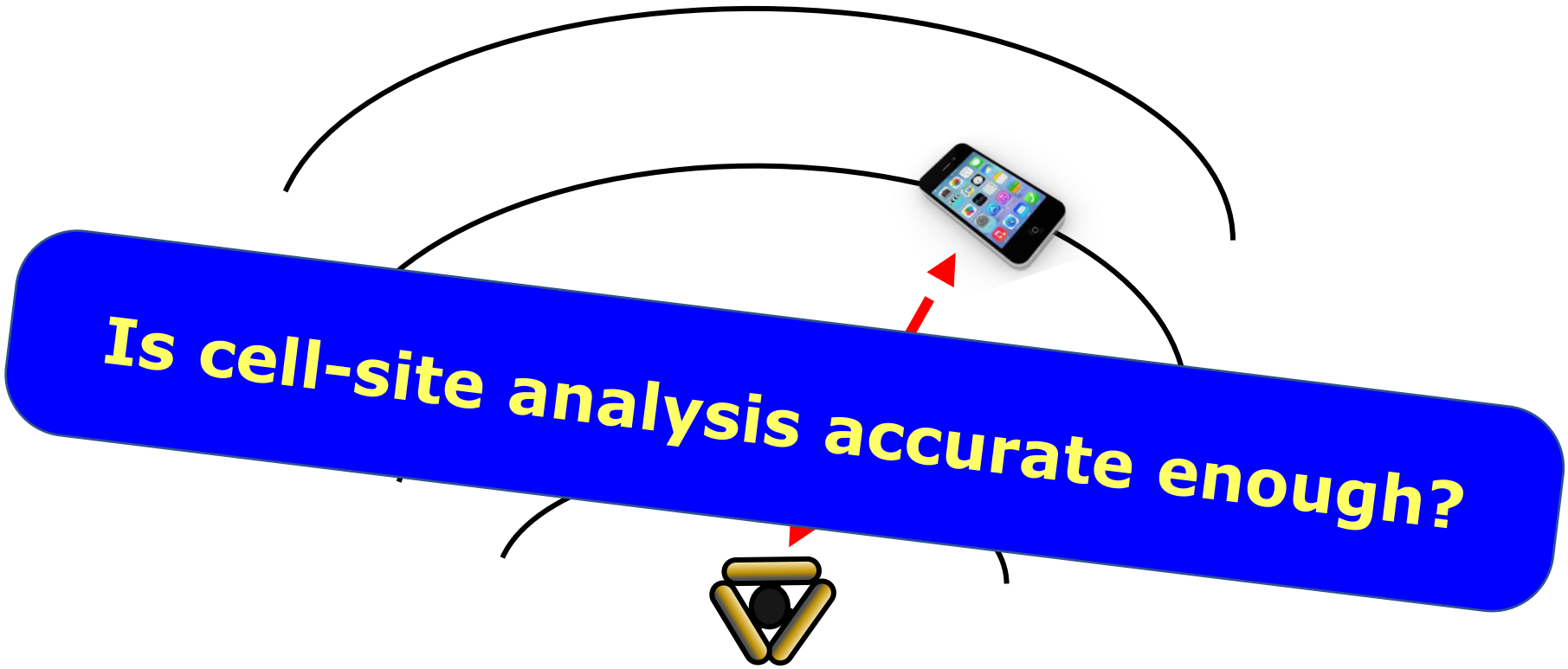
Cell Site Analysis

- 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

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 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

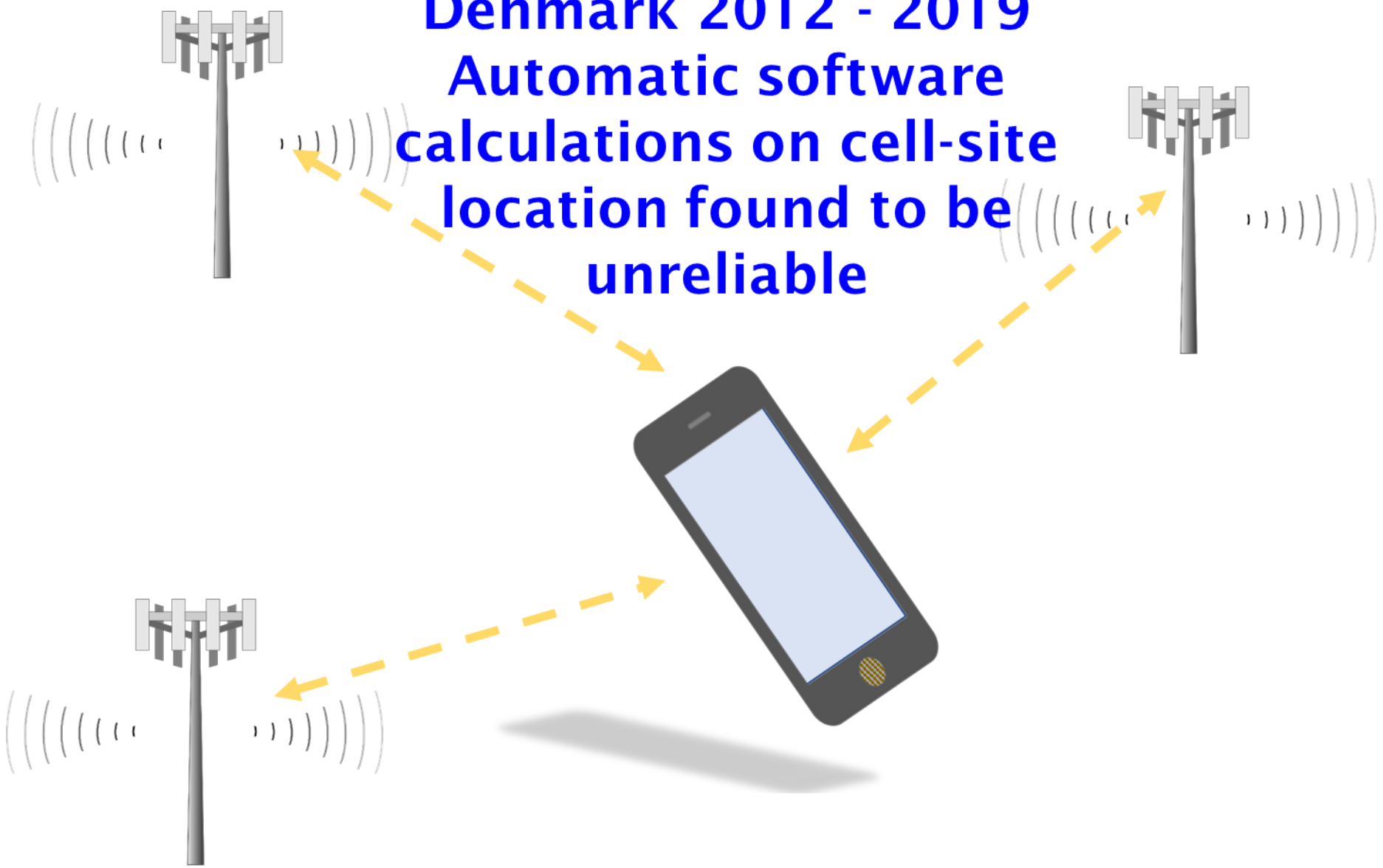
Docket Number	County	Crime	Sentence Type	Begin Date	Termination Date
020834931/01	MULT	MANSLAUGHTER I	Inmate Sentence	12/02/2004	-

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

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



InZeit
Excellence in Acuity

GPS

Global Positioning System (GPS)

Handsets have GPS chip

Network of 30+ satellites 27,000 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)

Location Based Services

- SatNav Driving instructions
- Uber taxi app
- Nearby restaurants
- Where car parked

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

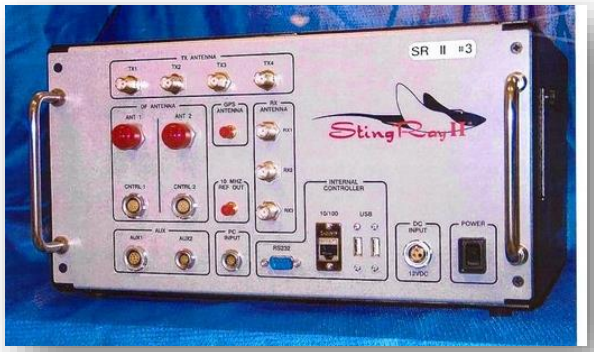
IMSI Catcher
(aka StingRay, Hailstorm, TriggerFish)

Device imitates mobile phone base station

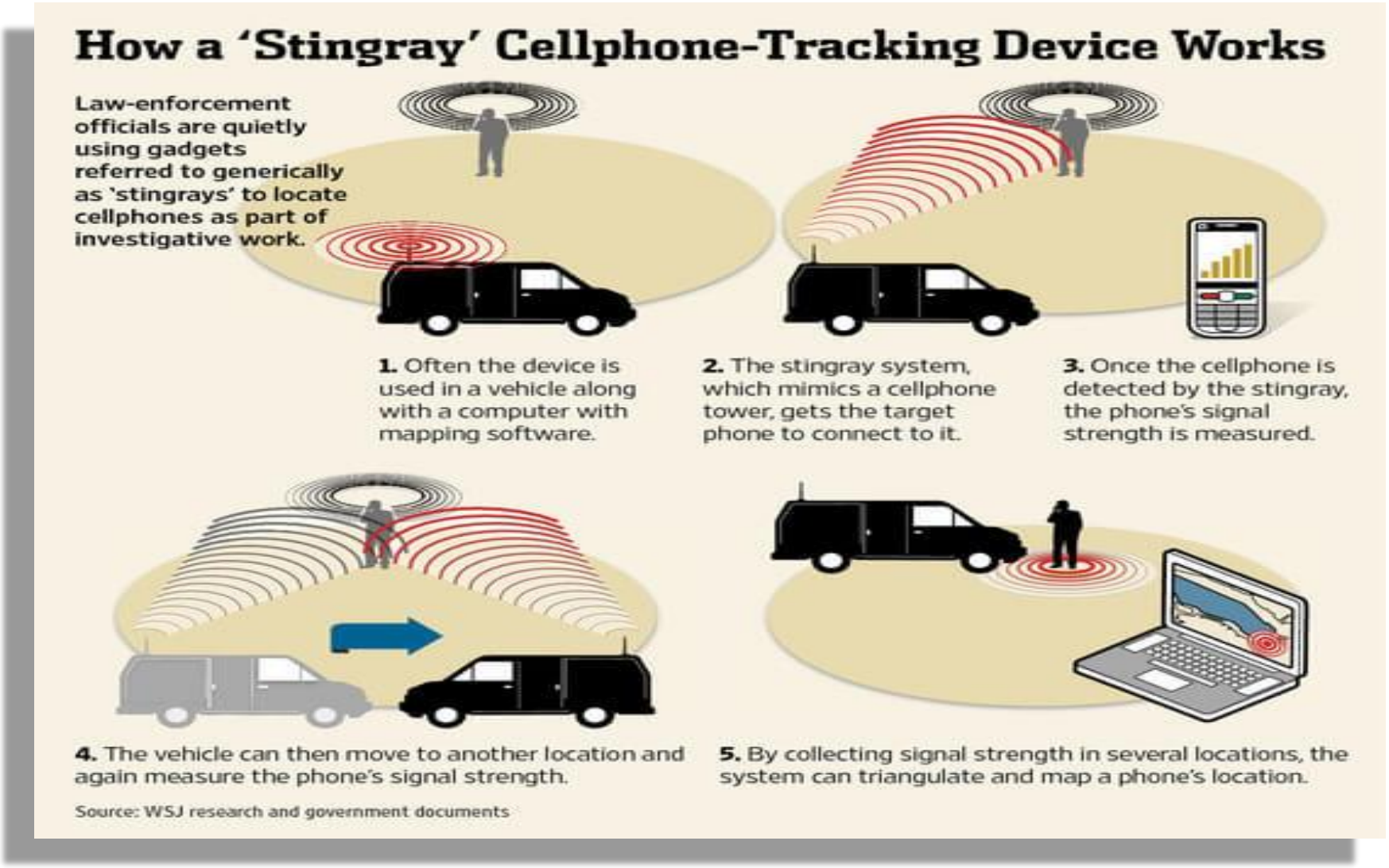
Phone automatically detects & connects to the IMSI catcher

All phone traffic passes through the IMSI catcher

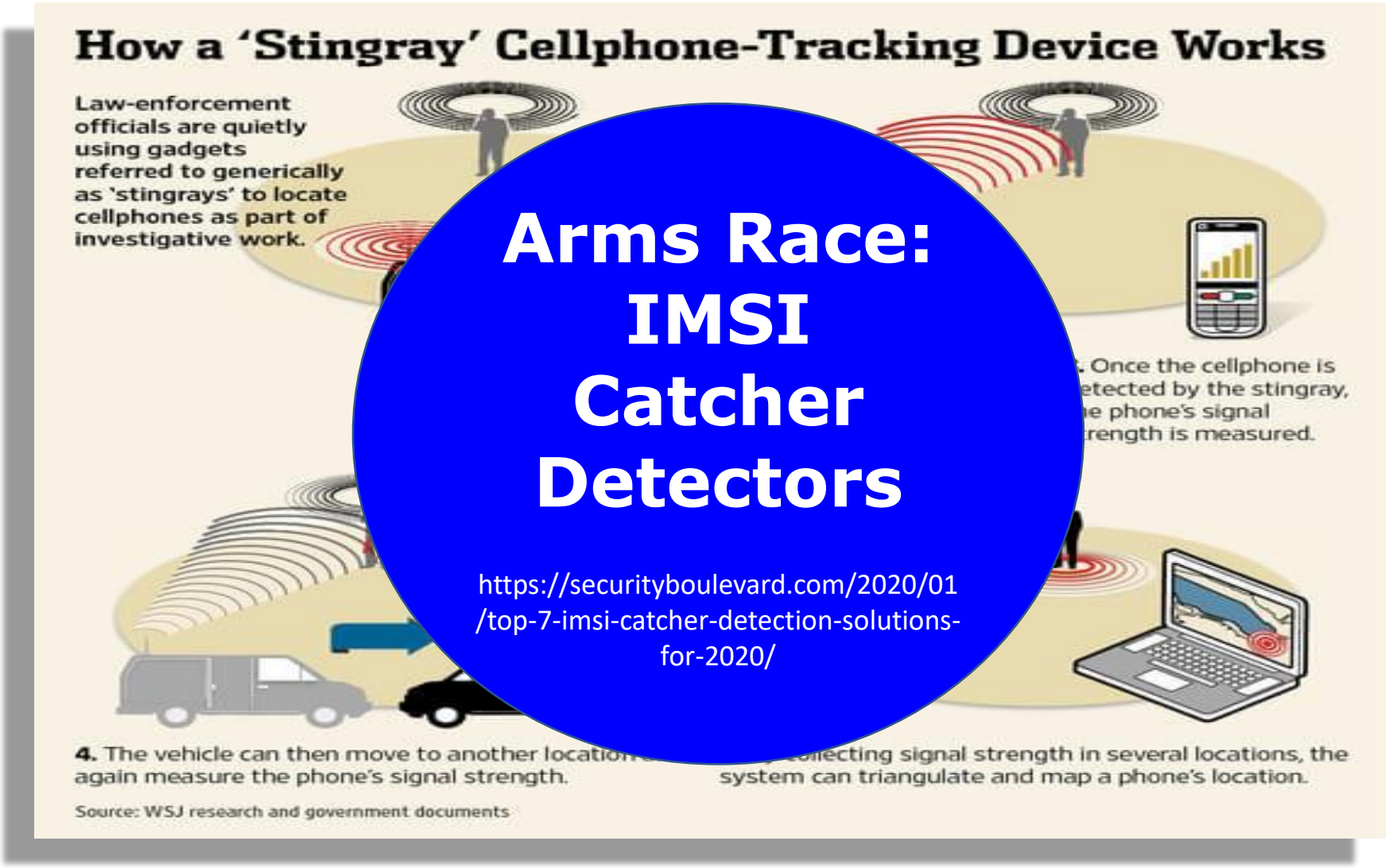
Based on 2G technology, but 3G/4G phones are compatible (3G/4G signal can be disrupted or suppressed)



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



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

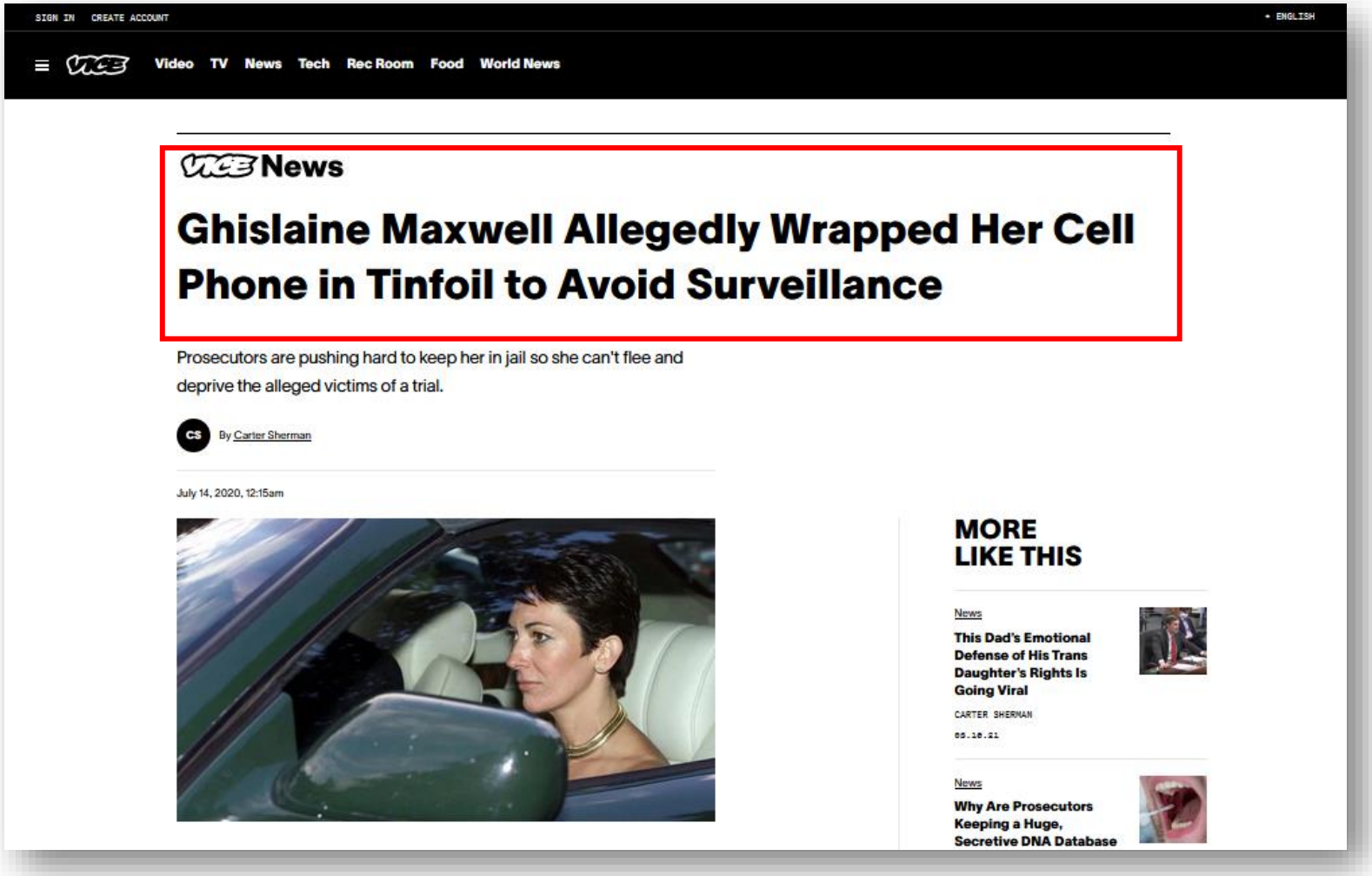
InZeit
Excellence in Acuity

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

UK 2019:
55.5 million smartphone users (82.9%)

Very high probability of phone evidence

Not just suspects …
victims & witnesses

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

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)

Ss19 & 20 Police and Criminal Evidence Act 1984 (PACE) in England & Wales

A constable may seize anything if s/he has reasonable grounds for believing:

- Evidence of an offence
- Obtained from an offence

Prevent loss/concealment/destruction/alteration

The constable may require any information which is stored in any electronic form to be produced in visible/legible form

- Warrant
- Other statutes & common law powers
- By consent

Ss19 & 20 Police and Criminal Evidence Act 1984 (PACE) in England & Wales

A constable may seize anything if s/he has reasonable grounds for believing:

- ...e of an offence
- ...m an offence
- Prev... .../destruction/alteration

The constab... ...rmation which is stored in any electronic fo... ...visible/legible form

- Warrant
- Other statutes & common law powe...
- By consent

Data can only be kept for the purposes of criminal investigation or for use at trial as evidence

InZeit
Excellence in Acuity

3 levels of data extraction of mobile devices (CPS):

Level 1 – Configured Logical Extraction - Digital Forensics Kiosks,

Level 2 – Logical & Physical Extraction - Digital Forensics Hubs or Laboratories or Forensic Service Providers, and

Level 3 – Specialist Extractions & Examinations - Central Digital Forensics Laboratories or Forensic Service Providers.

https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence

Digital Forensics Kiosk (Self Service)

= 'officer operated equipment based within operational police premises.'

