




**Understanding, Accessing
and Analysing Data**



This Event will start at 0900hrs

25th May 2021

Communications Data

Jill Dixon (Cuff)
25th May 2021


Jill Dixon (Cuff) 1980





Jill Dixon (Cuff) 2021






- Police Cadet
- Police Officer
- Support Staff FCR / PNC Administrator
- Home Office Accredited CDI SPoC
- Digital Media Investigator
- Malicious Communications Specialist
- Cyber Crime Trainer
- UK Communications Data Trainer
- International OSINT Trainer (public/private/military)
- SPoC Trainer / Subject Matter Expert – UK College of Policing
- Office for Communications Data Authorisations

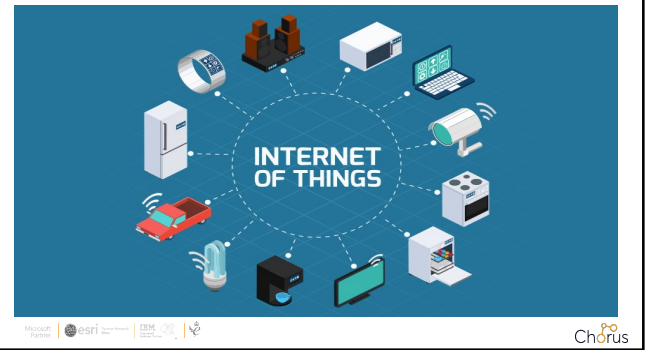


Topics

- Current legislation & Obtaining Data
- Attribution
- Types of Data Available
- What's New?

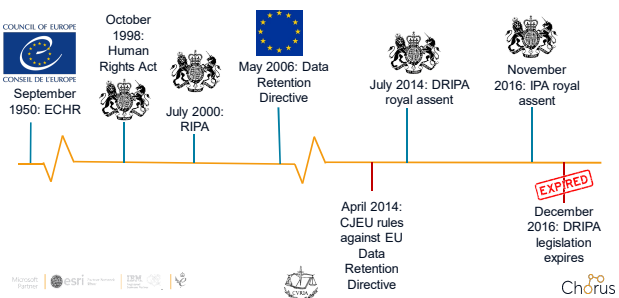
Microsoft Partner | esri | IBM | Chorus

Chorus



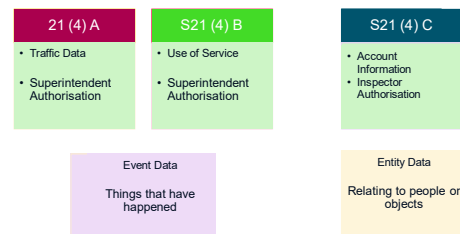
Chorus

The history of the legislation



Chorus

INVESTIGATORY POWERS ACT (2016): WHAT'S NEW?



Chorus

Serious Crime Definition

- An offence that attracts a prison sentence of at least 12 months
- An offence by a person who is not an individual (i.e. a corporate body)
- Where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose.
- An offence which involves, as an integral part of it, the sending of a communication or breach of a persons privacy

Microsoft | esri | IBM | Chorus

Chorus

New Offences:

- OFFENCE OF MAKING UNAUTHORISED DISCLOSURE
- OFFENCE OF KNOWINGLY OR RECKLESSLY OBTAINING COMMUNICATIONS DATA

Microsoft | esri | IBM | Chorus

Chorus

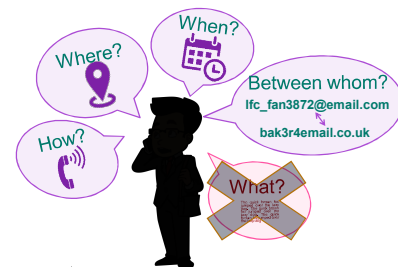
Public Authorities



Microsoft | esri | IBM | Chorus

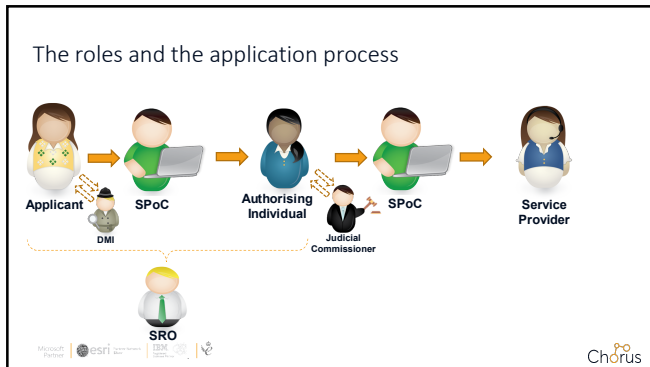
Chorus

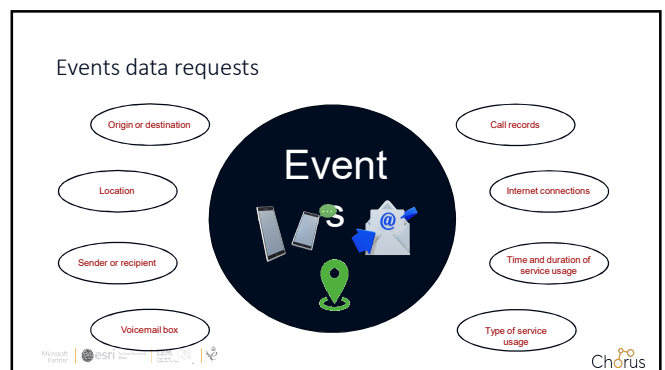
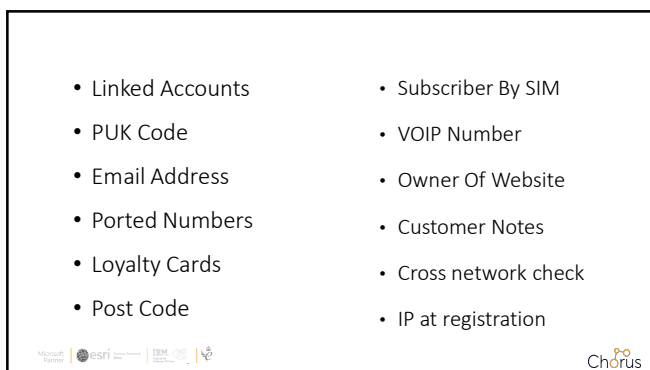
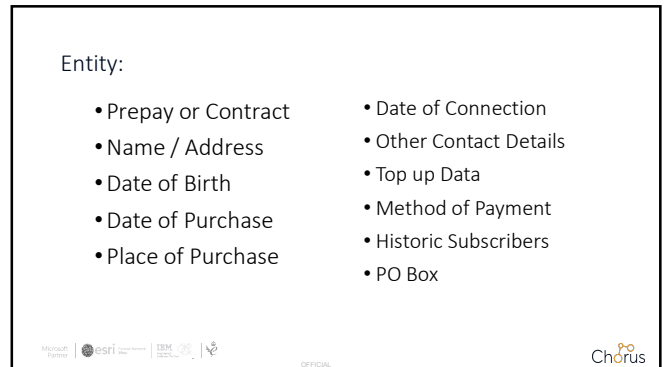
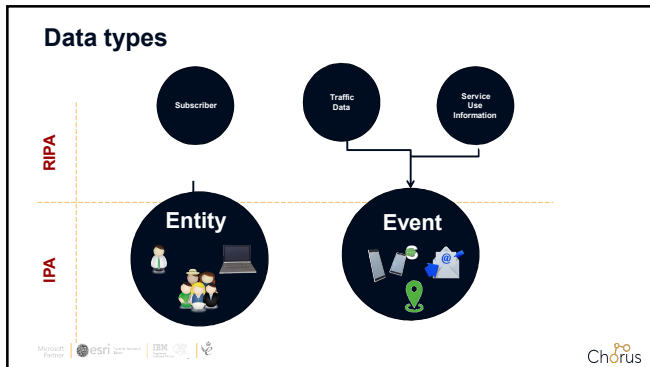
What is Communications Data?