Equipment Providers:

XRY (Micro Systemation – MSAB)
Cellebrite – now Japanese owned
(Universal Forensic Extraction Device (UFED))
ACESO (Radio Tactics)

'… preconfigured workflow'

Level 1 mobile device examination provides a "logical" extraction. A "logical" extraction provides the live data that is readily available on device, probably all of the data you could see if you were able to turn on the device and browse through it. A logical extraction will extract the live data that is supported by the extraction software. This could vary by handset, operating system and types of applications. It may not extract all of the data present and will not usually extract deleted material.

https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence

Privacy International complained:

- No independent oversight
  (although the Forensics Science Regulator, IPCC and Courts)
- Lack of national guidance and practice
  (Guidance at local level)
- No warrant required to download phone data (but phone data volatile and easily altered. General power to seize evidence)
- Also captures unrelated personal information and 3rd party information

https://www.privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile

Procedural challenges

(Attempting to balance needs of justice with privacy)

Digital Processing Notice

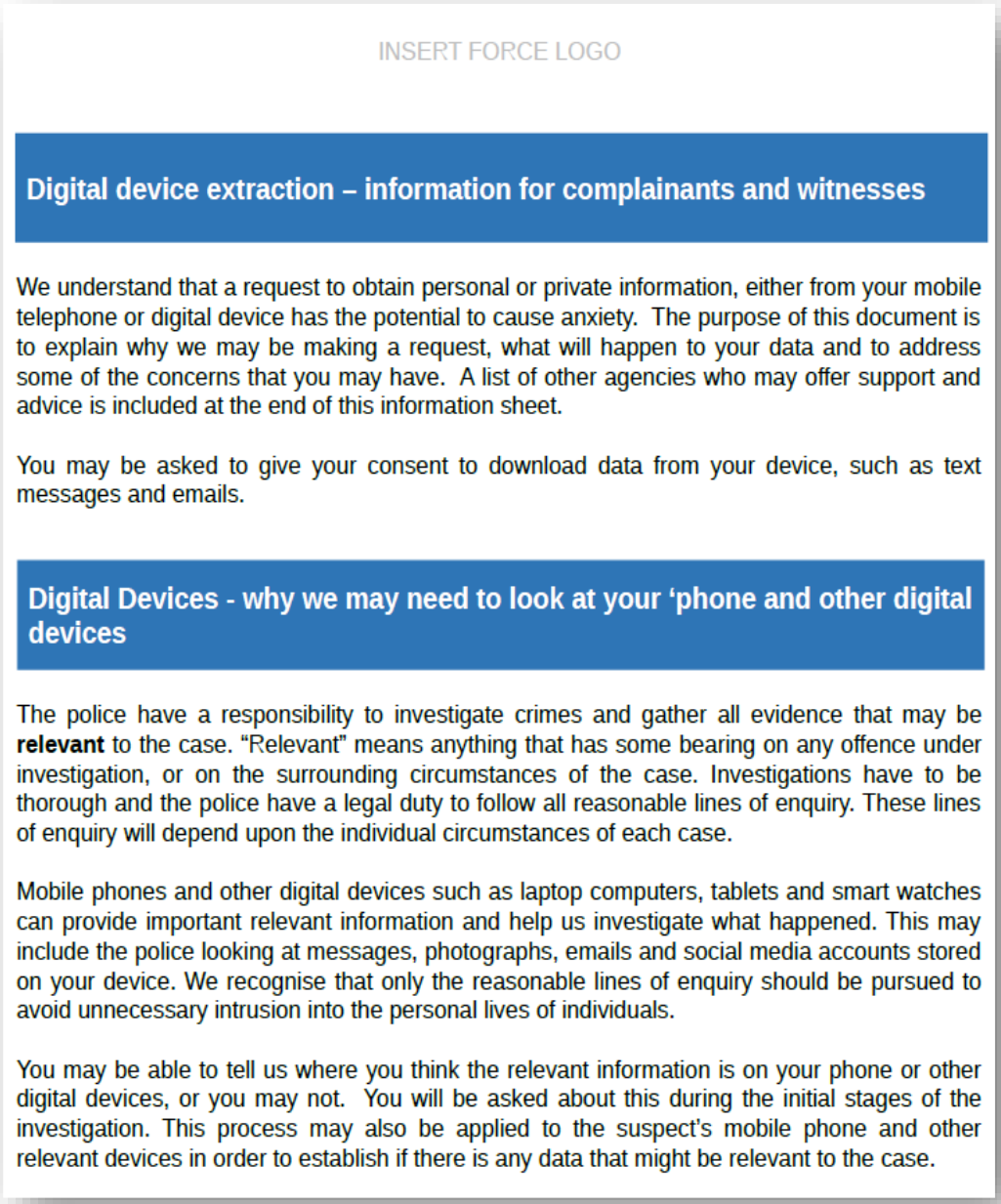
National standard April 2019

"Consent to phone data download or may not proceed"

Some dubbed it: "Digital Strip Search"

Consent forms already standard practice

Concerns that notice could deter victims from reporting



INSERT FORCE LOGO

Digital device extraction – information for complainants and witnesses

We understand that a request to obtain personal or private information, either from your mobile telephone or digital device has the potential to cause anxiety. The purpose of this document is to explain why we may be making a request, what will happen to your data and to address some of the concerns that you may have. A list of other agencies who may offer support and advice is included at the end of this information sheet.

You may be asked to give your consent to download data from your device, such as text messages and emails.

Digital Devices - why we may need to look at your 'phone and other digital devices

The police have a responsibility to investigate crimes and gather all evidence that may be **relevant** to the case. "Relevant" means anything that has some bearing on any offence under investigation, or on the surrounding circumstances of the case. Investigations have to be thorough and the police have a legal duty to follow all reasonable lines of enquiry. These lines of enquiry will depend upon the individual circumstances of each case.

Mobile phones and other digital devices such as laptop computers, tablets and smart watches can provide important relevant information and help us investigate what happened. This may include the police looking at messages, photographs, emails and social media accounts stored on your device. We recognise that only the reasonable lines of enquiry should be pursued to avoid unnecessary intrusion into the personal lives of individuals.

You may be able to tell us where you think the relevant information is on your phone or other digital devices, or you may not. You will be asked about this during the initial stages of the investigation. This process may also be applied to the suspect's mobile phone and other relevant devices in order to establish if there is any data that might be relevant to the case.

InZeit
Excellence in Acuity

[INSERT POLICE FORCE] DIGITAL PROCESSING NOTICE

Crime Reference Number:

The police request your consent to take possession of your mobile phone or other digital device (laptop, iPad etc.) for the purpose of extracting information considered to be relevant to the investigation that you are involved with.

This form describes our data protection and safe storage responsibilities. Separate forms will be used for each device requiring examination. You will be provided with a copy of this form and it will be retained by the police until the conclusion of any related criminal proceedings.

This notice must be served alongside the information document entitled "Digital device extraction – information for complainants and witnesses" which explains the reason the police are requesting your digital devices(s), and how the data extracted may be used.

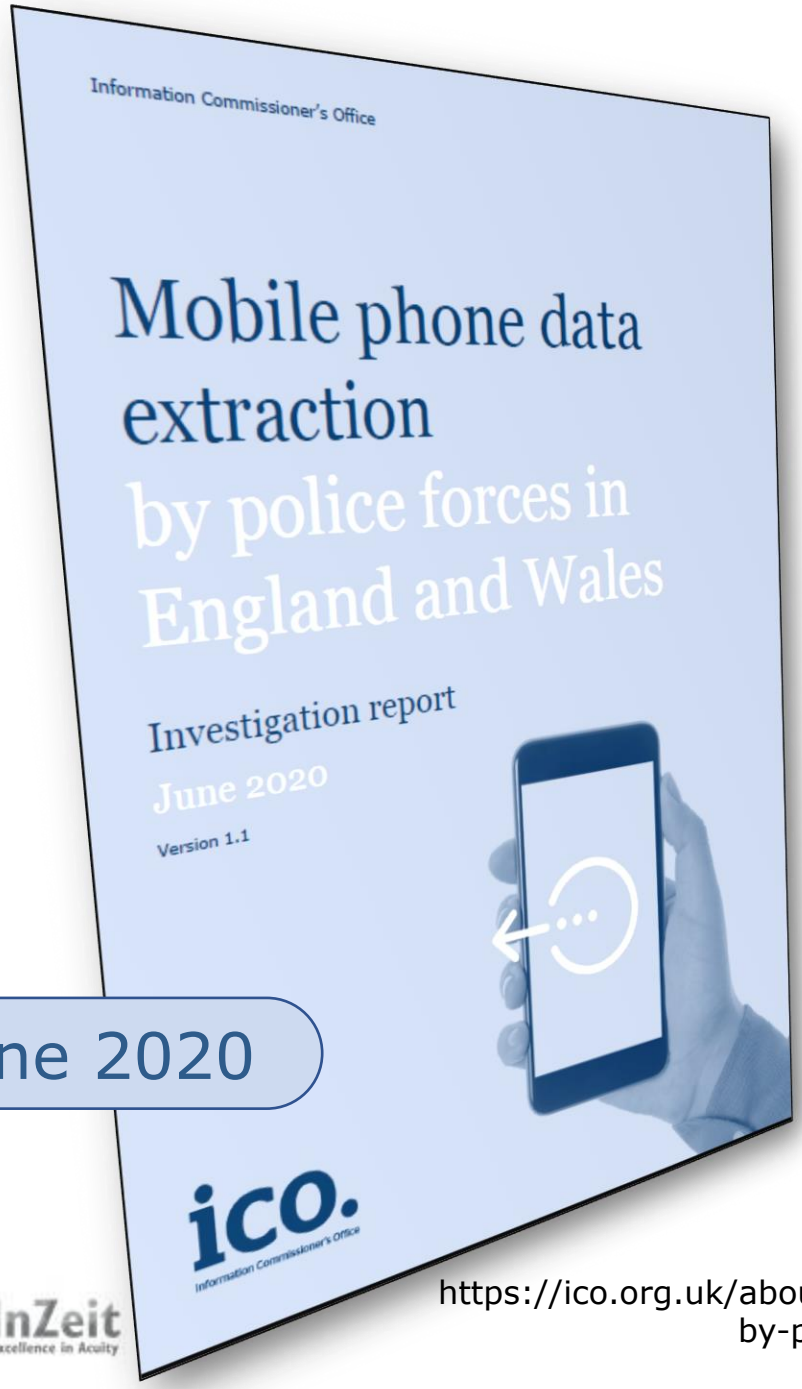
Please contact the investigating officer in your case should you wish to discuss further how we may use your data.

All information recovered in the course of a criminal investigation will be handled, stored and retained securely in accordance with the provisions of the Management of Police Information (MoPI). Further information on MoPI and other approved professional practice information can be found at the College of Policing Website (www.college.police.uk "APP"▸*"Information Management"*).

We also have a duty to retain certain information. The retention period of the data we collect from your device will vary depending upon the severity of the offence investigated.

The officer investigating your case can print out relevant parts of MoPI for you if you have concerns, or email you the link to the appropriate parts of the website. This document can also be emailed with the following links: MoPI 2005

5 May 2019: Police & Crime Commissioners Association (Political Police Oversight Officials) called for consent forms to be withdrawn 'likely to result in loss of confidence'

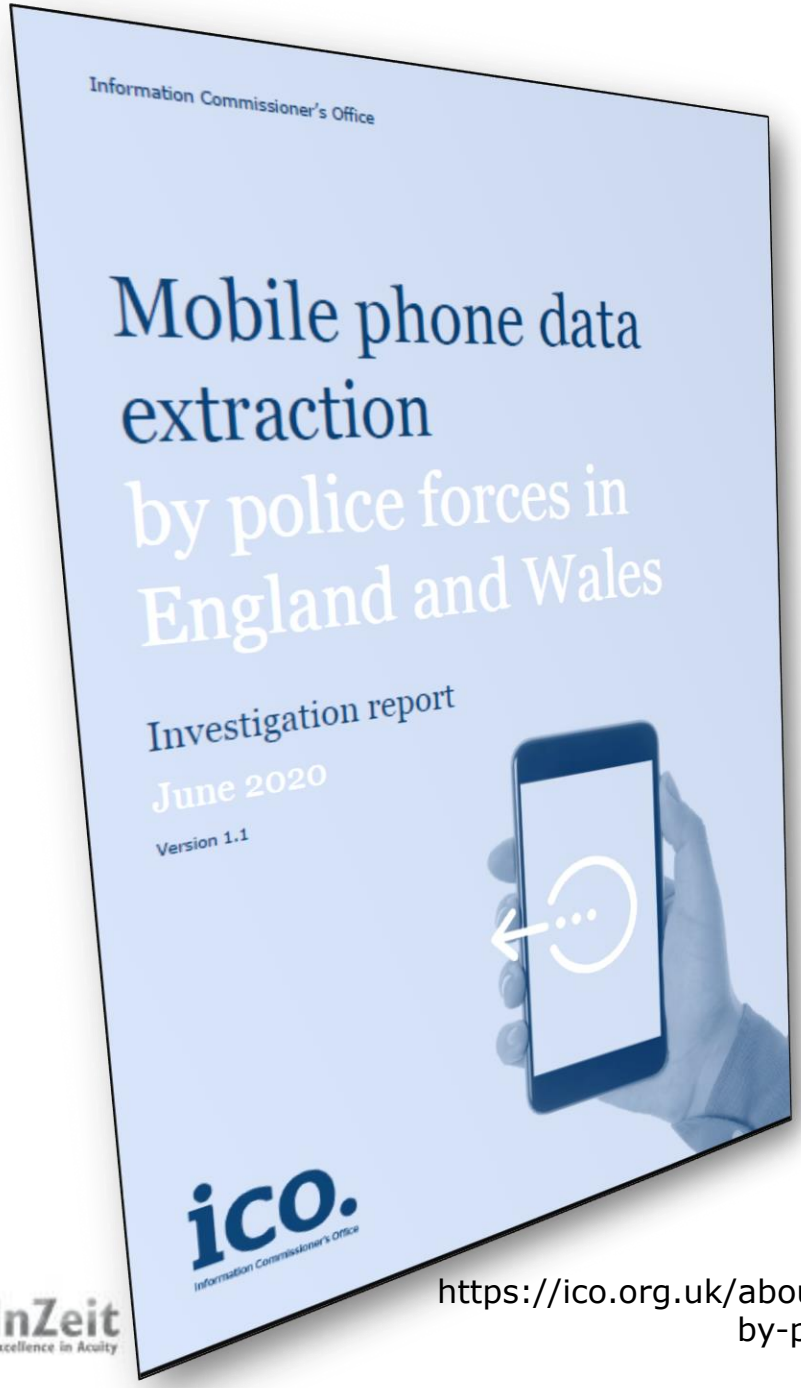


June 2020

Information Commissioner:
"Current mobile phone extraction practices and rules risk negatively affecting public confidence in our criminal justice system […] with excessive amounts of personal data often being extracted, stored, and made available to others, without an appropriate basis in existing data protection law."

https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/

InZeit
Excellence in Acuity



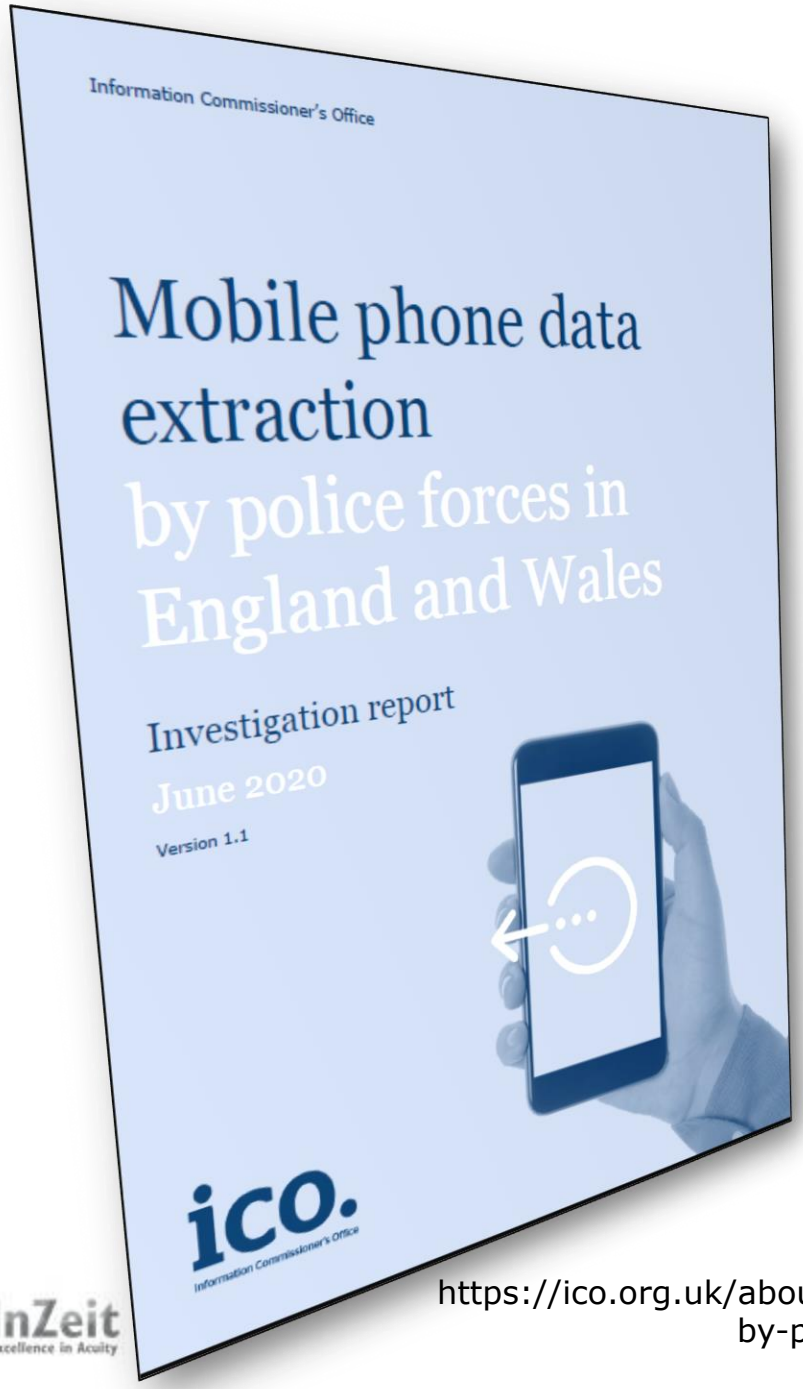
Executive Summary (paraphrasing)

Two conditions for extraction:

1). Consent:- Ensure [witness] has meaningful choice and control over how their data is used.

2). (Where consent not appropriate) only extract where strictly necessary for a law enforcement purpose (not a 'simply coercive option')

https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/



Recommendations:

Consistency in authorising data extracts across England and Wales

Robust policies on handling & deletion of irrelevant, but extracted data

More targeted extraction, further processing and disclosure to minimise intrusion

https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/

Information Commissioner's Office

Mobile phone data extraction by police forces in England and Wales

Investigation report

June 2020

Version 1.1

ico. Information Commissioner's Office

[Insert force logo]

Digital Processing authorisation form (DPNa)

**** To be completed by the officer taking possession of the device. A separate from must be completed for each device. Provide a copy of pages 1 - 3 to the device owner once complete. ****

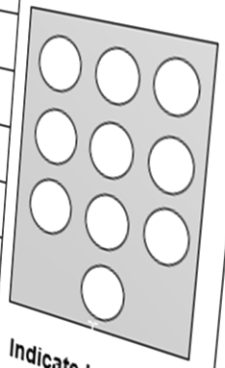
Throughout this form the term 'witness' is used to refer to victims and witnesses

Crime report No:	

OIC Details	
Station / Department / Team	
Name & Shoulder No	

Device Details			
Exhibit Ref			
Telephone No(s)			
Make of Device		Model	
Data Card present	Yes ☐ No ☐	No of Cards	
IMEI No.			
SIM PIN Code			
Alternative Lock Methods	If alternative lock methods are present (i.e. fingerprint or iris) please ask victim/witness to disable these	Device Pass Code	
Description of device condition (i.e. damage or faults, last used)			

Device Pattern Lock



Indicate beginning and end

September 2020

https://news.npcc.police.uk/resources/dpnb-witness-information-sheet

InZeit Excellence in Acuity

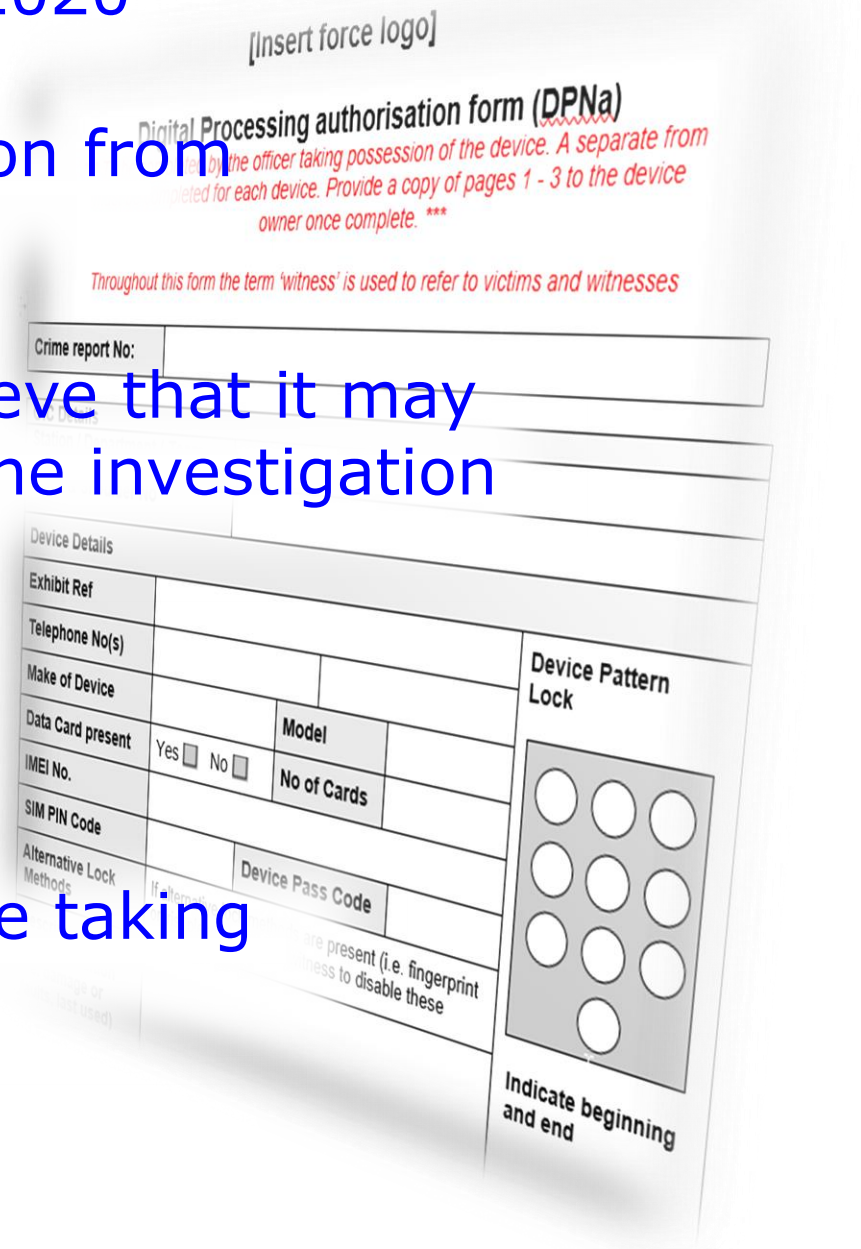
New Advice to Officers Sept 2020

Conditions for data extraction from witness'/victim's device

"Reasonable grounds to believe that it may reveal material relevant to the investigation or the likely issues at trial"

Not ROUTINELY obtained

Agreement of witness before taking possession of device


[insert force logo]

Digital Processing authorisation form (DPNa)

by the officer taking possession of the device. A separate from
leted for each device. Provide a copy of pages 1 - 3 to the device
owner once complete. ***

Throughout this form the term 'witness' is used to refer to victims and witnesses

Crime report No:

Device Details

Exhibit Ref

Telephone No(s)

Make of Device

Model

Data Card present

Yes No

No of Cards

IMEI No.