Microsoft | esri | IBM | Chorus

Chorus





Events:

- Record of Delivery
- Incoming Data
- Historic Data / Cell Site
- FF Historic Traffic Data
- Cell ID
- Historic Data
- SIM Swapping
- (Voice/SMS/MMS
- Cell Dumps
- Outgoing Call Data



Chorus

- Copy Bills
- Tap Files
- HLR (Near live trace)
- How Switched Off
- Internet (GPRS)
- IP Log History
- MAC log in locations (Public)
- IPAR
- Mobile IPAR



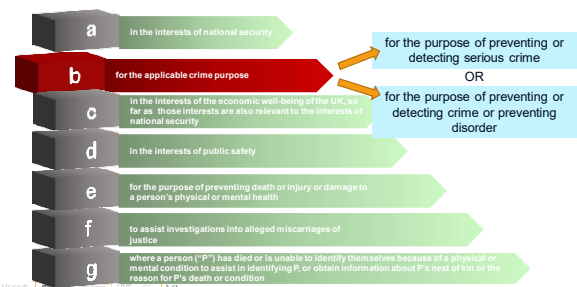
Chorus

Statutory purpose



Chorus

Applicable crime purpose



Chorus

CD and Sensitive professions



Microsoft Partner | esri | IBM |

Chorus

Attribution



Microsoft Partner | esri | IBM |

Chorus

EVIDENTIAL ATTRIBUTION

“Data becomes meaningless if devices/communication methods cannot be attributed to subjects”

Microsoft Partner | esri | IBM |

Chorus

Possession



Constructive Possession



Adopted in interview



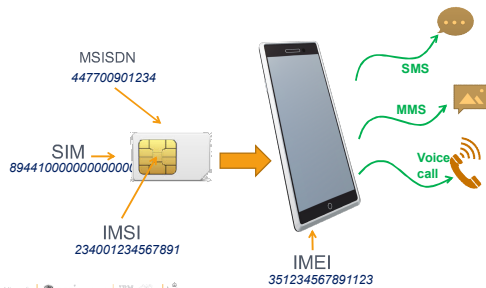
Witness statements / CHIS



Microsoft Partner | esri | IBM |

Chorus

Key identifiers and events



What can we do with the data?

- Lifestyling
- Associates
- Patterns of travel
- Put subject in the vicinity of a certain location
- Prove or disprove alibi
- Locate missing / vulnerable persons

COPO – Crime (Overseas Production Orders) Act 2019

Where an International agreement is in place:

- Enhance our international cooperation capacity
- Enable LE and prosecutors to access electronic information directly and more swiftly
- An overseas production order will be granted by a judge

COPO – Crime (Overseas Production Orders) Act 2019

This Act creates a new, standalone legal regime for UK law enforcement agencies and prosecuting authorities to obtain stored electronic data outside the UK.

“This Bill will give law enforcement officers and prosecutors the ability to get crucial data, from overseas providers, under strict legal safeguards and where an international arrangement exists, if they need it for their criminal investigations and prosecutions.”

Rt Hon Ben Wallace MP, Minister of State for Security and Economic Crime.”

So what's new?

- Telematics
- Internet Connection Records
- Mobile iPar
- Uber
- Amazon
- Google
- Air BnB
- What 3 Words
- My Hermes



Chorus

Telematics



Chorus

Telematics:

Telematics:

DPA to manufacturer to obtain VIN (EXCEPT VW, they want IPA to disclose all information, including VIN).

When VIN is known, IPA request to all 4 networks as the SIM will roam, and ask for IMSI, IMEI & ICCID (can't do anything with ICCID but with IMSI & IMEI can get location data).