SIM PIN Code

Alternative Lock Methods

Device Pass Code

present (i.e. fingerprint
ess to disable these

Device Pattern Lock

Indicate beginning and end

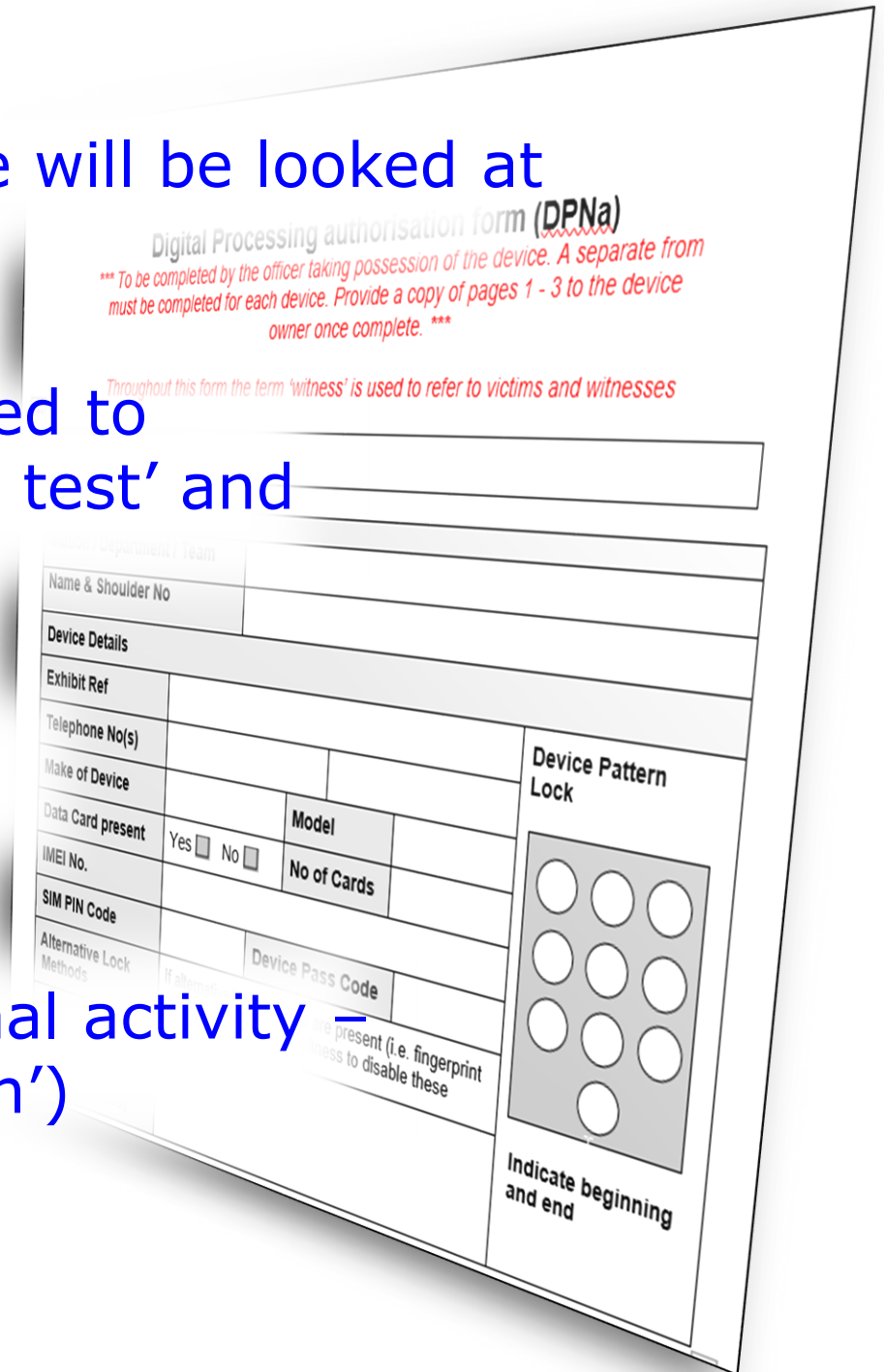
InZeit
Excellence in Acuity

Tell witness:
- which areas of their device will be looked at
- Dates/time-period

Disclosure: Data only provided to defence if 'it meets the strict test' and will be 'suitably redacted'

If witness refuses – take a statement of reasons

(Evidence of unrelated criminal activity – use a 'proportionate approach')


Digital Processing authorisation form (DPNa)

*** To be completed by the officer taking possession of the device. A separate from must be completed for each device. Provide a copy of pages 1 - 3 to the device owner once complete. ***

Throughout this form the term 'witness' is used to refer to victims and witnesses

Name & Shoulder No

Device Details

Exhibit Ref

Telephone No(s)

Make of Device

Model

Data Card present Yes No

No of Cards

IMEI No.

SIM PIN Code

Alternative Lock Methods

Device Pass Code

present (i.e. fingerprint
ess to disable these

Device Pattern Lock

Indicate beginning and end

InZeit
Excellence in Acuity

Home Office

Policy paper

Police, Crime, Sentencing and Courts Bill 2021: data extraction factsheet

Updated 16 April 2021

Contents

Print this page

" Investigators must observe the absolute right to a fair trial and the right to privacy. These considerations apply particularly in the extraction of data from mobile devices, which is increasingly a reasonable line of enquiry in criminal investigations. The proposed legislation would provide to practitioners and stakeholders much needed certainty in respect of the relevant law along with where, when and how it should be applied. This will serve to increase confidence in a critical area of investigative practice. The NPCC therefore supports this Bill."

Tim de Meyer, National Police Chiefs' Council Lead for Disclosure

1. What are we going to do?

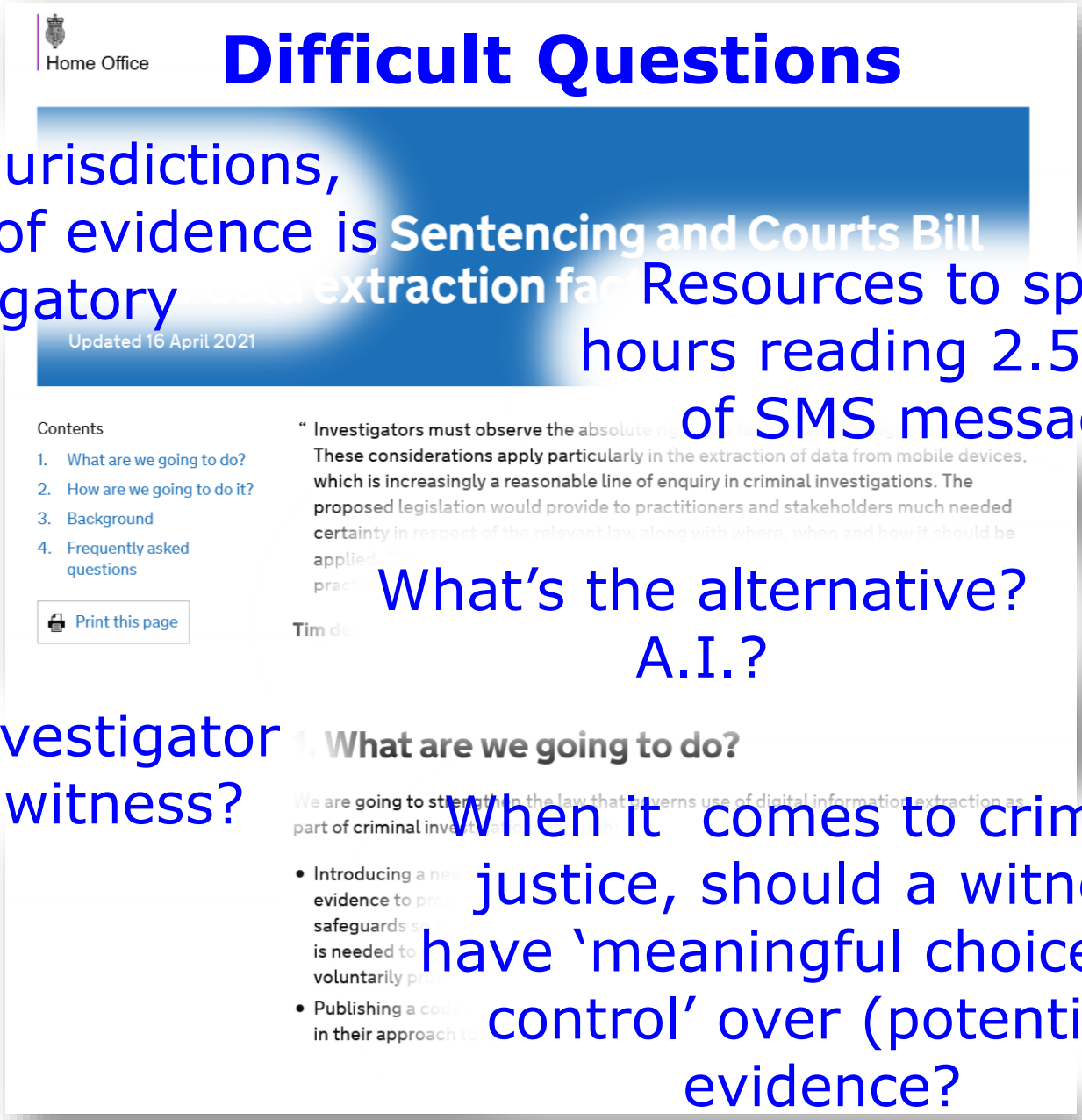
We are going to strengthen the law that governs use of digital information extraction as part of criminal investigations through:

- Introducing a new statutory power to ensure that the police can obtain digital evidence to prosecute criminals whilst strengthening whilst providing additional safeguards so that only information that is relevant to the investigation is taken. This is needed to protect privacy and to support victims of crime and others who voluntarily provide information to the police
- Publishing a code of practice to guide authorities and provide clarity and consistency in their approach to obtaining digital evidence from victims and others.

https://www.gov.uk/government/publications/police-crime-sentencing-and-courts-bill-2021-factsheets/police-crime-sentencing-and-courts-bill-2021-data-extraction-factsheet

Difficult Questions

In some jurisdictions, surrender of evidence is obligatory


Home Office

Sentencing and Courts Bill

extraction fa

Updated 16 April 2021

Contents

1. What are we going to do?
2. How are we going to do it?
3. Background
4. Frequently asked questions

Print this page

" Investigators must observe the absolute
These considerations apply particularly in the extraction of data from mobile devices, which is increasingly a reasonable line of enquiry in criminal investigations. The proposed legislation would provide to practitioners and stakeholders much needed certainty in respect of the relevant law along with where, when and how it should be applied

Tim

1. What are we going to do?

We are going to strengthen the law that governs use of digital information extraction as part of criminal inve

- Introducing a ne evidence to pro safeguards s is needed to voluntarily pr
- Publishing a co in their approach t

Resources to spend 6 hours reading 2.5K pages of SMS messages?

What's the alternative? A.I.?

Can an investigator 'trust' a witness?

When it comes to criminal justice, should a witness have 'meaningful choice and control' over (potential) evidence?

InZeit
Excellence in Acuity

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

Phone Kiosk Issues

Phones contain intimate and confidential material

Can't only extract the 'evidence'

Witnesses view it as invasion of privacy

Risk of incomplete evidential perspective

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

Robust investigation inevitably involves invasive powers (nothing new there)

Is 'consensual' evidence an acceptable basis where criminal justice is concerned?

How long before a miscarriage of justice occurs because the data extraction was incomplete?

Carefully framed codes of conduct and oversight 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

Bowcott,O. (2019*) Rape cases 'could fail' if victims refuse to give police access to phones T*he 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*

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/

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 Informatino 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

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/

HESSEN

Special investigation techniques: A new evidentiary frontier for prosecutors

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

Online seminar
10-11 May 2021

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

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

HESSEN

Encryption is an enabler for OCGs

Welcome to the Evolution

EncroChat is an end-to end security solution, not just another downloadable 'secure' software application.

Individual software applications cannot isolate themselves from other installed software applications, the operating system the device relies on, or the network they connect to. The integrity of the solution is paramount. This includes securing the hardware, operating system, software applications, data transit, network infrastructure and servers. Ignoring any facet of this is devastating and renders the actual security of the product to the level of marketing hype.

EncroChat protects conversations with the following four tenets

- **Perfect Forward Secrecy** Each message session with each contact is encrypted with a different set of keys. If any given key is ever compromised, it will never result in the compromise of previously transmitted messages – or even passive observation of future messages.
- **Repudiable Authentication** Messages do not employ digital signatures that provide third party proofs. However, you are still assured you are messaging with whom you think you are.
- **Deniability** Anyone can forge messages after a conversation is complete to make them look like they came from you. However, during a conversation

The Encrochat investigation

- **GUARANTEED ANONYMITY - No way to associate device or SIM card to customer account**
- **CUSTOMISED ANDROID PLATFORM Fully encrypted from power on. Focus on security and privacy. Simplified user settings.**
- **DUAL OPERATING SYSTEM Subscribers can now launch either a standard Android OS or the EncroChat OS. Two distinctive Operating Systems packaged with each device.**
- **MESSAGING PROTOCOL The electronic equivalent of a regular conversation between two people in an empty room.**
- **MESSAGES THAT SELF-DESTRUCT With our advanced burn a user can force wipe their own messages from another user's device using a timer countdown.**
- **PANIC WIPE From screen lock a user can type in a PIN and instantly wipe device's data.**
- **PASSWORD WIPE After a set amount of password attempts on device all data is wiped.**
- **SECURE BOOT Upon boot, the device internally checks itself to ensure no one has tampered with the system files.**

Hessisches Ministerium der Justiz

The Encrochat investigation

- "EncroChat" was a provider of cell phones on which an app was installed that allowed EncroChat users to send encrypted messages to each other.
- Due to the specifics of the system, the distribution channels, and the high cost of such a device, EncroChat phones were and are believed to be used almost exclusively for conducting criminal business.
- In 2020, a JIT of French and Dutch investigators succeeded in securing messages and images exchanged via the EncroChat server in unencrypted form.

The dismantling of an encrypted phone solution used by organised crime groups

(source: https://www.eurojust.europa.eu/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe)

Interception and analysis of millions of messages exchanged between criminals planning serious criminal acts

This intensive operation informed hundreds of ongoing investigations, providing insights and access to new evidence to tackle international criminal networks involved in drug smuggling, money laundering and other forms of serious and violent crime, including murder, extortion, robbery, grievous assault and hostage taking.

Intensive analysis was undertaken by Europol.

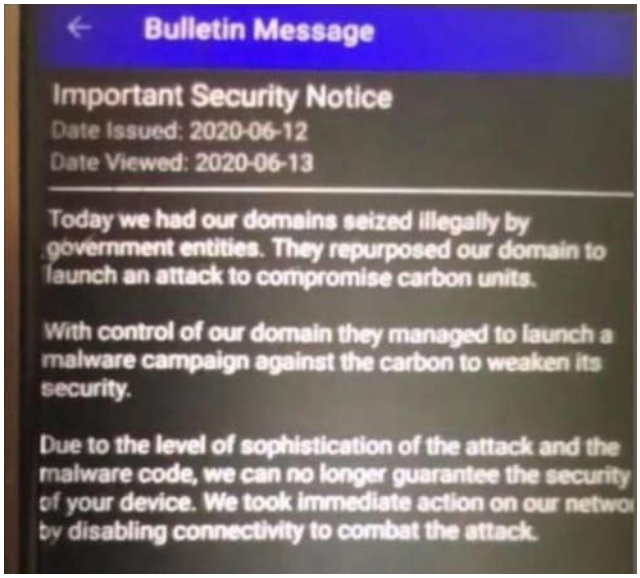
Five coordination meetings were held at Eurojust, with the active participation of national police forces and Europol to ensure smooth communication and coordination between all parties to the JIT. Two of these meetings also involved other countries, including Spain, Sweden, the UK and Norway. **Daily coordination meetings** between involved law enforcement partners were held at Europol.

A **joint investigation team (JIT) agreement** was signed between the national police and judicial authorities of France and the Netherlands in April 2020, supported by the French and Dutch Desks at Eurojust and by Europol.

The case was opened by the French Desk and brought to the Dutch Desk at Eurojust in April 2019.

In 2017, **French police and judicial authorities began investigating** phones using the secured communication tool *EncroChat*, an encrypted phone solution widely used by criminal networks across the globe.

The Encrochat investigation



- During the night of June 12 to 13, 2020, EncroChat issued a security alert to its customers, indicating that the solution was the victim of an "illegal seizure" by "government entities".
- They were advised to physically dispose of their device ("You are advised to power off and physically dispose your device immediatly").

HESSEN

The Encrochat investigation

Hessisches Ministerium der Justiz

HESSEN

The Encrochat investigation

- French investigative authorities have forwarded the data to many states outside the JIT, including Germany.
- In the course of evaluating the data, a large number of proceedings have been initiated throughout Germany or the data have been added to investigations already underway.
- Within these preliminary proceedings, the defense often doubts the admissibility of the data.

HESSEN

Legal issues

- Different legislations have different rules on wiretapping / interception of telecommunications.
- In international transborder investigations, e.g. under the rules of an (EU) JIT, there might be legal options to share information gained through the interception of a telecommunication.
- Interception of TC vs. hidden search of the suspects data stored on mobile device: legal?
- Were the communications intercepted while they were being transmitted or while they were being stored in or by the system?

HESSEN

Legal issues regarding cross border exchange of data

COUNCIL FRAMEWORK DECISION 2006/960/JHA

of 18 December 2006

Article 7

Spontaneous exchange of information and intelligence

1. Without prejudice to Article 10, the competent law enforcement authorities shall, without any prior request being necessary, provide to the competent law enforcement authorities of other Member States concerned information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences referred to in Article 2(2) of Framework Decision 2002/584/JHA. The modalities of such spontaneous exchange shall be regulated by the national law of the Member States providing the information.

2. The provision of information and intelligence shall be limited to what is deemed relevant and necessary for the successful detection, prevention or investigation of the crime or criminal activity in question.

HESSEN

Best practices

- Promoting effective cooperation, coordination, mutual legal assistance, and communication with relevant actors
- Allowing, where possible, alternatives to formal requests for mutual legal assistance
- Developing mechanisms for parallel or joint investigations
- Preserving the chain of custody and respecting the integrity of the criminal proceedings

HESSEN

Handling Codes - Example

SIENA H3 handling code for exchange of data within Eurojust case

The provided data may be disclosed related to the XY investigations of the following countries:

Without prior permission from the providing authority you are not allowed to share this data with any other country.

In case the provided data leads to any entity in and/or link to the providing country, the providing authority would like to be informed as soon as possible.

The provided data can only be used for the purpose of the XY-investigations in the stated countries.

Upon finalization of the cases related to the XY-investigations, the provided data has to be destroyed at the earliest moment possible according to national law of the respective country, e. g. when the statute of limitations for criminal prosecution has come into effect or a conviction is final.

HESSEN

Considerations for Electronic Evidence

Admissibility: Since the ultimate goal is the use of acquired and analysed evidence to support a case in court, electronic evidence must be obtained in compliance with existing legislation and best practice procedure to be admissible in a trial. Although the details differ depending on national legislation, the following basic criteria must generally be taken into account.

Hessisches Ministerium der Justiz

HESSEN

Considerations for Electronic Evidence

Authenticity: It must be possible to positively tie evidentiary material to the investigated incident.

Completeness: It must tell the whole story and not just a particular perspective.

Reliability: There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity.

HESSEN

Considerations for Electronic Evidence

Believability: It must be readily believable and understandable to a judge and/or the members of a jury.

Proportionality: its application to Digital Forensics establishes that the whole investigative process must be adequate and appropriate: the benefits that are to be gained by using a specific measure must outweigh the harms for the party or parties affected by the measure.

BELIEVABILITY MATTERS

HESSEN

Expert Witness

- Technical ability
- Industry background
- Excellent teaming ability
- Excellent communication skills

HESSEN

Presentation in Courtroom

- Establishing the link between “digital” and “human” domains (attribution):

  No fingerprints or DNA in cyberspace

- Presentation of “technology” to the jury and judge:

  Technical terms only if necessary

- *Make the crime real*

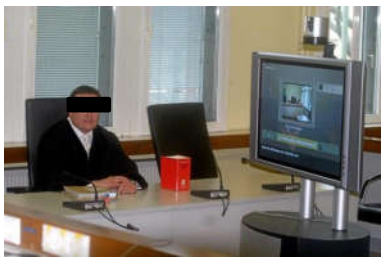
Hessisches Ministerium der Justiz

HESSEN

Presentation in Courtroom

- Presentation of electronic evidence to the court is more effective if it is visual.
- Research has found that many people give more attention to what they see rather than hear.
- Since a prosecutor’s duty is to put forward the prosecution case in the best possible light, visual presentation of evidence especially in complicated cases is advisable.

  .
- Presentation of electronic evidence to the court is more effective if it is visual, using projector devices, PowerPoint presentations, video demonstrations, computer graphics and flipcharts.



HESSEN

Presentation in Courtroom

- Get the court's permission in advance for your electronic presentation.
- Try to get a feeling for the judge's concerns about the technology and adapt accordingly.
- Don't overdo the technological presentation.
- Be sure that the technology is working, visit the courtroom site in advance of the proceedings and check!

HESSEN

Thank you for your attention!
Questions? Remarks?

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

HANDLING ELECTRONIC EVIDENCE ON MOBILE DEVICES: DEFENCE PERSPECTIVE

EUROPEAN ACADEMY OF LAW

11 May 2021

MUTHUPANDI GANESAN

BARRISTER

ALIANT LAW

ALIANT
An International Law Firm

This presentation will cover:

- Capturing evidence from the mobile devices
- Importance of chain custody in handling the evidence
- Trial considerations: methods of presentation and admissibility test

UK - Legislations

- Human Rights Act 1998
- Data Protection Act 2018
- Computer Misuse Act 1990
- Investigatory Powers Act 2016
- RIPA 2000
- Police Act 1997

NPCC Guidance on Open Source Investigation / Research

ACPO – Good Practice Guide for Digital Evidence – March 2012

ACPO - Good practice Guide for Computer-Based Electronic Evidence (v4.0)

General principles

The general principles to be followed by investigators in handling and examining digital material are:

(i) No action taken by investigators or their agents should change data held on a computer or storage media which may subsequently be relied upon in court;

(ii) In circumstances where a person finds it necessary to access original data held on computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions;

(iii) An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes (see further the sections headed Record keeping and Scheduling below); and,

(iv) d. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are followed.

(Attorney General's Guidelines on Disclosure: For investigators, prosecutors and defence practitioners – December 2013 but updated March 2018)

Digital evidence : International Issues

59.The obligations under the CPIA Code to pursue all reasonable lines of enquiry apply to material held overseas.

60.Where it appears that there is relevant material, the prosecutor must take reasonable steps to obtain it, either informally or making use of the powers contained in the Crime (International Co-operation) Act 2003 and any EU and international conventions. See CPS Guidance 'Obtaining Evidence and Information from Abroad'.

UK Guidance

- CPS Guidance 'Obtaining Evidence and Information from Abroad
- Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice
- MUTUAL LEGAL ASSISTANCE
- EXTRADITION

TYPE OF EVIDENCE

PERSONAL FAMILY & FRIENDS

PRIVATE MEDICAL

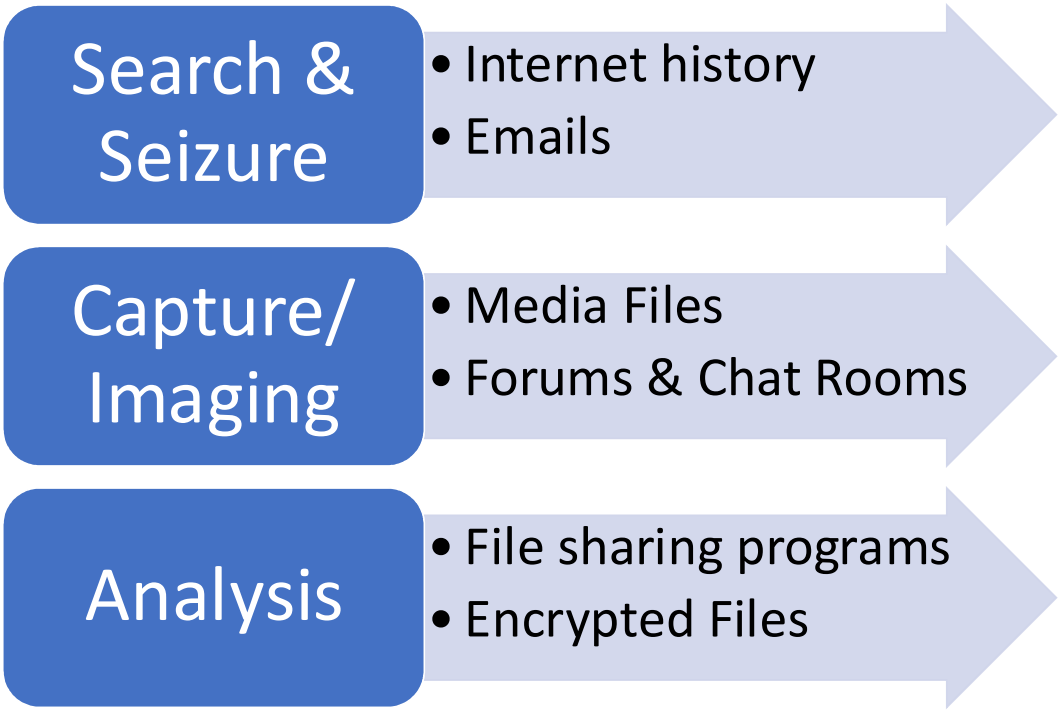
HEALTH, NUTRITION

FINANCIAL

DATA: MOVEMENT, HOBBIES, ROUTINE

EDUCATION

INTERNET, APPS, GAMES


Search & Seizure
• Internet history
• Emails
Capture/ Imaging
• Media Files
• Forums & Chat Rooms
Analysis
• File sharing programs
• Encrypted Files


Witness statements
Reports
Expert Evidence

TRIAL CONSIDERATOINS: PRESENATION & ADMISSIBILITY

1. VOLUME OF DATA
2. FUNDING
3. EQUIPMENT
4. TRAINNING – FOR JUDGES, PROSECUTORS, DEFENCE LAWYERS AND CLIENTS
5. NATURE OF EVIDNECE: CCTV, TEXT MESSAGES, SOCIAL NETWORKING EXCHANGES OF DATA, WHATSAPP MESSAGES

DISCLOSURE: QUALITY OF KNOWLEDGE : JUDGE V JURY

- SECURITY & AUTHENTICITY OF DATA
- ACCURACY
- CONTINUITY
- TELEPHONE DATA / TELEPHONE MAST DATA
- PRESENTATION OF DATA TO THE JURY

https://www.telegraph.co.uk/news/2018/06/05/almost-50-court-cases-dropped-six-weeks-issues-disclosure-cps/

Almost 50 court cases dropped in six weeks because of issues with disclosure, CPS reveals

share
Save

Almost 50 court cases dropped in six weeks because of issues with disclosure, CPS reveals (stock image) CREDIT: ARNE DEDERT/EPA

MORE STORIES

1 Danny John-Jules's Strictly exit is nothing to do with bullying, and everything to do with skin...

2 Jeremy Corbyn criticised for wearing 'scruffy' anorak to Armistice Day service

3 Theresa May's Brexit choices are now tactical, not technical

4 What your heart rate is really trying to tell you

Nearly 50 rape, sex assault cases halted after mass disclosure failings discovered by police, DPP

Published time: 6 Jun, 2018 09:48
Edited time: 7 Jun, 2018 07:09
Get short URL

© Erika Kyte © Getty Images

to defense lawyers. As a result, the Director of Public Prosecutions has been slammed by MPs.

DPP Alison Saunders attended the Commons Justice Committee on Tuesday, facing off with MPs who accused her of failing to take action within the prosecutor's service.

Read more

'I'm going to ruin his life lol': Teen 'rapist' latest victim of police disclosure failings

Saunders said the prosecution's failure to disclose evidence in sex crime cases – including a case that nearly saw an innocent man, Liam Allan, jailed on 12 counts of rape and sexual assault after falling victim to a vexatious ex-girlfriend – admitted that the problem was systemic and due to *"cultural failings."*

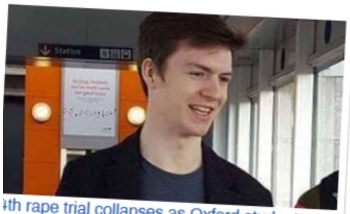
She admitted that such failings had *"been there for a long time,"* but said that she has now *"accepted… that [scrutiny of disclosure] has been frankly too late in the process. It is about doing this as early as possible."*

DPP Saunders was accused of failing to take adequate action by MPs on the Commons Justice Committee yesterday. Saunders hit back, telling the committee that she doesn't *"think it was inadequate."* She added: *"I think there were lots of improvements."*

The Crown Prosecutors Service reviewed 3,637 cases across England and Wales that were live between January and mid-February. The CPS identified disclosure failings in 47 cases, all of which were halted. In five of those cases, issues with disclosure of evidence was the primary reason.

In the other 42 cases, there were additional reasons including communications data like text messages, emails, and social media being examined too late; a failure to get material from third parties such as medical or social services records; or new evidence emerging.

Read more



th rape trial collapses as Oxford student leared of charges before trial

A total of 14 defendants were in custody when their cases were dropped due to the disclosure failings.

In response to questions from Chairman of the Committee Bob Neill, Saunders accepted that the DPP's failings were upsetting. Neill said that *"disclosure has been a blight for too long"* and as a result of the disclosure failings, people like Liam Allan could be wrongfully jailed.

"I feel every single failure, it is not something that we want," Saunders said, adding: *"I believe that the initiatives we have put in place will make a difference."*

The initiatives in question will include training for all 3,000 prosecutors in England and Wales, speeding up the process so that disclosure takes place much sooner and is reviewed regularly. Disclosure *"champions"* will also be placed in all crown and

EXPERT EVIDENCE IN DIGITAL / CLOUD COMPUTING

- It should always be kept in mind that expert evidence is merely one tool to be used in proving a case. The danger in placing too much reliance on the findings of experts is demonstrated in a series of cases in relation to DNA analysis, where there was no other evidence against the accused save the presence of his DNA found at the scene of a crime. The Court of Appeal has emphasised that expert evidence can only be judged in the light of the other evidence in the case. In these cases, the absence of any other evidence, however limited, should have been fatal to the case being charged - see
- The dangers of an over-reliance on expert evidence without considering the significance of the other evidence in the case is a factor that prosecutors need to consider in reviewing any file presented by the police for advice and review.

EXPERT WITNESS

Section 30 of the Criminal Justice Act 1988 & Criminal Procedure Rules – Part 33

1. Assistance to the Court
2. Relevant Expertise
3. Impartial
4. Evidence is reliable

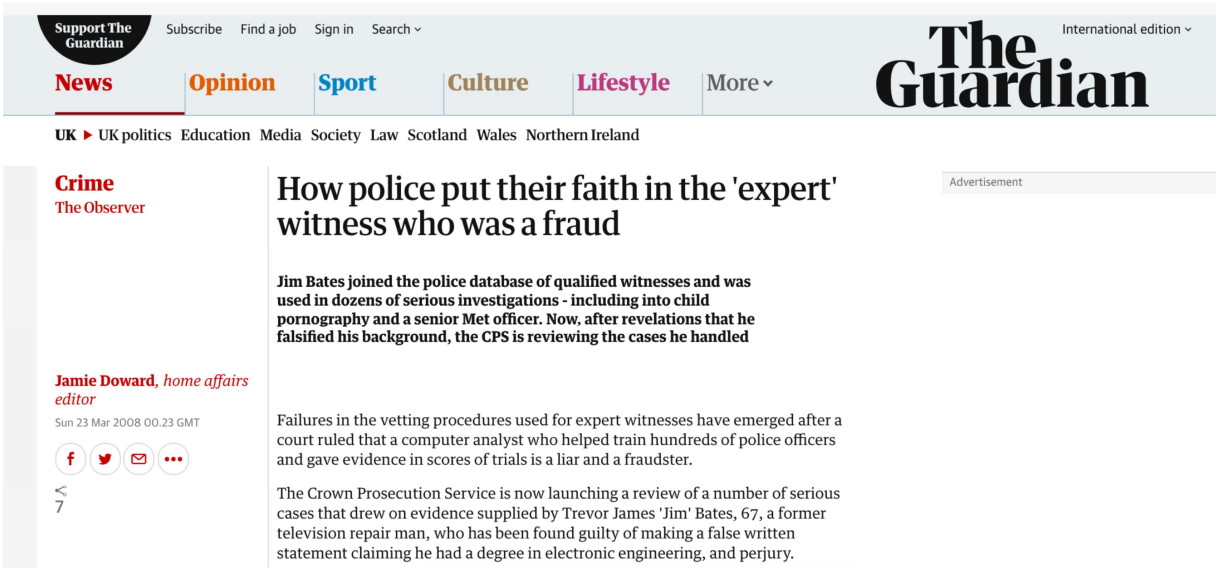
Definition of Expert Witness: An expert witness is a witness who provides to the court a statement of opinion on any admissible matter calling for expertise by the witness and is qualified to give such an opinion.

The Duty of an Expert Witness: The duty of an expert witness is to provide independent assistance to the court by way of objective, unbiased opinion in relation to matters within their expertise. This is a duty that is owed to the court and overrides any obligation to the party from whom the expert is receiving instructions - see R v Harris and others [2005] EWCA Crim.1980.

Expert evidence: Challenges

1. By an application to the judge (on a voir dire or at a case management hearing) to exclude expert evidence that is biased, unhelpful or unreliable evidence under section 78 PACE and R v Turner (1975) 60 Cr. App R. 80;
2. By an application to the judge to exclude expert evidence due to noncompliance with Criminal Procedure Rules;
3. By requesting that evidence be edited to remove comment on matters outside of expert's experience, or amended where conclusions are overstated;
4. By requesting the preparation of a joint expert's report may result in reports being amended to more accurately reflect the underlying science; or •
5. By testing the expert's hypothesis in cross examination to ensure it has been the subject of sufficient scrutiny and peer reviews. For example, in drink driving cases, where defence experts produce new and unproven claims about breath test machines suffering from "long blow" or "long purge". There is no accepted legal basis for either claim.

Expert evidence: expertise must be reviewed carefully!



Support The Guardian Subscribe Find a job Sign in Search International edition

The Guardian

News Opinion Sport Culture Lifestyle More

UK ▸ UK politics Education Media Society Law Scotland Wales Northern Ireland

Crime
The Observer

How police put their faith in the 'expert' witness who was a fraud

Jim Bates joined the police database of qualified witnesses and was used in dozens of serious investigations - including into child pornography and a senior Met officer. Now, after revelations that he falsified his background, the CPS is reviewing the cases he handled

Jamie Doward, *home affairs editor*

Sun 23 Mar 2008 00.23 GMT

< 7

Failures in the vetting procedures used for expert witnesses have emerged after a court ruled that a computer analyst who helped train hundreds of police officers and gave evidence in scores of trials is a liar and a fraudster.

The Crown Prosecution Service is now launching a review of a number of serious cases that drew on evidence supplied by Trevor James 'Jim' Bates, 67, a former television repair man, who has been found guilty of making a false written statement claiming he had a degree in electronic engineering, and perjury.

Advertisement

Muthupandi Ganesan
Barrister

Aliant Law
10 Lower Thames Street
London, EC3R 6AF
England, UK
E-mail: mganesan@aliantlaw.com

Tel: +447837450397

ALIANT
An International Law Firm

ERA Seminar on E-Evidence - Thessaloniki

10-11 May 2021

Mobile Devices – Investigation Techniques

Detective Sergeant Paul Johnstone

Garda National Cyber Crime Bureau, Dublin

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

1

Some Statistics

- 5.11bn mobile owners
- 2.86bn smartphone owners
- 94% of 18-30s have smartphones
- 70% internet traffic
- 79% of usage is Apps
- Most mobile Apps offer encryption

2

Computer in your Pocket

- **Email**
- **Social media**
- **Photographs & video**
- **Mapping & location**
- **Calendar & diary**
- **Internet access**

…

- And a phone

3

Connections from your Pocket

- **Cellular network**
- **Wi-Fi Networks**
- **Local network**
- **Hotspots**
- **Bluetooth**

…

- Same as other computers

4

The Evidence in your Pocket

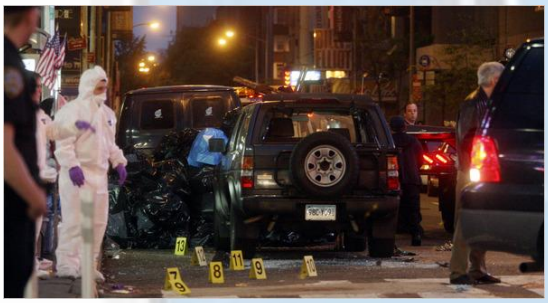
- **CEM** – images and videos
- **Exploitation/Harassment** – social media content
- **Frauds** – emails and banking details
- **Hacking** – Internet history and software tools
- **Usage** – Applications/Users/messages
- **Personal** – GEO data/documents/to do list/diary/call logs/cell site analysis
- **Owner** – IMEI/IP address/Cell number

- **Preferred offender devices** – secure/portable/disposable

5

Mobile Devices – The Importance

NYC Times Square - 2010



DPP v Graham Dwyer - 2015

6

Pre Exam Procedures

- Faraday Bag
- Keep On
- Note PIN/code
- Airplane Mode

Exam Procedures

- Seizure
- Secure
- Acquire *(not imaging)*
- *Clone (Mulready Woods)*
- Analyse

Tools

- Cellebrite®
- Blackbag®
- Axiom®
- Belkasoft®
- Elcomsoft®
- XRY®
- Linux dd copy

7

Technical Challenges….some

- Hardware differences
- Operating systems - evolution
- Encryption & security features
- Resources
- Always On
- Remote Access/Wipe
- Passcodes
- Legal Issues

8

Legal Challenges…some

- Data Retention directive
- Dwyer v Ireland & Ors
- Tele Sverige
- Digital Rights Ireland

- Privacy v Protection
- Expect More

9

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

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

Sapfo Katsanaki
Deputy prosecutor
Public Prosecutor´s Office to the Athens Court of First Instance
LLM IT Law (London)
LLM Penal Sciences (Athens)

Thessaloniki, 11 May 2021

1

Why e-evidence is so important?

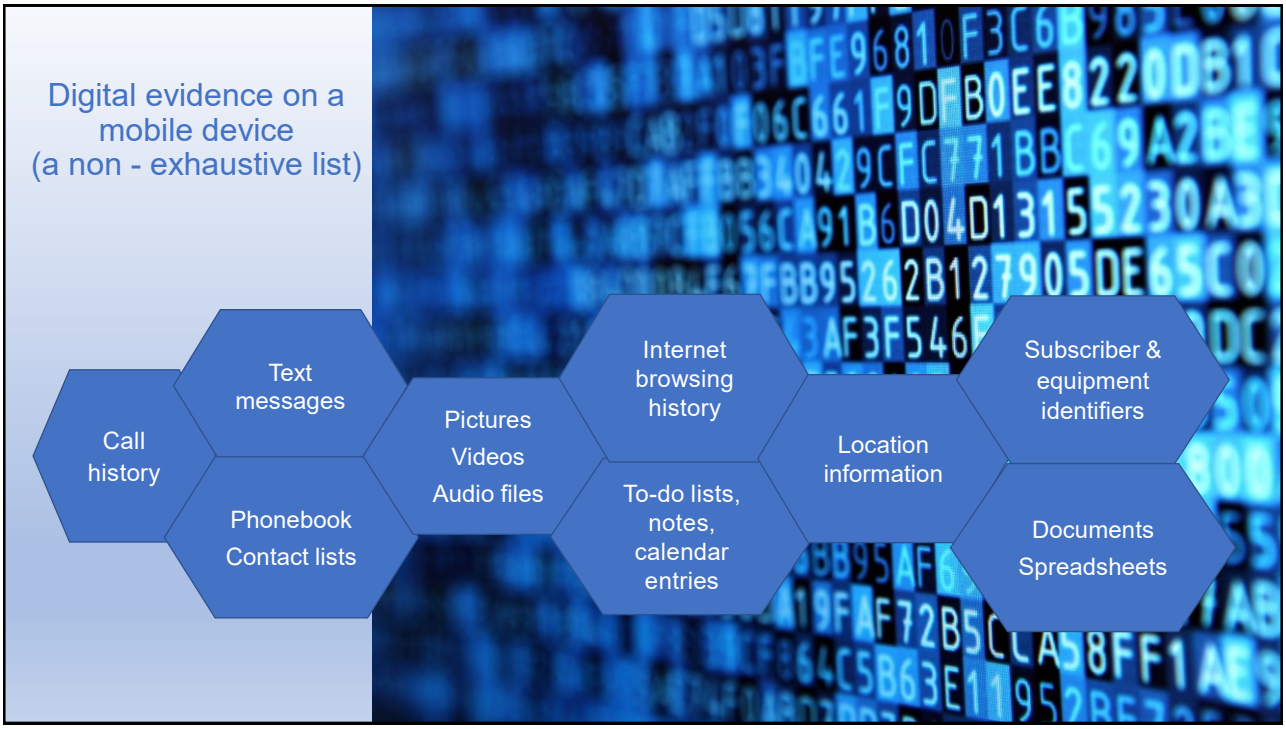
More and more crimes committed online and facilitated by electronic devices such as mobile devices ➡ traces of the crimes are left on these devices.

HOWEVER, e- evidence is

- Ephemeral
- Volatile/ Subject to easy movement and manipulation by computers
- Hard to locate

2

Digital evidence on a mobile device (a non - exhaustive list)



3

Seizure of Digital Data

Procedure laid down in Article 265 of New Criminal Procedure Code (entered into force July 2019)

Provisions for the seizure of

- ✓a computer system or part of it and computer data stored therein
- ✓ a computer-data storage medium in which computer data may be stored
- ✓a remote computer system or part of it and computer data stored therein or in a remote computer-data storage medium, interconnected to the computer system to which the person conducting the investigation has physical access.

4

Procedure of seizure

Seizure is imposed with the use of appropriate equipment which permits:

- Removal and Seizure of the medium where data is stored
- Copy and extraction of the data stored
- Reproduction and verification of the authenticity and integrity of the data seized

5

After the seizure (Art.265 para 4 Criminal Procedure Code)

- ✓During criminal procedures digital data seized remains stored in a data storage medium, which is included in the case file.
- ✓A safe copy of this data storage medium is kept by the office of exhibits of the Court to ensure retrieval in case of damage/loss.
- ✓Accessibility and reproduction of the data seized is strictly controlled and protected (by encryption/use of passwords).
- ✓Seized data can only be copied, following the prior authorization of the Court, the prosecutor, or the investigating judge in order to be used in another case.

6

Who examines and analyses digital data?

The Forensic Science Division of the Hellenic Police is the National Forensic Service of Greece

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=90090&Itemid=274&lang=EN

Digital data is examined and analyzed by the Digital Forensic Department and the results of the analysis are documented in a report (Art.30 para 10 Presidential Decree 14/2001).

Opinion 6/2021 of the Prosecutor of the Supreme Court on the seizure of digital data: The report drafted by the expert personnel of the Digital Forensic Department with the use of proper equipment, regarding the collection, extraction, analysis, reproduction, authentication and verification of the data is an *expert opinion*, the conclusions and results of which constitute an indivisible part of the report for the seizure of the physical carrier .