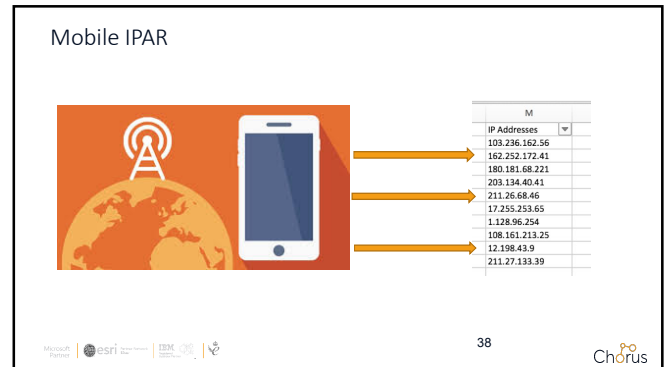
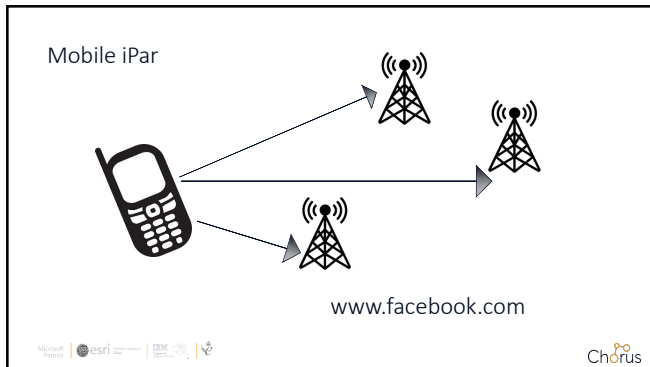
35

Chorus

Internet Connection Records (ICRs)



Chorus



6,000 & 10,000 customers sharing one IP address.

Minimum of 3 IP addresses

Filter 1: Type of phone

Filter 2: Location

Logos: Microsoft, esri, IBM, Chorus

What can UBER do for us?

Logos: Microsoft, esri, IBM, Chorus

Trip details – the route from A to B

- Time & date of the journey
- Vehicle details
- Driver + photograph
- Pick up / drop off
- Bank details (card or Paypal)

Data Protection Act



Chorus

- Mobile number to access the app
- Email address
- CDRs between driver & rider

Investigatory Powers Act



Chorus

What else?

- Split fare with associate
- GPS data available

Name of customer is not verified



Chorus

Amazon

Postal Operator or Not?

DPA for personal data:

- Name
- Address
- Telephone number
- Email address
- Payment details

IPA for CD:

- IP log on history
- Tracking

Identifiers:

- Phone number
- Street address
- Email address
- Bar codes
- Tracking numbers

44



Chorus



Google account is gateway to all products and services
 Typically Gmail account
 IP from Message ID
 Street view
 Google payments
 You Tube

Android

Target Identifiers

- IMEI / MEID
- Google Account email address
- Serial number with Make & Model



WHAT IS TIK TOK?


Legal process:

- Name of TO TikTok UK
- Context and offence under investigation
- Format must be non editable legal process
- Provide valid user account identifier, where possible a screenshot of the users profile page.



Entity Data IPA - BSI

- | | |
|---|------------------------------|
| • Registration First & Last name (if available) | • Sign up method |
| • Registration Date & Time (UTC) | • Device Registration ID |
| • Tik Tok Username | • Device registration Model |
| • Other Social Media Details (if available) | • Registration Location |
| • Mobile / Phone Number | • IP Address at Registration |
| • Email Address(es) | |








Identifiers:

- Address
- URL of Listing
- Name & DOB
- Phone number
- Payment Instrument
- Reservation code

Data Provided:

- BSI to include
- Name
- Payment method / bank account
- Reservation History
- IP Logs
- Content of communication (MLAT)


Must request Non Disclosure


...and finally

- In the last decade, over 95% of all offences / crimes had an element of Comms Data.
- Do you feel confident that you know what's available and equipped to submit a successful application for Comms Data?
- Avoid re submissions
- Up to 40% of applications are returned for rework by the SPoC
- Over 12440 applications were returned for rework by OCDA in the last year.

3 day applicant course available...



- The course outlines relevant legislation, including Investigatory Power Act, Human Rights, CPIA & GDPR.
- The role of the Applicant
- Single Point of Contact
- OCDA
- Senior Responsible Officer
- Investigatory Powers Commissioners Office
- What is Communications Data
- Retention periods



- Statutory purposes
- Gradings, including the urgent oral process
- Attribution
- Less intrusive means to obtain the data (Open & Closed Source opportunities)
- Entity & Events for cellular and internet devices and services.
- Investigating websites, Emails, Games devices, social media etc.
- With practical examples and practice applications.

Microsoft
Esri
IBM
UK Home Office

Chorus

Please feel free to contact us for further details

Thank you



j.dixon@chorusintel.com

Tel: 07557 017445

Chorus