7

Rights of the suspect/accused person

- Be present during the research and seizure of digital data
- Appoint a technical consultant who has the right to be present during the examination of the evidence, comment on the findings of the report of the Digital Forensic Department and draft a report with his / her proper findings (art.204,207,208 Criminal Procedure Code) ➡ **Violation** of this right is considered a violation of the rights of defense, as provided under Art. 171 par.1d Criminal Procedure Code and thus nullity is implied which can be claimed by the accused/suspected or be taken into consideration by Court ex officio.

Case Law

- Three-member Air Force Court 137/2006: The defendant claimed that the messages in question appear to have been sent by his mobile with the use of the method of the caller ID spoofing and he invoked a report drafted by an expert appointed by him, analysing this method. The allegation was refuted on the grounds that the caller ID spoofing does not permit “biderectional” communication.

8

What happens if you can't unlock the mobile?

- No mandatory key disclosure/mandatory decryption laws
- Suspect/accused person cannot be compelled to hand over cryptographic keys or to provide any assistance/ right against self-incrimination and right to silence

The mobile won't be unlocked, and the stored data will not be seized and analyzed

If assistance is required and denied by third parties (service providers)

Possible criminal liability for harboring the offender ?

9

Jurisdictional Issues

Search and seizure of extraterritorially located data

- Direct cooperation with service providers (esp. Request of an IP)
- Request though a European investigation order
- Unilateral transborder access according to Art. 32 of the Convention on Cybercrime (ratified by L.4411/2016)

10

Evidence from social networks

Judgment 8/2019 of First Instance Mixed Court of Heraklion, Crete

- Mobile phones should be considered computers
- sms is a form of distant communication and thus should be evalutated as a letter. Messages exchanged in social networks are admissible as evidence and not violate the rights to free communications and to secrecy of communications when they are brought as evidence by either of the communicating parties. However, they would constitute prohibited evidence and would be inadmissible, if they are brought by a third party, who did not participate in the communication

↓

It was held that the conversations from messenger between the accused and the victim, brought by either of them, can be used as evidence.

- A photo constitutes personal data. However, if a photo is published in the Facebook profile and is accessible by everybody,

↓

It can be used as evidence since no privacy right is violated.

11

Dark web investigations Case study

Videos and photos with child pornography on the darknet indicating that the perpetratror was a greek resident

→

Lawful interception of communications ordered by the judicial council and a house search followed,during which skype and google accounts were searched and the material found on the account files was printed.

→

Tha accounts were seized and hard disks, laptops, mobile phones, SIM cards and micro sd cards were also seized and sent to the Digital Forensic Department

12

Special investigative techniques Case study

A judicial council decision was issued permitting the interception of communications and the undercover police investigation in a file sharing application, where child pornography material was shared and a user (Greek resident) had a file with child pornography available for sharing

The undercover agent obtained the password of the file. The IP used and the subscriber data of the user were disclosed. A house search was conducted but no child pornography was found. However it was noticed that more than one PCs were connected to the router.

The e-mail used for the creation of the account was given to the authorities and the subscriber data of the owner of the account was disclosed. New house search but again no material relating to child pronography was found....

13

And the invstigation goes on...

A picture of the administrator of the account was shown to the resident of the last appartement searched, who recognised an old classmate living next door.

A new house search on the latter´s house where child pornography was found on the pc, as well as the communication with the undercover agent and the photo used for the creation of the account, which was taken by a NOKIA 500 mobile also found and seized in the appartment.

Hard disc and the mobile phone were sent to the Digital Forensic Department. The report drafted confirmed that the photo was taken by a NOKIA 500. According to the report pornography material, the file sharing and communication software and the account used for the dissemination of the material were stored in the hard disc.

14

Thank you

Questions?

15

Prosecutors Office of Estonia

Electronic evidence and criminal procedure. Selected issues.

Eneli Laurits
Prosecutor

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

1

Prosecutors Office of Estonia

Setting the stage

1. Using electronic evidence in court. Some thoughts about possible issues that could be raised, evidentiary objections.
2. How to collect electronic evidence ***according to law***?
3. Publicly available data and social media. Reasonable expectation of privacy and restrictions to collection of evidence.
4. Jurisdiction.

2

Prosecutors Office of Estonia

Electronic evidence in court proceedings

As far as the applicable law allows for it, and subject to the court's discretion, the acceptance as evidence of all types of electronic evidence is encouraged and recommended for court practice.

If there is a dispute, the parties generally identify the issues to be resolved, and unless a party raises the issue of the authenticity of the electronic evidence, the court does not need to raise the issue on its own initiative.

The party seeking to rely on electronic evidence may be required to demonstrate its authenticity.

3

Prosecutors Office of Estonia

Electronic evidence in court proceedings

Evidence is generally admissable almost automatically as long as no party objects its admissal.

Digital evidence must be obtained in compliance with existing legislation and best practices to be admissible in court.

Any piece of digital evidence should be complete and tell the whole story.

Digital evidence must be collected, handled and analysed in a way which does not cause doubt about its veracity.

Digital evidence must be believable and understandable to a judge.

4

Prosecutors Office of Estonia

Evidentiary objections

- **The identity of the author may be in dispute (SODDI).**

Evidentiary goal:

- Prove the identity using circumstantial evidence.

- **It may be claimed that the records were altered, manipulated, or damaged between the time they were created and the time they appear in court as evidence.**

Evidentiary goal:

- Prove that digital evidence is authentic, complete and reliable.

5

Prosecutors Office of Estonia

Evidentiary objections

- **The reliability of the computer program that generated the record may be questioned.**

Evidentiary goal:

- Prove that computer program was working as intended and show its function.

- **It may be claimed that malware was the source of problems/records.**

Evidentiary goal:

- Prove that mentioned malware does not work the way described or prove absence of malware.

6

Prosecutors Office of Estonia

Requirements for admissibility - legitimacy

Digital evidence is considered legitimate and lawful when:

- It has been gathered without violating fundamental rights.
- It has been obtained and processed according to the procedure established by law.

7

Prosecutors Office of Estonia

Capturing evidence from the internet

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

A Party may, without the authorization of another Party:

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

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

8

Prosecutors Office of Estonia

Legal requirements for digital evidence collection in Estonia

In the Estonian Code of Criminal Procedure, there is no regulation for the taking of data across borders. Estonian law enforcement agencies (hereinafter as LEA) see four possibilities for obtaining data from foreign servers:

1) either the suspect provides it voluntarily (very often during a house-search),
2) the person controlling the data (the ISP) gives it out voluntarily as a response to a request;
3) the location of the information is identified, and a request for legal assistance submitted to the corresponding State or
4) data is collected with surveillance measures.

9

Prosecutors Office of Estonia

What to keep in mind

Digital evidence:

- Is latent, like fingerprints or DNA evidence;
- Crosses jurisdictional borders quickly and easily;
- Is easily altered, damaged, or destroyed;
- Can be time sensitive.

- Which issues might this raise in courts?

10

Prosecutors Office of Estonia

Collection – need for procedural rules?

- The principles of computer-based electronic evidence (ACPO Guidlines):

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

11

Prosecutors Office of Estonia

The principles of computer-based electronic evidence.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

12

Prosecutors Office of Estonia

The principles of computer-based electronic evidence.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

13

Prosecutors Office of Estonia

The principles of computer-based electronic evidence.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

14

Prosecutors Office of Estonia

Capturing evidence from the internet

As a general rule, data recovered by the investigator will have to withstand some of the following questions being asked:

- Where does the data come from?
- Are you sure about the integrity of this data?
- Are you sure about the completeness of this data?
- Are you sure there aren't any details you might be unaware of, regarding the data which might render your conclusions drawn upon it invalid?

Or simply: Can you guarantee the integrity of you evidence?

15

Prosecutors Office of Estonia

Capturing evidence from the internet

- The point here is, you simply can't rely on a screenshot as a solid piece of evidence given how easy it is to manipulate the contents of a given website to generate an altered screenshot.
- Perhaps one should use the source? All browsers have the ability to save web pages (browser menu options "Save Page As" or "File -> Save As")
- Alternatively, most browsers will give you an option called "View source" if you right-click on a given web page, you can also copy and paste the html source code from there.
- How to use that in court? Is it understandable to the judge?

16

Prosecutors Office of Estonia

- Printouts of electronic evidence can be easily manipulated as they exclude metadata or other hidden data. Consequently, a screen printout from a web browser is not reliable evidence as it is nothing but a copy of the screen display.
- It can be modified in a very simple manner because no special software or hardware are required for this purpose.

17

Prosecutors Office of Estonia

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

A Party may, without the authorization of another Party:

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

There is not much data that is openly available and that has evidentary value in criminal proceedings.

What is publicly available afterall?

Legal (ethical?) restrictions?

Reasonable expectation of privacy?

18

Prosecutors Office of Estonia

US v Auernheimer

The defendant was convicted of unauthorised access for collecting information from a website of US telecommunication provider which was accessible on a hard to guess website that was not intended to be accessed.

Although the data was publicly accessible the court stated that analogous to a home where 'the front door is left open or unlocked' the data was still protected.

The defence argued that the information was made available to everyone and the general public was authorised to view the information.

19

Prosecutors Office of Estonia

Social media evidence – publicly available?

- Social media evidence includes, among ohter things, photographs, status updates, a person's location at a certain time, and direct communications to or from a certain social media account.
- Facebook—and social media generally—present novel questions regarding their users' expectations of privacy. Facebook users may decide to keep their profiles completely private, share them only with "friends" or more expansively with "friends of friends," or disseminate them to the public at large.

20

Prosecutors Office of Estonia

Social media evidence – privacy concerns

- When a social media user disseminates his postings and information to the public, they are not protected for privacy. However, postings using more secure privacy settings reflect the user's intent to preserve information as private.
- When a person with a public privacy setting tweets, he or she intends that anyone that wants to read the tweet may do so, so there can be no reasonable expectation of privacy.

21

Prosecutors Office of Estonia

Thilo Gottschalk
The Data-Laundromat?
Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement

„A sub-section of the surface web is social media (eg Instagram, Snapchat, Facebook, Tinder). Social connections have always been an important investigative approach, with the shift from real-life to electronic communication these connections are often easily accessible and generate valuable insights for law enforcement.

Some of the currently existing networks allow users to limit the reach of their content to certain user groups (everyone, network participants, friends, friends of friends).

The public availability for such restricted data hence often depends on factual barriers that these settings eventually raise. Data on social networks are easily relatable to natural persons and often give insights in particularly sensitive areas of a persons' life such as religious or political beliefs or sexual preferences. Accessing social media data is hence bears severe risks to the fundamental rights of the data subject. While data on social media may be manifestly made public, this cannot be re-interpreted as consent or abandoning fundamental rights protection.“

22

Prosecutors Office of Estonia

United States v. Meregildo

Government's method of collecting evidence was challenged, that is Government's use of a cooperating witness who was one of suspect's Facebook "friends" and gave the Government access to suspect's Facebook profile.

To which extent can one say that his social media account is private? Could it be at some circumstances be seen as publicly available information? Could LEA collect such data without any further authorisation?

23

Prosecutors Office of Estonia

- Where Facebook privacy settings allow viewership of postings by "friends," could the Government access them through a cooperating witness who is a "friend" without violating the rights for privacy?
- While user undoubtedly believe that his Facebook profile would not be shared with law enforcement, does he have justifiable expectation that his "friends" would keep his profile private? And the wider his circle of "friends," the more likely his posts would be viewed by someone he never expected to see them.
- User's legitimate expectation of privacy ends when he disseminates posts to his "friends" because those "friends" are free to use the information however they want—including sharing it with the Government.
- The argument that the user with a private setting has a reasonable expectation of privacy because he had a limited number of followers has nothing to do with his attempts to keep his messages private.

24

Prosecutors Office of Estonia

Social media evidence

Social media is subject to same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media as well as the ease with which it can be manipulated or falsified creates hurdles to admissibility not faced with other evidence.

Methods of authentication include:

1. presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it),
2. searching the computer itself to see if it was used to post or create the information, or
3. attempting to obtain the information in question from the actual social media company that maintained the information in the ordinary course of their business.

25

Prosecutors Office of Estonia

Social media evidence

There are two distinct types of authentication that must occur for evidence from social networking sites.

1. One is to authenticate the authorship of the evidence on the website.
2. The other is to authenticate that the exhibit used at trial, typically a printout of the webpage, is a fair and accurate representation of what was on the computer screen.

Testimony by a witness who viewed the information on the website is usually sufficient to meet the latter requirement.

26

Prosecutors Office of Estonia

- The fact that a witness held and managed an account does not provide enough of a foundation for authentication; the proponent must show that the communication in question came from the witness and "not simply from her Facebook account."
- Courts have raised concerns because social networking accounts may be compromised by hackers and anyone may create a fictitious account under another's name. In addition, users "frequently remain logged in to their accounts while leaving their computers and cell phones unattended," raising the likelihood of third parties creating unauthorized posts.

27

Prosecutors Office of Estonia

Capturing evidence with surveillance methods

The Advisory Guidelines on IT-Evidence, prepared on 24.05.2016 by LEA, claim that in case of public investigative measures (inspection, search) and covert surveillance, no request for legal assistance is needed for data stored in the cloud on foreign States' servers.

The reason is that action (the copying of data) is performed in the territory of Estonia by an Estonian body conducting proceedings, and the data can be received without physically leaving the territory of Estonia. Estonia has the jurisdiction to copy the data.

28

Prosecutors Office of Estonia

Capturing evidence with surveillance methods

When collecting data from a digital account, it is considered as covert inspection according to Estonian legislation and case-law. This requires a prosecutor's authorisation.

If this measure involves accessing a computer system, then the authorisation from a judge is also needed.

Essentially it means that both authorisations are needed, as there is no other way to collect data from a foreign server without accessing a computer system.

However, the critical issue with jurisdiction remains.

29

Prosecutors Office of Estonia

Electronic evidence in court proceedings

„According to the analysis of the legislation, electronic evidence is considered to be equivalent to traditional evidence."

– European study on the admissibility of electronic evidence in court (AEEC) (Project JLS/2005/AGIS/119)

- No uniform European regulation on the requirements for the admissibility of digital evidence exists.
- Many European countries pertain no legislation specifically dealing with digital evidence.
- Courts are forced to make use of the general rules and principles on admissibility of evidence.

30

de Rechtspraak
Rechtbank Zeeland – West-Brabant

The proposed European Production Order (EPO) and its effectiveness in collecting evidence

OBTAINING E-EVIDENCE WHEN INVESTIGATING AND PROSECUTING CRIMES

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

1

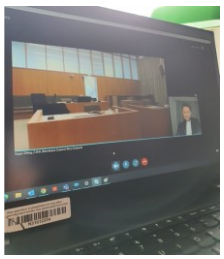
de Rechtspraak
Rechtbank Zeeland – West-Brabant

Introduction

Studies:
- Computer Science
- Law School

Professional experience:
- Legal assistant, Lawyer at the Dutch Judiciary
- Legal advisor, Policy Officer cybercrime and digital investigations at the Dutch Police

Current Position and Additional Position:
- CISO Engie NL
- Judge at the criminal court



2

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Guideline

- Introduction and some figures
- Mutual Legal assistants
- Difficulties in investigating cybercrime
- European Production Order
- Case study

3

de Rechtspraak
Rechtbank Zeeland – West-Brabant

We are under attack

Cybercriminals are increasing efficiency with coordinated attacks

The lost productivity as a result of the WannaCry attack cost $ 4 billion

2019

- **January** — MEGA cloud (NZ) suffered a data breach exposing 770 million emails and 21 million passwords.
- **February** — Verification.io (US) exposed ca. 800 million records.
- **March** — Norsk Hydro (NO) victim of a ransomware attack.
- **April** — Facebook (US) reported a data breach exposing 540 M user records on exposed servers.
- **May** — Thyssen Krupp and Bayer (DE) targeted with espionage malware.
- **June** — Five hospitals in Romania (RO) hit by Badrabbit ransomware.
- **July** — City Power (ZA) victim of a ransomware attack disrupting the energy supply in Johannesburg.
- **August** — Bulgarian (BG) Personal Tax Revenue office suffered a data breach exposing PII from all adult citizens.
- **September** — Mastercard (BE) suffered a data breach affecting ca. 90K customers in Europe.
- **October** — Websites and the national TV broadcaster in Georgia (GE) suffered a coordinated cyberattack.
- **November** — UniCredit (IT) victim of a data breach leaking 3M records.
- **December** — Prosegur (SP) suffered a ransomware attack disrupting its operation.

2020

- **January** — Austria's Foreign Ministry (AT) targeted by a cyberattack.
- **February** — INA Group (HR) victim of ransomware attack.
- **March** — ENTSO-E (BE) network compromised, victim of an intrusion.
- **April** — Over 500K Zoom (US) accounts found for sale in the dark web.

Suffering Financial Impact From Data Breaches (Nonfines)	Loseing Customers	Suffering From Reputation Damage
46%	45%	44%

SECTOR	MOST POPULAR THREATS/ATTACKS	INCIDENTS TRENDS
Individual	• Phishing • Malware • Information leakage • Data theft	Stable
Multiple industries	• Web application attacks • Phishing • Malware	Increasing
Public Administration, Defence, Social Services	• Malware • Phishing • Web based attack	Stable slightly decreasing
Financial/Banking/ Insurance	• Web application attacks • Insider threat (unintentional abuse) • Malware • Data theft	Stable
Health/Medical	• Malware • Insider threat (unintentional abuse/error) • Web application attacks	Increasing
Education	• Malware • Ransomware • Web based attacks	Stable slightly decreasing
Information and Communication	• Web application attacks • Insider threat (unintentional abuse/error) • Malware	Stable
Professional/Digital Services	• Web application attack • Insider threat (unintentional abuse/error) • Malware	Stable
Arts, Entertainment and gaming	• Web application attacks • Malware • Phishing	Stable
Manufacturing	• Malware • Web application attacks • Insider threat (unintentional abuse/error)	Stable

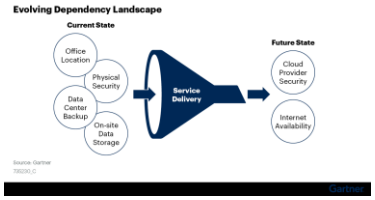
enisa

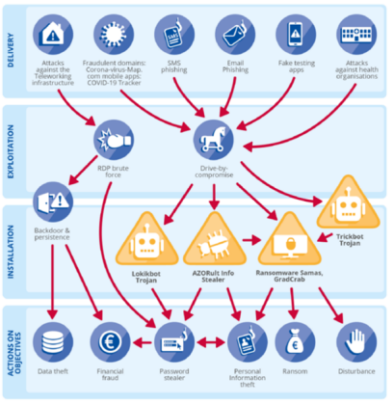
4

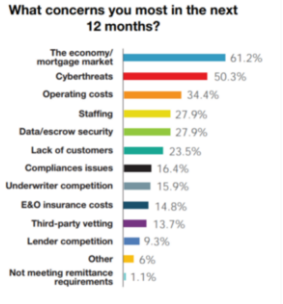
de Rechtspraak
Rechtbank Zeeland – West-Brabant

Near future, post Covid 19

During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface."







5

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Developments

Achievements

Vera Jourová, EU Commissioner for Justice: "*While law enforcement authorities still work with cumbersome methods, criminals use fast and cutting-edge technology to operate. We need to equip law enforcement authorities with 21st century methods to tackle crime, just as criminals use 21st century methods to commit crime.*"

6

Mutual Legal Assistance

European Convention on Mutual Assistance in Criminal Matters (ETS No. 30)

- Under this Convention, Parties agree to afford each other the widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons etc.
- National procedures on judicial co-operation in the criminal field.
- Practitioners are urged to consult the lists of signatures and ratifications as well as the declarations and reservations of any convention.
- Treaties create binding obligations on states parties, but actual execution of a request for international cooperation also requires analysis and consideration of the domestic laws of the requesting and requested states

7

General Principles International Cooperation in Criminal Matters

- Widest Cooperation Possible
- Dual Criminality
- Specialty Principle
- Proportionality

8

Difficulties traditional MLA in cybercrime cases

Traditional legal concepts → Territoriality → Jurisdiction

the need to have access to digital evidence which has been growing exponentially!

9

European Production and Preservation Orders
Background

- Current framework is not sufficiently workable
- The information and communication technology in everyday life

First

Digital evidence is held on servers owned by service providers.

Second

the territorial approach to the jurisdiction to enforce – that is impractical and outdated

10

European Production and Preservation Orders
Summary of the proposed Regulation

- Issued or validated by a judicial authority of a Member State
- Preservation or production of data that is stored by a service provider located in another jurisdiction
- Necessary as evidence in criminal investigations or criminal proceedings
- Only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

- **Legal basis**
- **Choice of the instrument**
- **Subsidiarity**
- **proportionality**

European Production and Preservation Orders
Legal Basis, Subsidiarity and Proportionality

13

Case Study ‘Car theft and international chop up of cars’

14

10 May 2021

de Rechtspraak
Rechtbank Zeeland – West-Brabant

Thanks!

Questions?

Contact:
https://www.linkedin.com/in/jordy-mullers-5583b829/
J.mullers@rechtspraak.nl

15

USING OPEN SOURCE INTELLIGENCE TO GATHER EVIDENCE ONLINE

Dipl.-Ing. Dennis Pielken

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

1

WELCOME

RR, Dipl.-Ing.
Dennis Pielken

- Expert Witness for digital forensics
- Working in digital forensics and digital investigations for the last 13 years
- Areas of Expertise:
  - Digitale Forensics
  - OSINT
  - Digital Investigations

2

AGENDA

1. Basic Concept of the Internet and Addresses
2. What do you VPN und Proxies offer?
3. The DarkNet and the TOR-Network
4. Websites – What do they consist of?

3

THE INTERNET AND IP-ADDRESS

Basic Concepts

4

THE IP-ADDRESS

Examples:

Public IPv4 Address:

- 12.223.87.98

Private IPv4 Address:

- 192.168.0.1

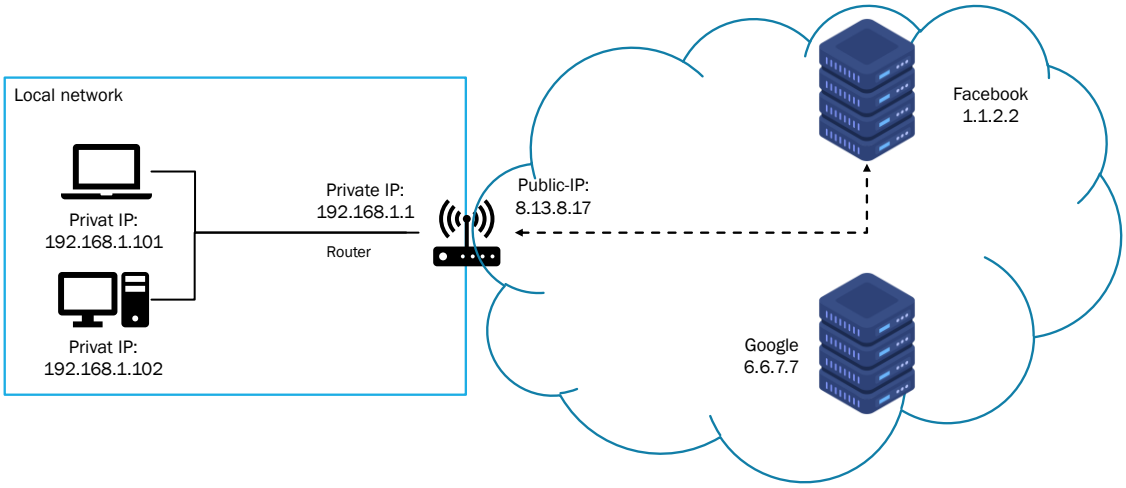
Public IPv6 Address:

- abcd:12ab:1:2:89:778:9:12f
- ef::123:12a

- An IP-Address is like a postal address in the internet
- An IP-Address is either assigned to a dedicated device or internet connection. This assignment can be
  - Temporary – dynamic IP-Address
  - Permanently – static IP-Address
- Only public IP-Addresses can be used to access the internet
  - Privat IP-Addresses are used in local networks, such as home networks or business networks

5

EXAMPLE OF IP-ADDRESSES

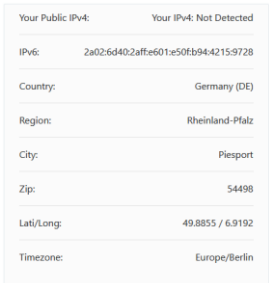


6

IP-ADDRESS – PUBLICLY AVAILABLE INFORMATION

- IP-Addresses are assigned to organizations by a central authority (IANA) – such as Internet Service Providers (ISP)
- Whenever an IP-Address is assigned to an organization, this is made public in the WHOIS-Database
- This database can be queried by everyone
- Geo-IP-Address Database contains information, in what part of a country a given IP-Address is used. This information may be unreliable.

Example IP Location:



Your Public IPv4:	Your IPv4: Not Detected
IPv6:	2a02:6d40:2affe601:e50f:b94:4215:9728
Country:	Germany (DE)
Region:	Rheinland-Pfalz
City:	Piesport
Zip:	54498
Lati/Long:	49.8855 / 6.9192
Timezone:	Europe/Berlin

Example WHOIS Information:

organisation	ORG-IG45-RIPE
org-name	inexio Informationstechnologie und Telekommunikation Gmbh
country	DE
org-type	LIR
address	Am Saaraltarm 1
address	66740
address	Saarlouis
address	GERMANY
phone	+49683150300
fax-no	+4968315030120

DOMAIN

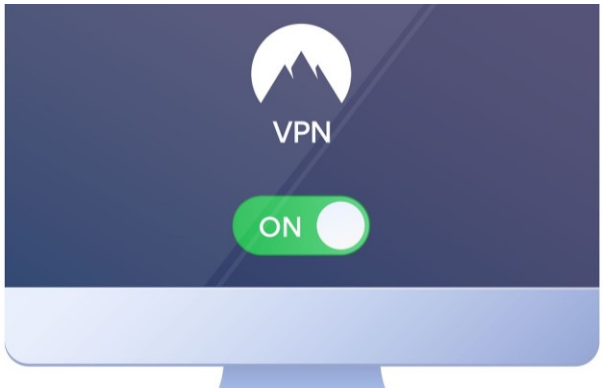
- A domain can be translated into an IP-Address
- The domain consists of various levels
- Domains can be registered by anyone
- A domain is always registered by the owner of the upper hierarchy level
- A German domain (.de) can translate to an IP-Address of a US-company

Domain:

- www.fbi.gov
- www.era.int
- news.info.com

Domain Name System

- DNS is the technology that translates a domain into an IP-Address
- An IP-Address can also be translated into a domain
- Whereas one domain always translates into one IP-Address, one IP-Address can translate into several domains



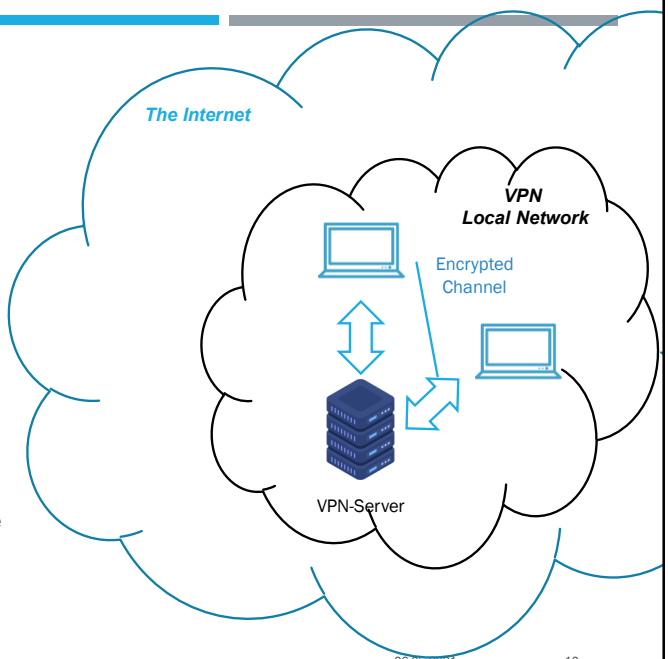
PROXY AND VPN

What is this?

9

VIRTUAL PRIVATE NETWORK

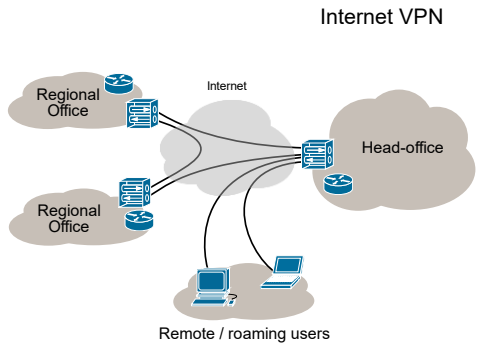
- A VPN provides the technology that server participants can be connected so that it seems like they are in the same local/private network, whereas they are all connected to each other over the internet.
- From each participant an encrypted channel is established (over the internet) to a central server – the VPN server.
- This channel ensures that all communication is
  - confidential and
  - secured against any changes (integrity)
- Through this VPN server users can access services inside the VPN or use a gateway to access other internet services.



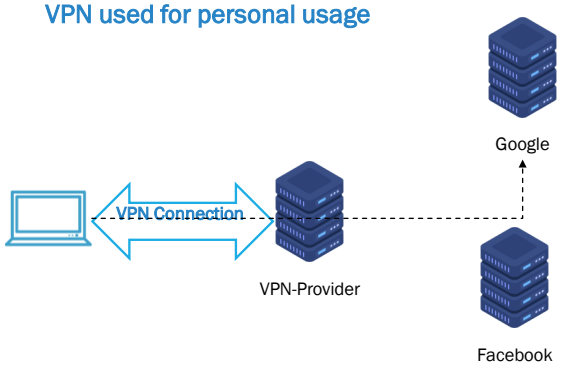
10

VPN - POSSIBLE APPLICATIONS

VPN used in business

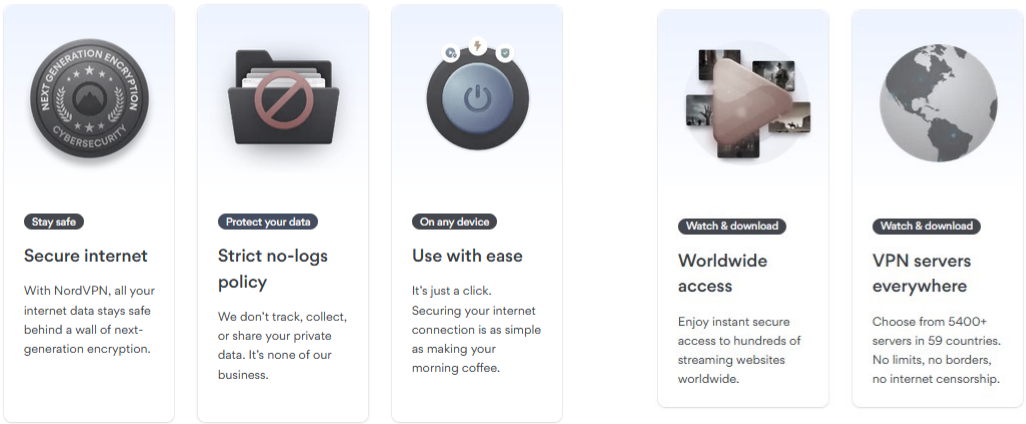


VPN used for personal usage



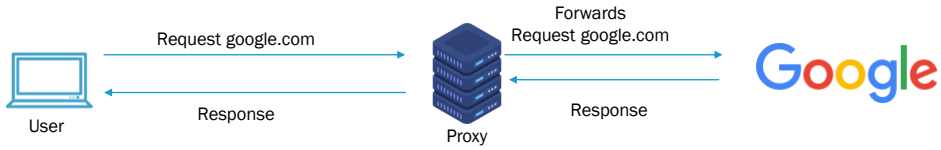
11

EXAMPLE *NORDVPN* – SELECTED FEATURES



12

PROXY



- A Proxy server is used to forward request and responses
- The connection from the user to the Proxy server does not need to be encrypted
- In a business environment Proxy servers are used to filter web traffic
- Proxy server may only support the forwarding of one protocol (such as http/https)

DO A VPN OR A PROXY PROVIDE ANONYMITY & SECURITY?

It depends:

- The central component (VPN or proxy provider) can identify the user
- The central component can keep protocol what each user accessed
- The central component may be able to alter traffic

Therefore, the question is: Is the central component trustworthy?

THE ONION ROUTER

And the Darknet

15

TERMINOLOGY

Darknet

- To access this part of the internet, you need either special software, an account or maybe a personal invitation
- Usually ensures sender and receiver anonymity
- Various different Dark-Networks exist, the most famous one is the TOR-Network

Underground Site

- Usually connected to illegal activities
- Provide discussion forums or online shop – maybe both
- Accessible via the clear web or the dark web

16

SOME FACTS ABOUT TOR – PART I

The Idea

„The goal of onion routing was to have a **way to use the internet** with as much **privacy as possible**, and the idea was to **route traffic through multiple servers** and encrypt it each step of the way." This is still a simple explanation for how TOR works today.

U.S. Naval Research Lab (NRL) 1996

2002

First software implementation is released

2003

The network has over 10 volunteers that provide access nodes – mostly from the USA and Germany

17

SOME FACTS ABOUT TOR – PART II

2006

The TOR Project, Inc. was founded. A 501(c)3 Nonprofit-Organisation.

2012

Donation for the development of the TOR Network is provided by:

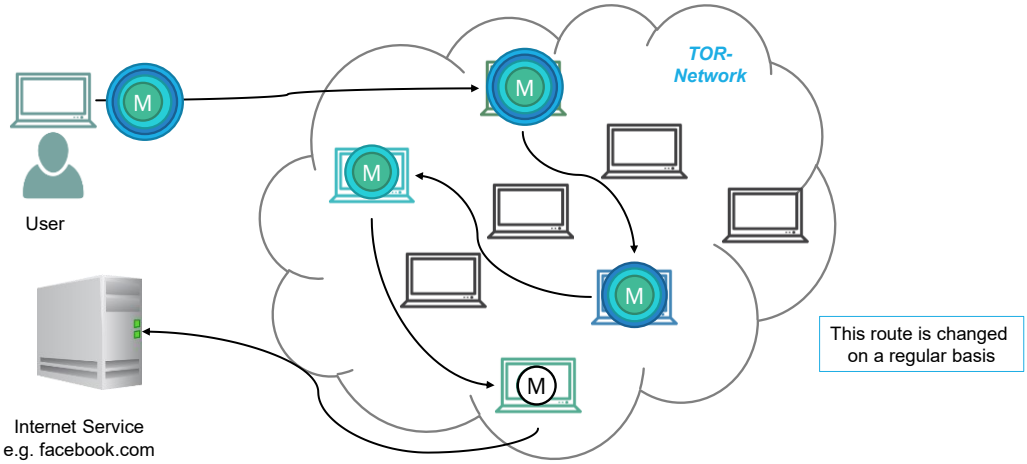
- 80% US-Government (2 Mio. USD)
- 20 % Swedish Government

2014

Operation „Onymous" de-anonymizes 400 TOR hidden services and identifies 17 administrators of illegal websites

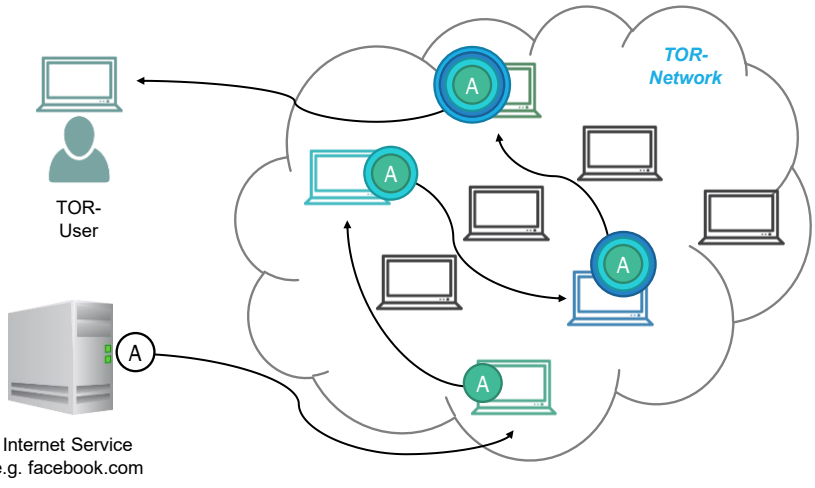
18

TOR NETWORK – HOW IS SENDER ANONYMITY ENSURED? (PART 1)



19

TOR NETWORK – HOW IS SENDER ANONYMITY ENSURED? (PART 2)



20

HIDDEN SERVICES

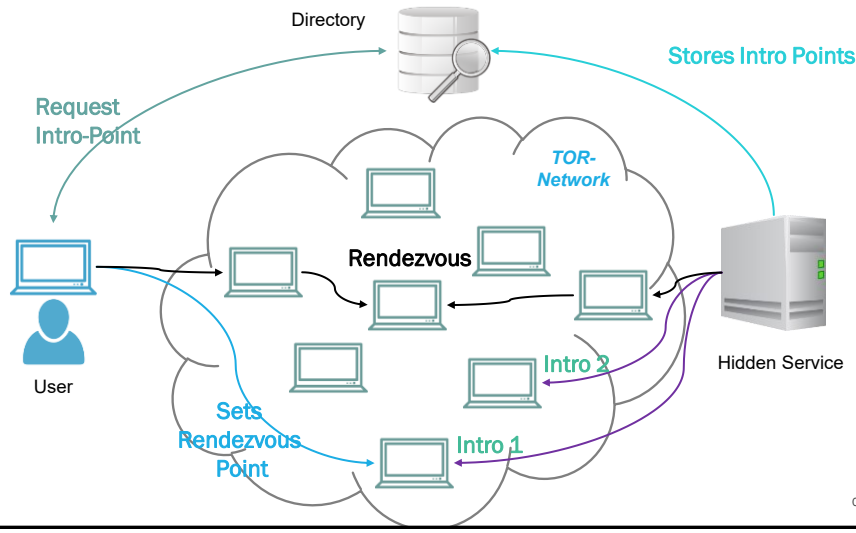
Facts:

- Internet Services
- Only accessible through the TOR Network
- Access via ONION-URLs (.onion)

- A hidden service provides anonymity to the service – meaning the user does not know the service
  - IP-Address nor
  - The location
- Hidden Services cannot be found directly through a search engine
- Directories of Onion-URLs exist – such as the hidden wiki
- Most hidden services can only be accessed with a user account

21

TOR NETWORK – HOW IS RECEIVER ANONYMITY ENSURED? (PART 2)



22

TOR INVESTIGATIONS

Known facts: An unknown TOR-User provides a plattform in the darkweb to share and distribute child pornography.

This TOR-User has a unique username.

Based on English terms used by this user, his country of origin can be guessed.

He also mentions in "public" chats that he is a passionate mountain bike driver.

Almost the same pseudonym was used in a mountain bike community, where this user published his tracks.

User was identified based on this information using traditional Police investigation techniques.

23

WEB CONTENT AND WEBPAGES

Welcome to WWW

24

WWW – WHAT IS THIS ANYWAYS?

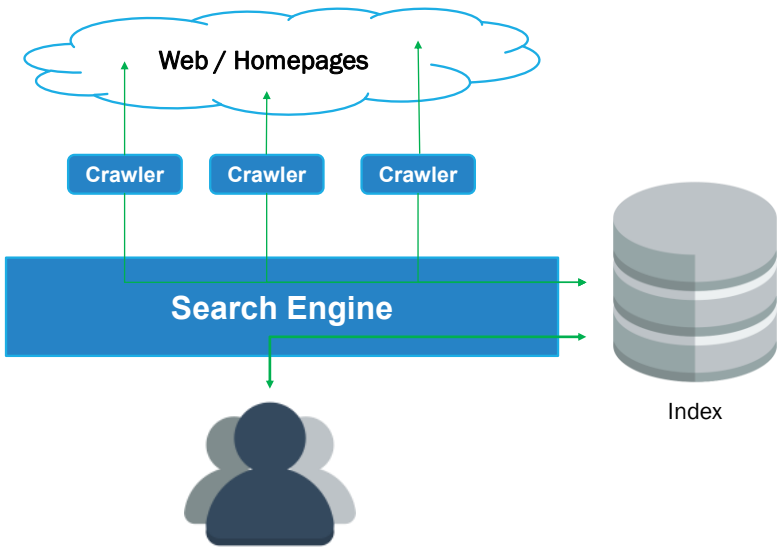
- **Easy explanation:** The part of the internet that can be accessed by a webbrowser

https://en.wikipedia.org/wiki/World_Wide_Web

- **More complex:**
  - Information system, that mainly consists of documents
  - These documents are accessed through the Hyper Text Transport Protocol and Uniformed Resource Locators
  - These documents can be interlinked via hyperlinks

INTERNET SEARCH ENGINES – BASICS

- Crawlers are used to discover web pages and their content (text & images)
- The content is stored in an index
- The index is queried by users when performing searches
- The content of the index can be accessed via the cache



INFORMATION NOT VISIBLE TO THE USER

Server-Side

- HTTP/1.1 200 OK
- **Server**: nginx/1.17.3
- Date: Thu, 05 Sep 2019 17:50:24 GMT
- Content-Type: text/html
- Content-Length: 117
- **Last-Modified**: Thu, 05 Sep 2019 17:40:42 GMT
- Connection: close
- ETag: "5d71489a-75"
- Accept-Ranges: bytes

Client

- **Refered From**: https://www.whatsmyip.org/
- **User Agent**: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36 Edg/90.0.818.51
- Screen Resolution: 1920 x 1080 (pixels)
- Browser Dimensions: 1920 x 969 (pixels)
- Cookie Status: Enabled
- Browser Plugins:
  - Microsoft Edge PDF Plugin (internal-pdf-viewer)
  - Microsoft Edge PDF Viewer (mhjfbmdgcfjbbpaeojofohoefgiehjai)
  - Native Client (internal-nacl-plugin)

THE END

QUESTIONS?

energie, technologie en optimisme

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

10/05/2021

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

Introduction

- Remco Sprooten
- Team leader for the ENGIE SDO Security operations center
- Team leader for the SDO Red Team
- Former digital forensic investigator for the Dutch Police
- Activities include:
  - Ethical hacking (penetration testing)
  - Freelance malware research
  - Incident responder

ERA
Europäische Rechtsakademie
Academy of European Law
Académie de Droit Européen
Accademia di Diritto Europeo

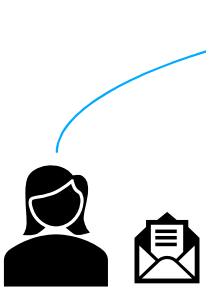
Co-funded by the Justice Programme of the European Union 2014-2020

Encryption and privacy (basics)

Alice

Bob

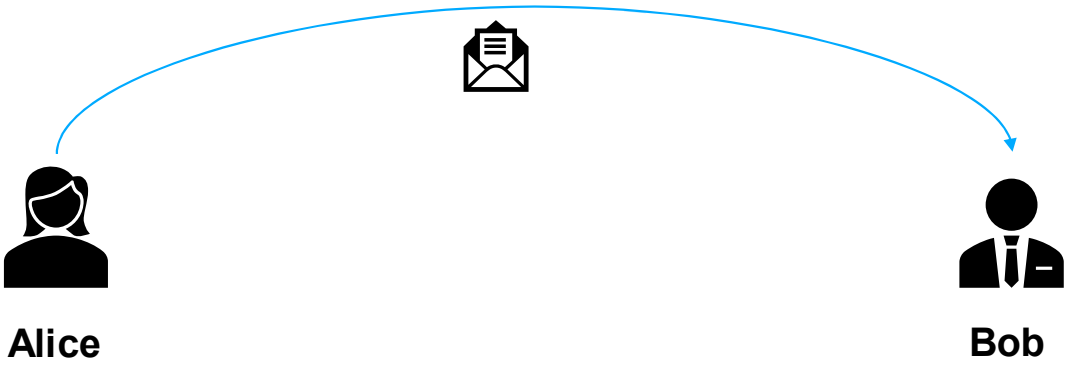
Encryption and privacy (basics)



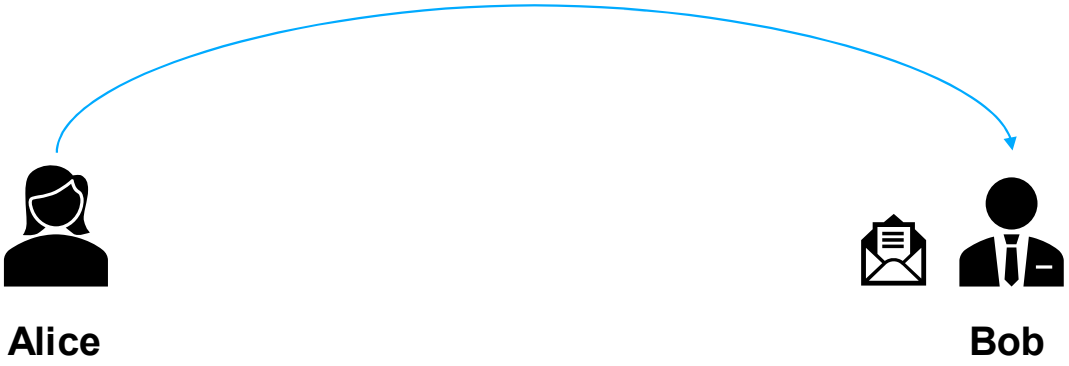
Alice

Bob

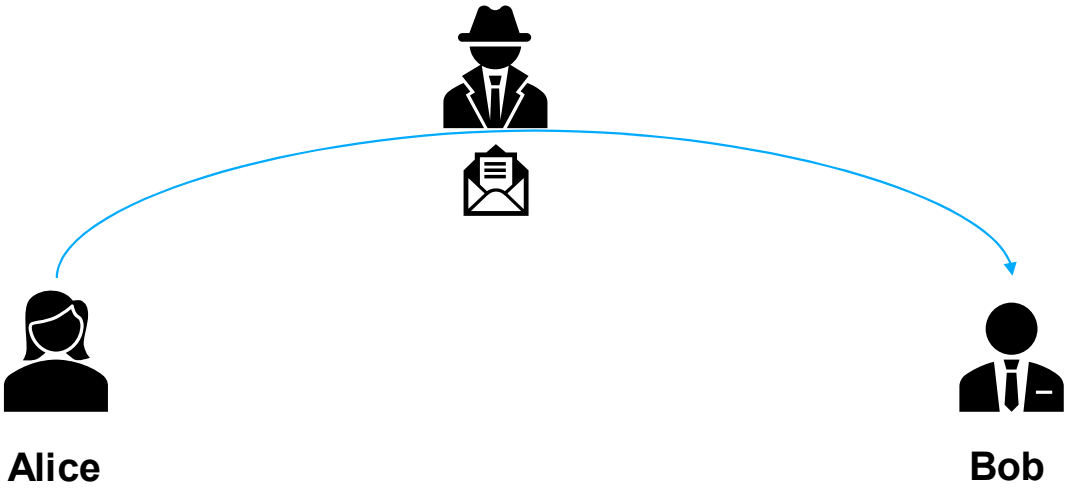
Encryption and privacy (basics)



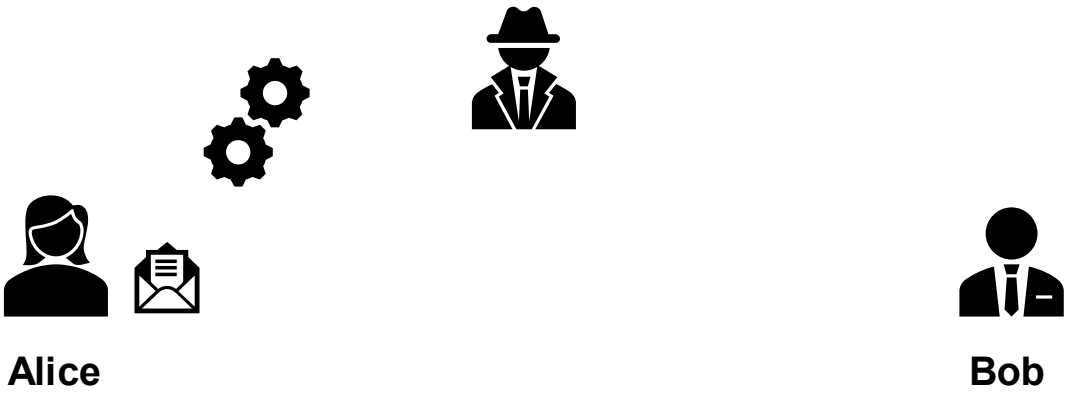
Encryption and privacy (basics)



Encryption and privacy (basics)



Encryption and privacy (basics)



Encryption and privacy (basics)

Alice

Bob

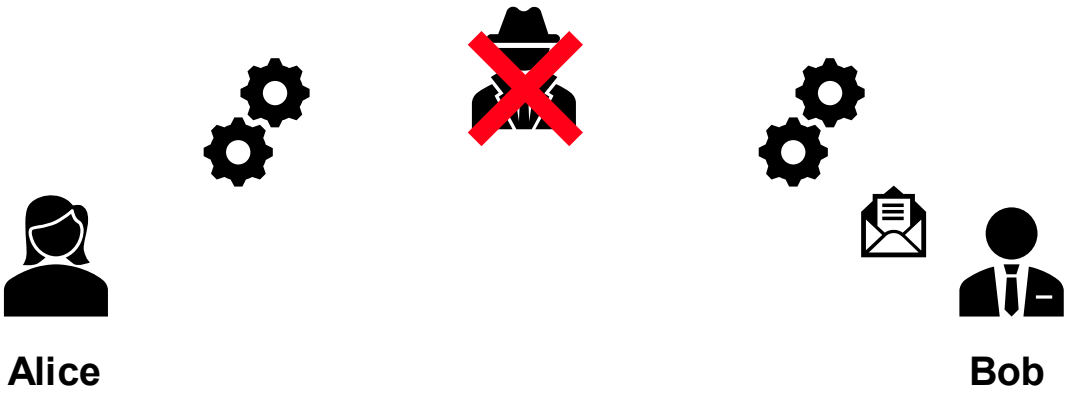
Encryption and privacy (basics)

Alice

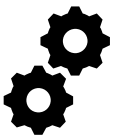
Bob

Encryption and privacy (basics)

Encryption and privacy (basics)



Encryption and privacy (basics)



Message

Encryption algorithm

Key

Encryption and privacy (basics)

11101
01010
11101
01010
10101
01110
10101
01010
10

Ciphertext

Encryption algorithm

Key

Encryption and privacy (basics)

Ciphertext: The encrypted message

- Is assumed to be known

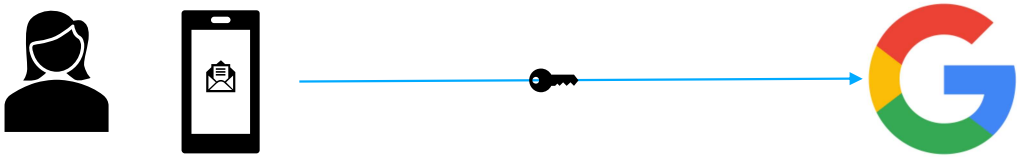
Encryption algorithm

- Is assumed to be known

The key

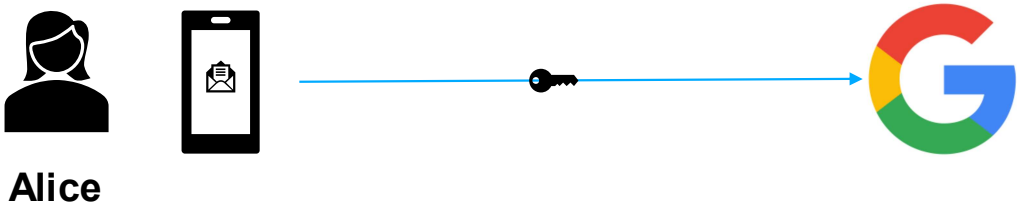
- Should be kept private

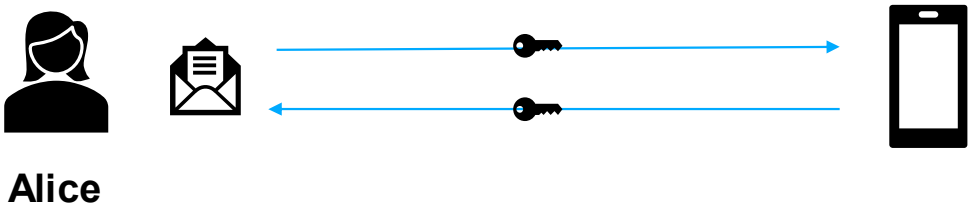
Encryption on smartphones



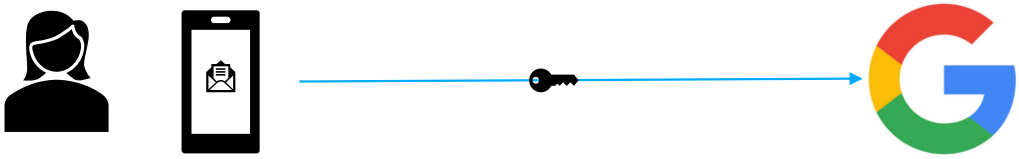
Alice

Encryption on smartphones

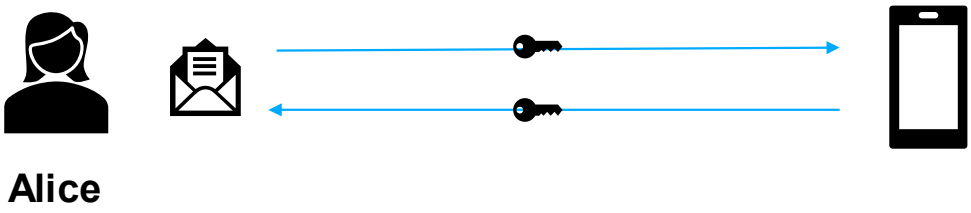




Encryption on smartphones



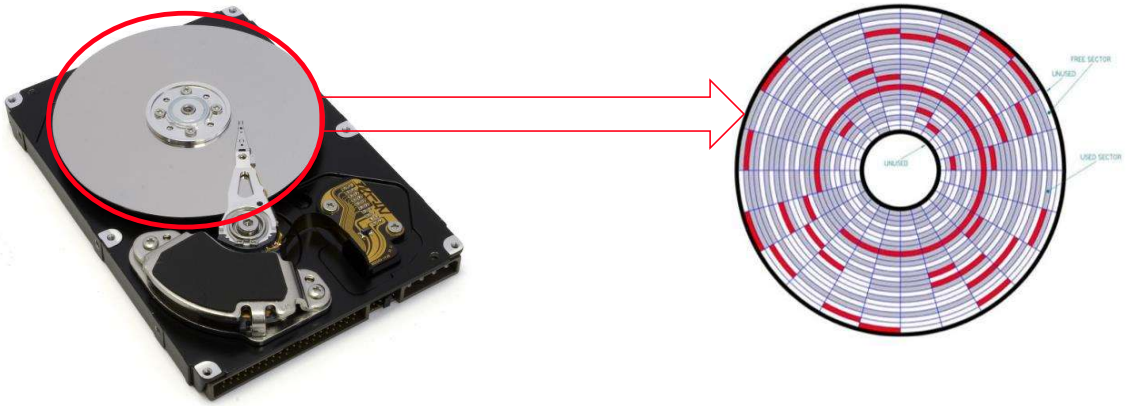
Key is agreed upon during the connection



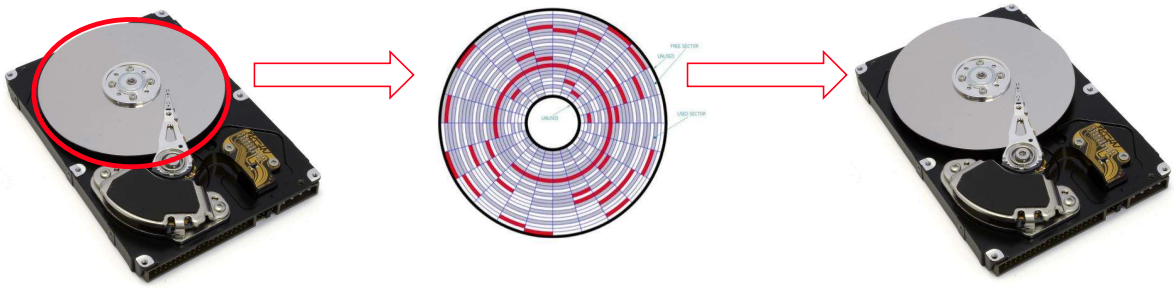
Key is based on the PIN/Password cobined with the device

Physical Extraction

Physical Extraction



Physical Extraction



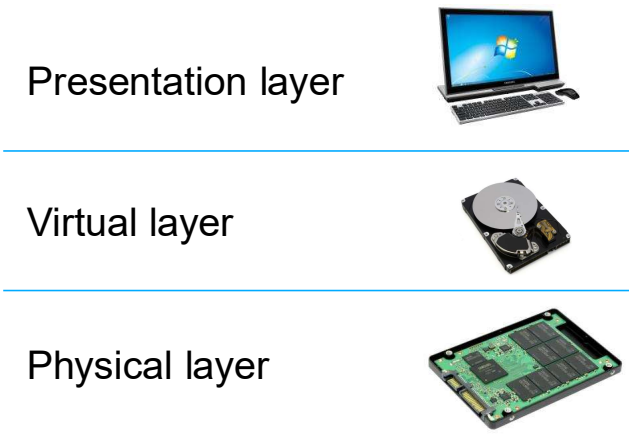
Physical to Logical

- New storage technology
  - Solid stade drives (SSD)
  - Flash memory
- Data is no longer stored in predictical locations
- Computers / devices still rely on these locations

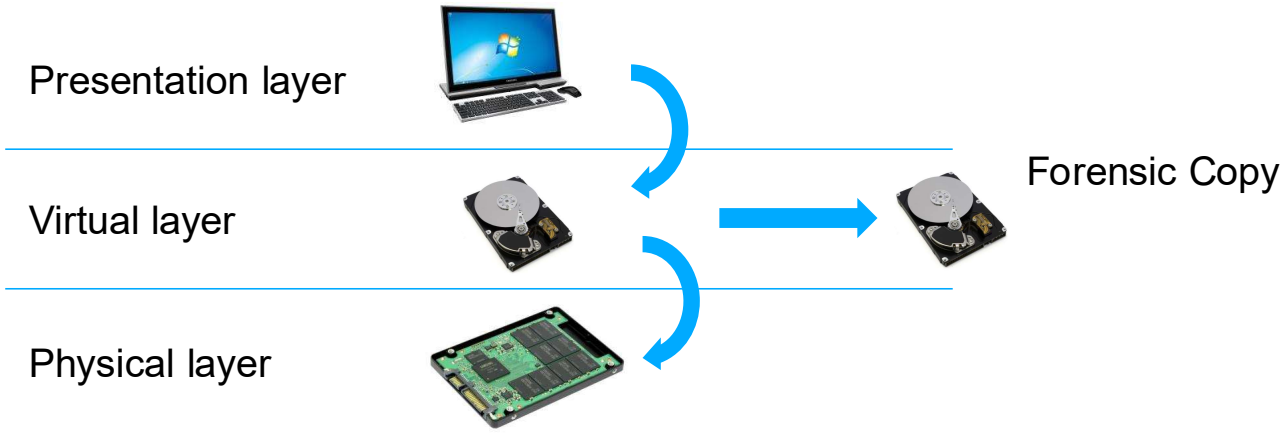
Physical to Logical

- New storage technology
  - Solid stade drives (SSD)
  - Flash memory
- Data is no longer stored in predictical locations
- Computers / devices still rely on these locations
- Physical is less physical

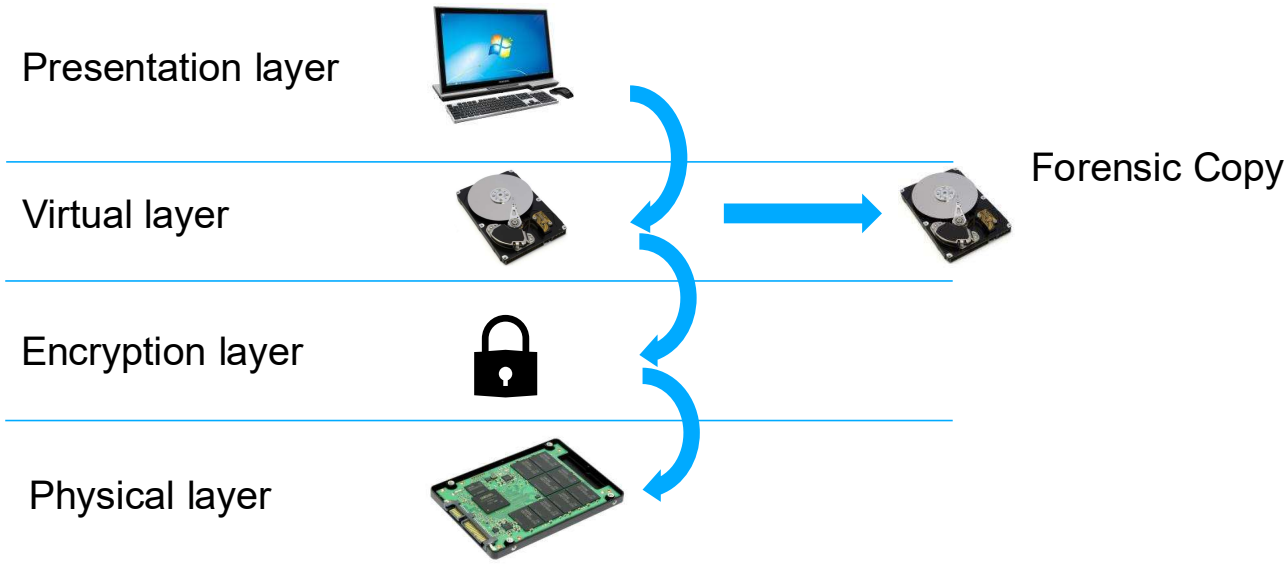
Physical to Logical



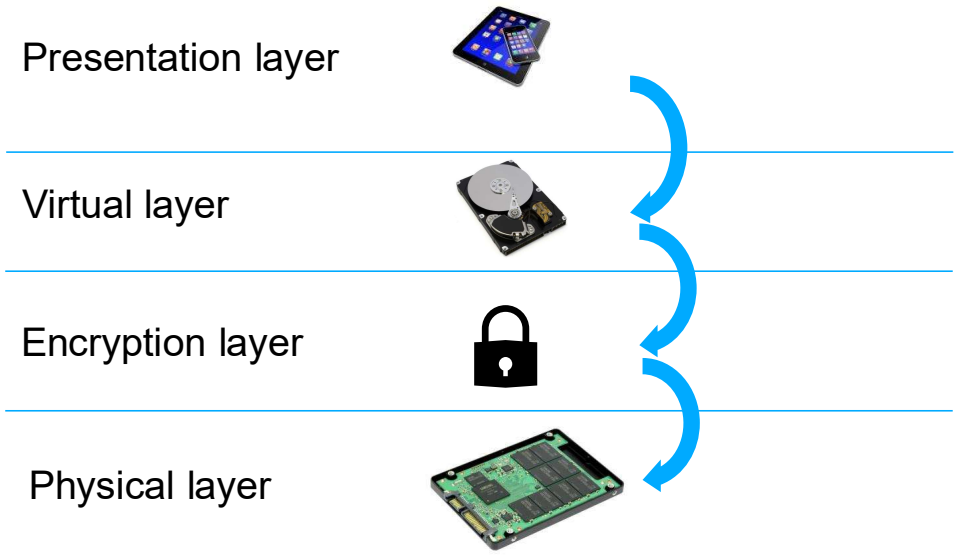
Physical to Logical



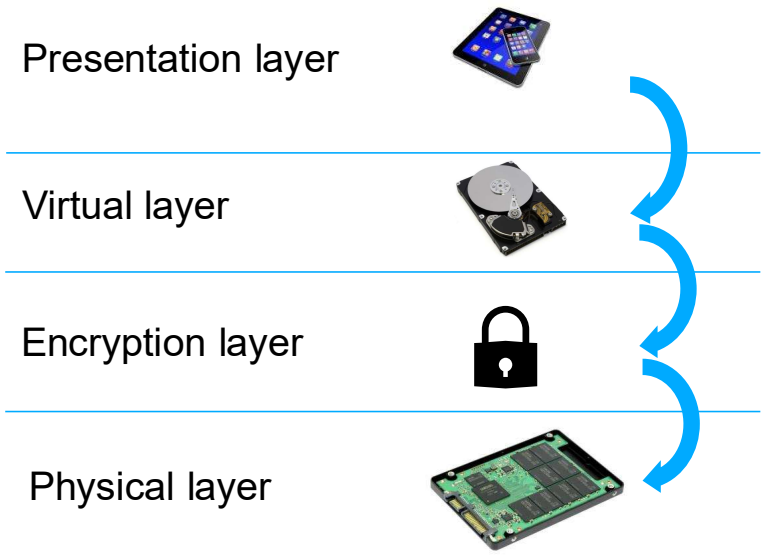
Physical to Logical



Physical to Logical

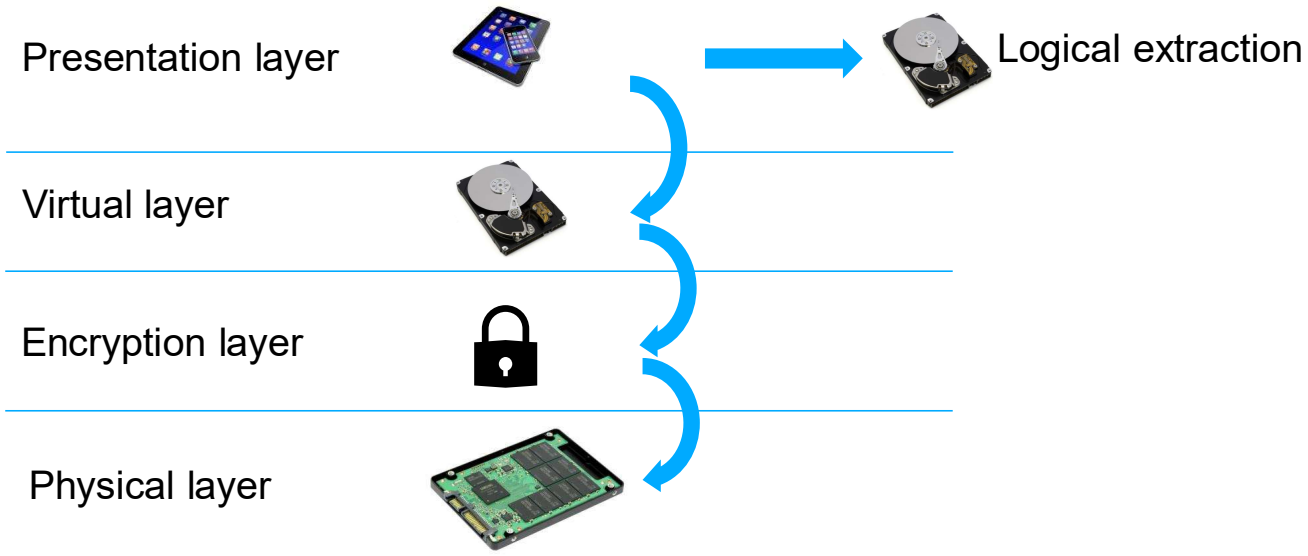


Physical to Logical

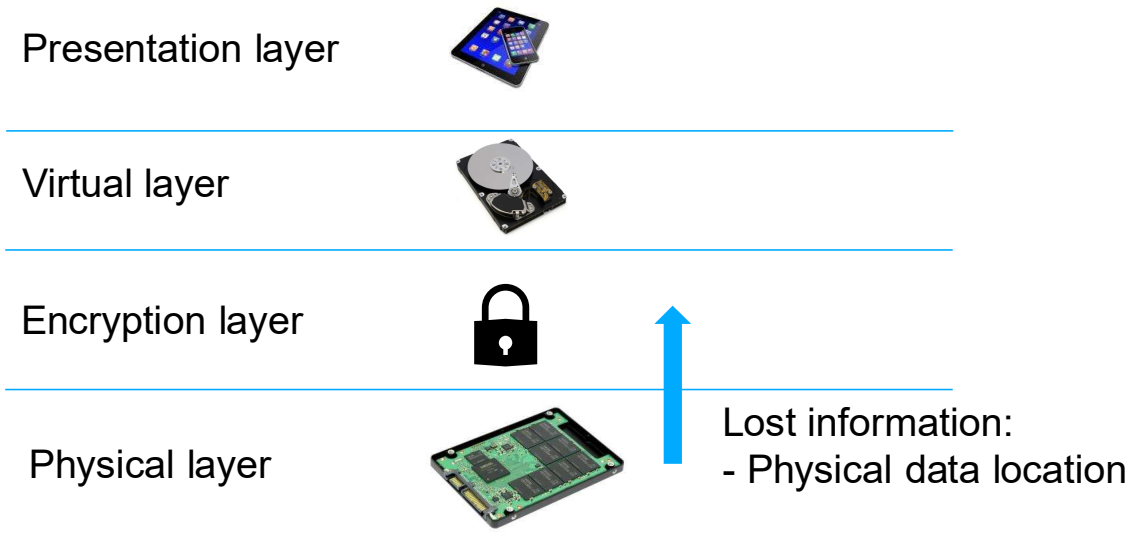


Mobile devices add extra (security) layers

Physical to Logical



Logical Extractions



Physical to Logical

Presentation layer 

Virtual layer 

Encryption layer 

Physical layer 

Lost information:
- Physical data location

Physical to Logical

Presentation layer 

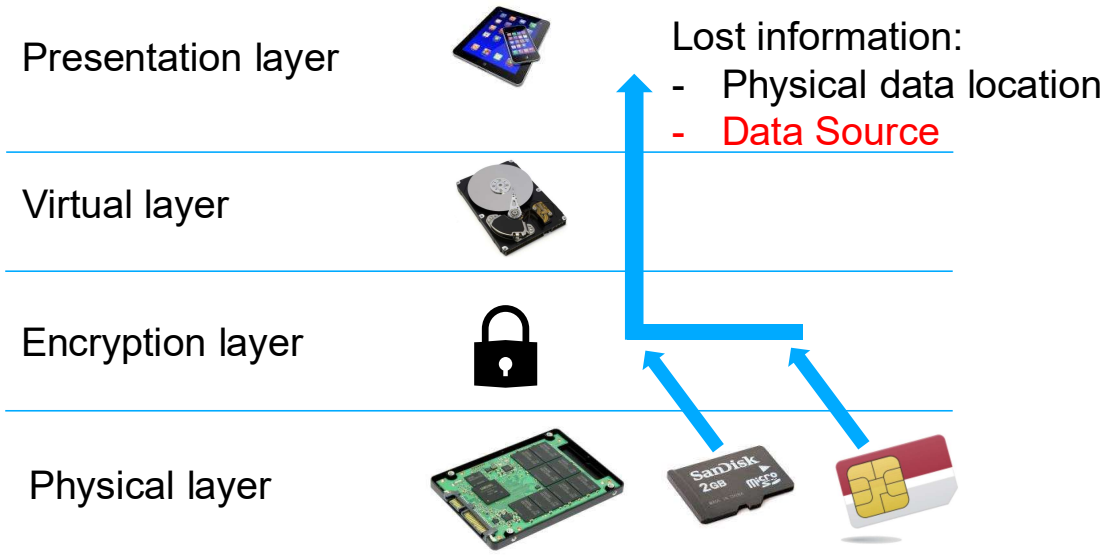
Virtual layer 

Encryption layer 

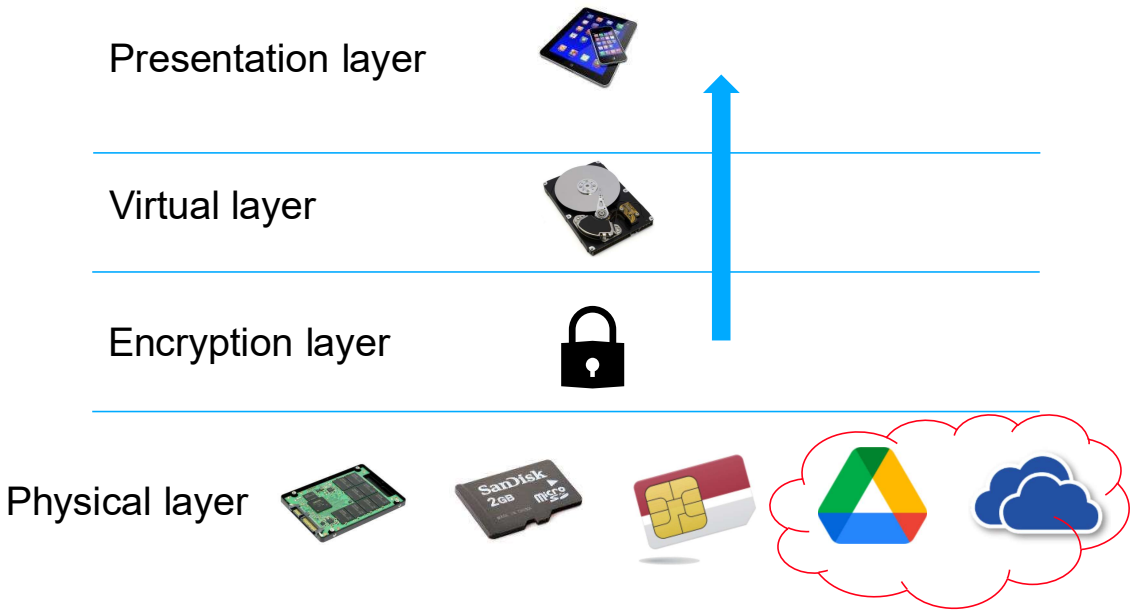
Physical layer 

Lost information:
- Physical data location
- Data Source

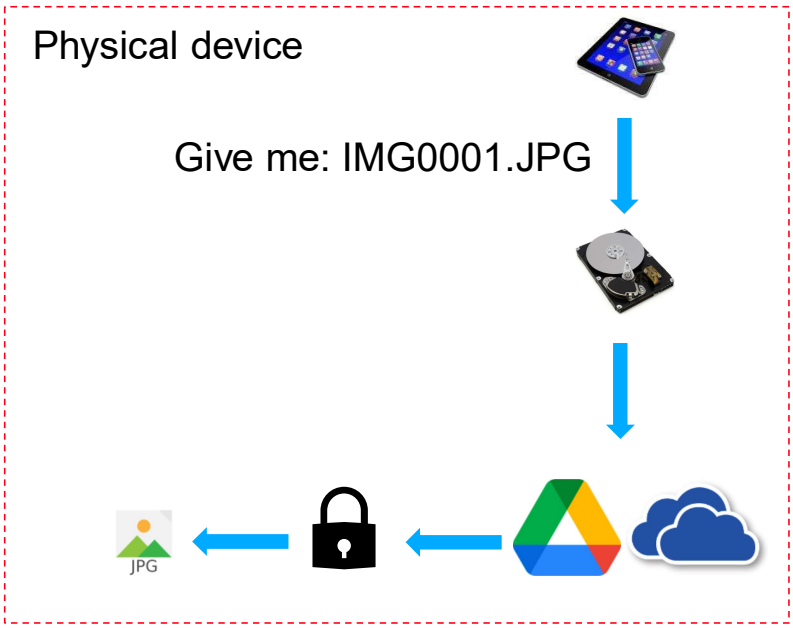
Physical to Logical



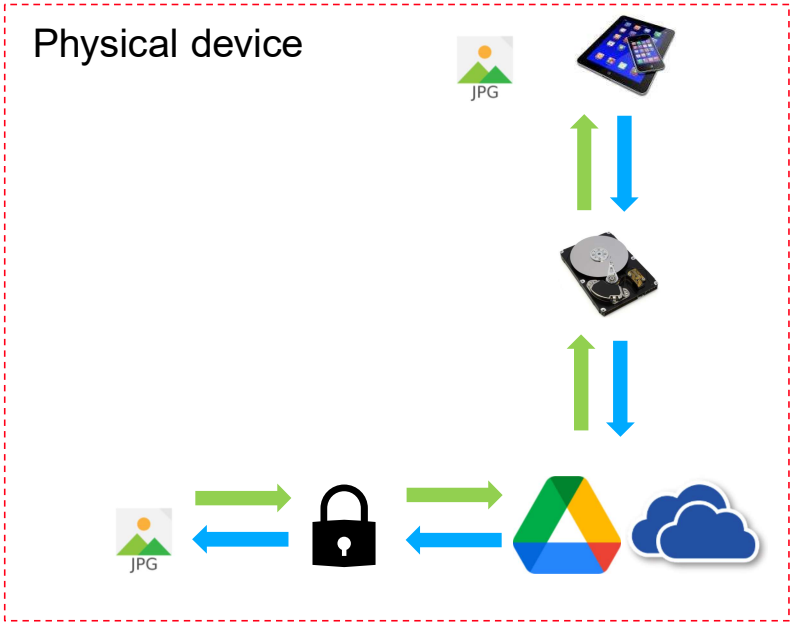
Physical to Logical



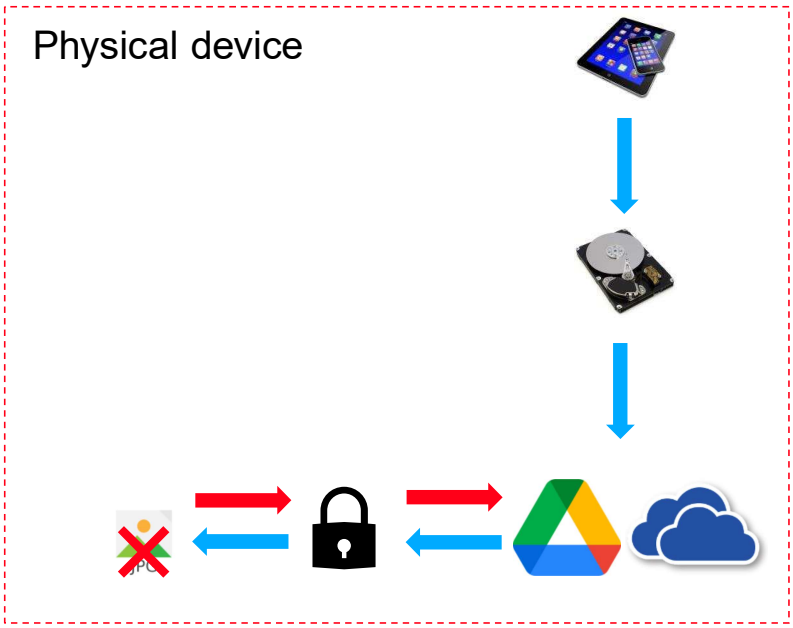
Physical to Logical



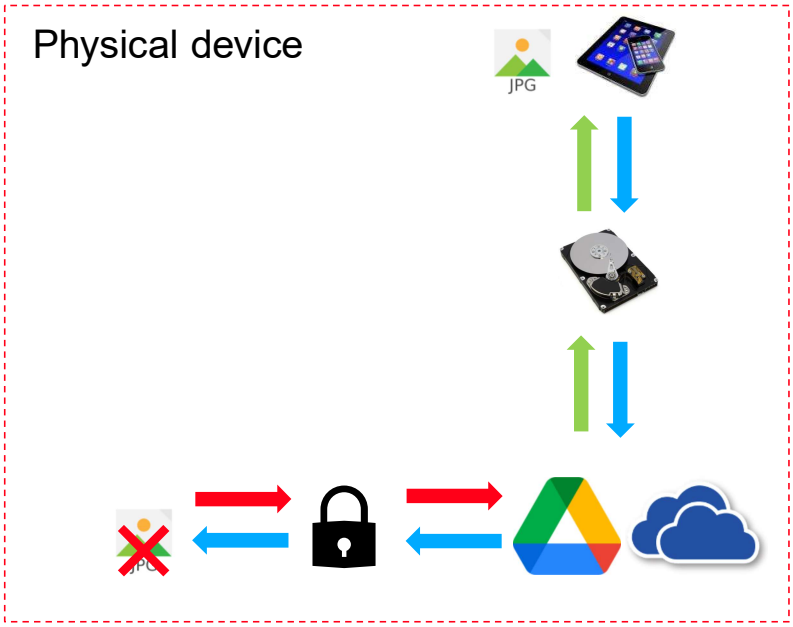
Physical to Logical



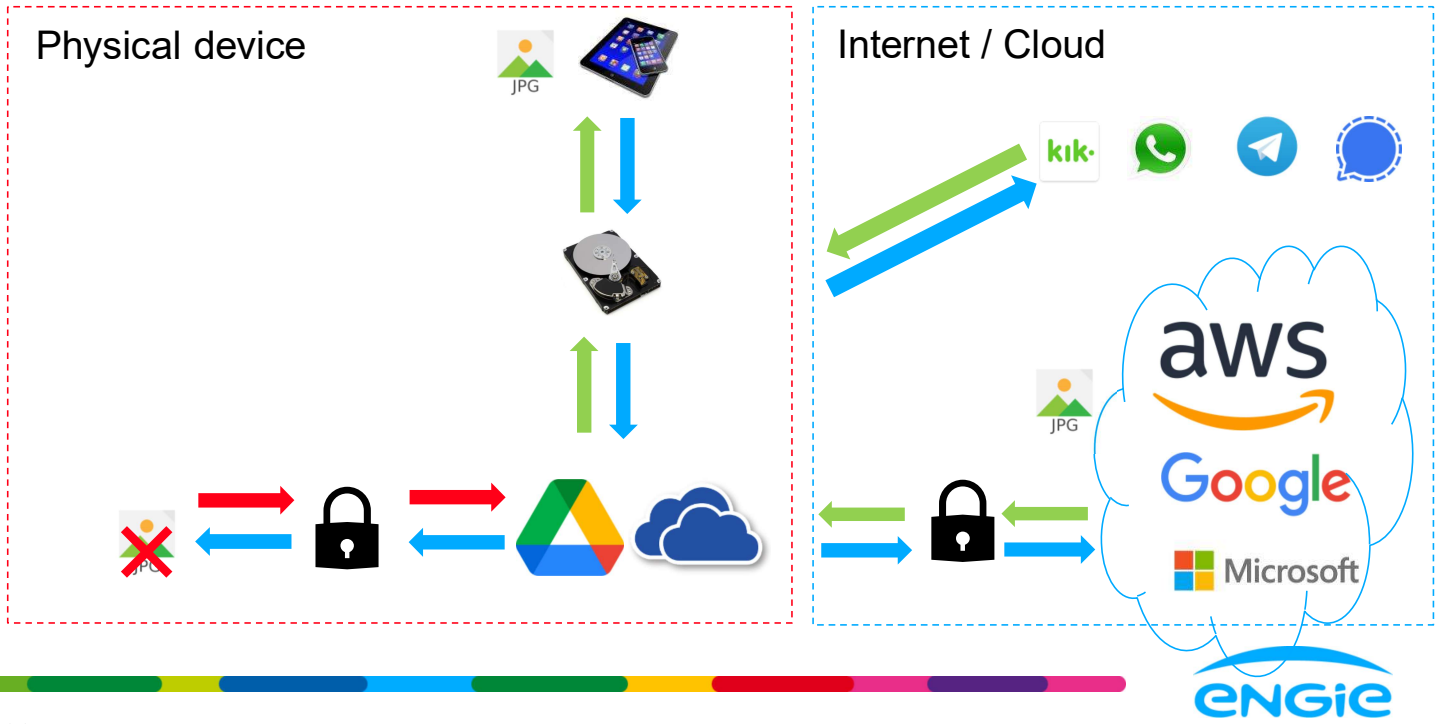
Physical to Logical



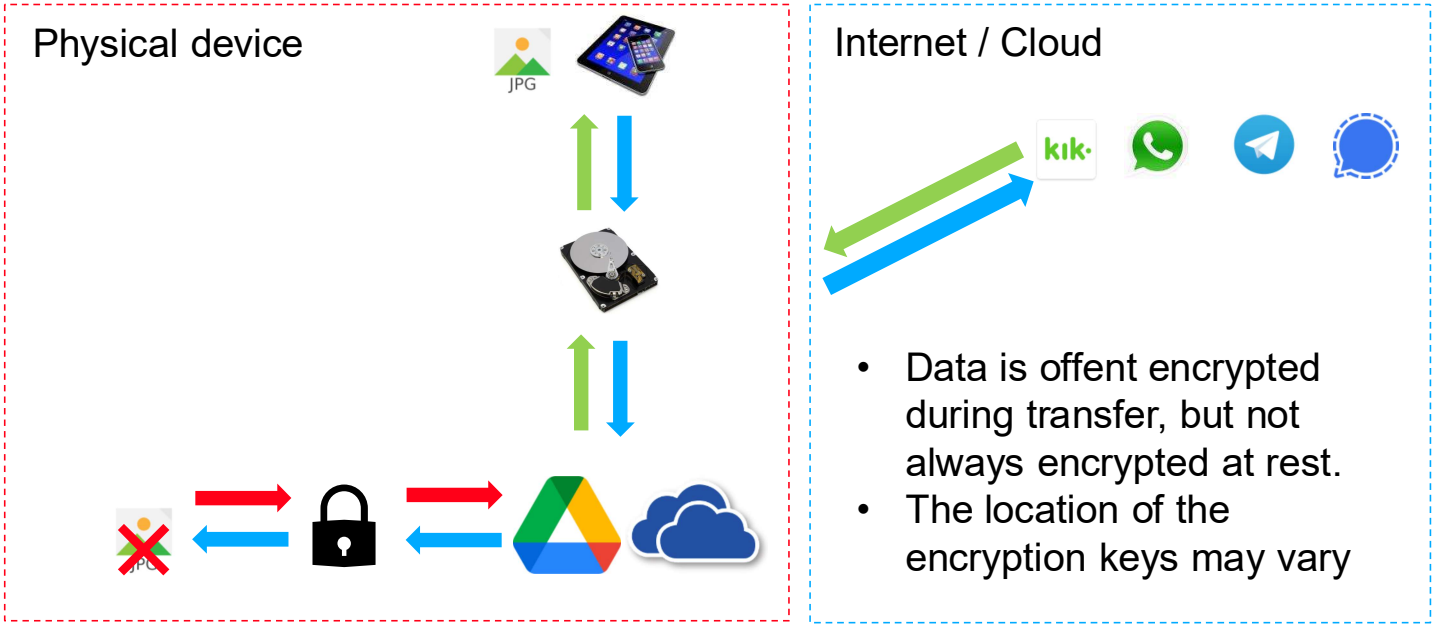
Physical to Logical



Physical to Logical



Physical to Logical



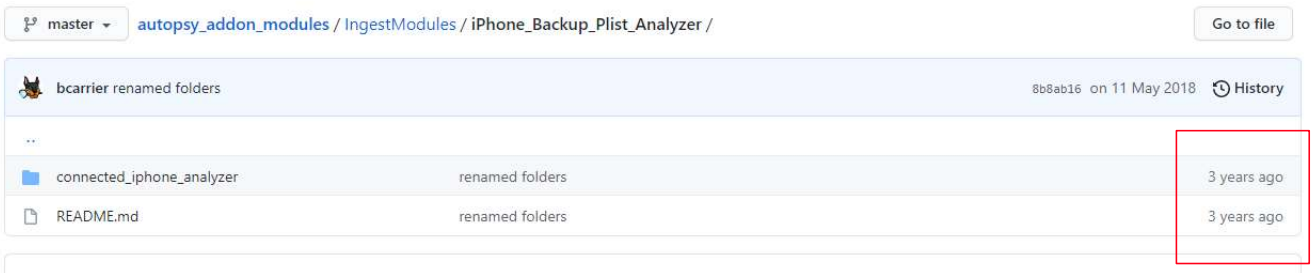
- Data is offent encrypted during transfer, but not always encrypted at rest.
- The location of the encryption keys may vary

Extraction challanges

- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.

Extraction challanges

- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.



Extraction challanges

- Pythsical extractions are becoming a thing of the past. Data is often lost.
- While Open source tools exist for forensic analysis the development in the field is very fast.
- Are we allowed to connect to the cloud to retive the data not on the device?

Summary

- When handeling mobile devices access to the pythsical storage is restricted
- Encryption added aditional layers or virtual access
- Data location is not always known by the user.
- Data is presented in a usniform way to the user.


ENGIE
energie,
technologie
en optimisme
ERA
Europäisches Rechtsakademie
Academy of European Law
Académie de Droit Européen
Accademia di Diritto Europeo
Thank you!
Co-funded by the Justice Programme of the European Union 2014-2020