Webinar 3 March 2021

Venetic/Encro:
Understanding and Evaluating the Technical Evidence

Peter Sommer
www.pmsommer.com

Aim of Webinar

- Much of the evidence tendered in Op Venetic/Emma involves novel investigatory and forensic methods
- Some of this has impacts on admissibility arguments
- The aim is to enable legal professionals to evaluate the specific evidence adduced against their clients
  - ➔ To advise clients
  - ➔ To set a defence strategy

Reliability and Continuity

Three issues:

1. **Venetic uses number of novel investigatory and forensic techniques**
2. **Digital Evidence is highly volatile; the "scene" must be frozen and conclusions drawn from that state of play**
   - **We need to know how this is achieved**
3. **French refuse to provide full witness statements describing precise methods and tools – citing French national security laws**
   - **At first instance judge allowed hearsay evidence from Jeremy Decou and others But allowing hearsay does not make evidence reliable**

How EncroChat worked

- **Customers bought subscriptions – and were given a handset.**
  - ➔ **They were identified to the system by a nickname, not their real name**
- **All communications between handsets was mediated through a server (or possibly several servers)**
- **At each use the server authenticated the handset and allowed contacts with other authenticated handsets**
- **Server had the ability to update handsets with new apps – and switch off handsets**

How EncroChat worked (1)

- Contacts were end-to-end encrypted
  - → Encryption requires a generic algorithm plus a unique key
  - → At the outset of a conversation handsets exchanged information with each other and agreed a unique session key
    - Session key renewed for each message
  - → Encryption and decryption take place on the handsets
    - The only places where the clear unencrypted messages can be read is on the handsets
  - → In theory this means that the server cannot read the traffic between the handsets.
    - (Some experts dispute this but we will not cover this here)

How EncroChat worked (2)

- Users had the option for messages to be deleted on both originating and receiving handsets
  - → Usually 7 days – in evidence expressed in seconds – 604800
    - "Burn time"
- Also featured:
  - → Notes
  - → Images
  - → Voice
    - But we get no instances of this in evidence or disclosure

How EncroChat was breached

- Handsets were resistant to direct attack by LE
  - → Data port engineering/debugging facility had been removed
- The only way to get inside them was over-the-air – that was only possible via the server
- French/Dutch JIT acquired a copy of the server to understand how it worked
  - → and covert EncroPhones to see how they worked
- French/Dutch crafted an "implant" to be sent over the air to each handset
- Implant was able to harvest some of the contents

How EncroChat was breached (1)

- Implant was able to harvest some of the contents of the handset
  - → Not that different from some forms of regular malware, where the object is to collect financial and private data for onward selling and exploitation
- When it received an appropriate command from the server it disgorged its harvest – which was then collected
  - → Many times during the investigation
- All this required extensive testing
  - → To see if things worked effectively
  - → To keep the activities secret/covert in order to avoid thwarting the investigation

>>>> Operation Emma

How EncroChat was breached (2)

- French/Dutch formed a Joint Investigation Team (JIT)
- NCA was not part of that but had fairly close contact
- NCA received data via Europol

What we get from the Evidence

- Operation Emma was supposed to run from 1 April 2020 to 1 July 2020
  - → Encro detected breach on 12/13 June
- Historic messages already on handset
  - → Class 1
  - → Usually on 7 days' worth because of "burn time"
- "Live" messages collected 01/04/2020 – 13/06/2020
  - → Class 2
  - → Collected on many different occasions

What we don't know about Op Emma

- How far overall arrangements – Server plus Implant - were subjected to external testing / quality assurance
- Precise coding and tasking of Implant
- Frequency with which implant was asked to disgorge its harvest
- Where the harvest was sent to for law enforcement use
- Any analysis carried out by French/Dutch JIT prior to its passing on to Europol – and thence to the NCA
  - → Selection of records limited to specific jurisdictions, threat to life issues
- Any further review to check for contamination, errors during these processes

What we don't know

There is no continuity of evidence and no testable provenance before material is delivered via Europol LFE to NCA.

Once in the hands of the NCA, we have:

- → Continuity statements
- → Explanations of activities
- → Provision of software code used to analyse

NCA passed their findings to local ROCUs

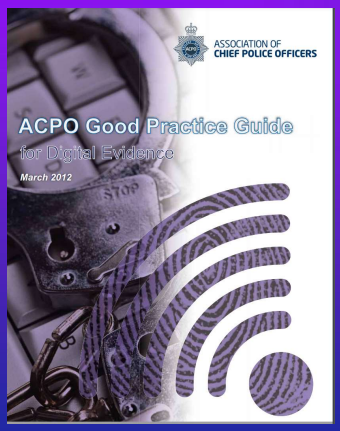
- → We don't always have information about the analyses ROCUs carried out, eg for attribution

Reliability Tests

ACPO Good Practice Guidelines for Digital Evidence

- **Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.**
- **Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.**
- **Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.**
- **Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.**

Reliability Tests (1)



ACPO Good Practice Guidelines for Digital Evidence

Every single one of these Principles are violated!

Reliability Tests (2)

CPR 19 Practice Directions

- **Sufficiently reliable scientific basis** (not ***Daubert v Merrell Dow***, but…)

19A.4 In its judgment in *R v Dlugosz and Others* [2013] EWCA Crim 2, the Court of Appeal observed (at paragraph 11): "It is essential to recall the principle which is applicable, namely in determining the issue of admissibility, the court must be satisfied that there is a sufficiently reliable scientific basis for the evidence to be admitted. If there is then the court leaves the opposing views to be tested before the jury." Nothing at common law precludes assessment by the court of the reliability of an expert opinion by reference to substantially similar factors to those the Law Commission recommended as conditions of admissibility, and courts are encouraged actively to enquire into such factors.

Reliability Tests (2)

(a) the extent and quality of the data on which the expert's opinion is based, and the validity of the methods by which they were obtained;

(b) if the expert's opinion relies on an inference from any findings, whether the opinion properly explains how safe or unsafe the inference is (whether by reference to statistical significance or in other appropriate terms);

(c) if the expert's opinion relies on the results of the use of any method (for instance, a test, measurement or survey), whether the opinion takes proper account of matters, such as the degree of precision or margin of uncertainty, affecting the accuracy or reliability of those results;

(d) the extent to which any material upon which the expert's opinion is based has been reviewed by others with relevant expertise (for instance, in peer-reviewed publications), and the views of those others on that material;

(e) the extent to which the expert's opinion is based on material falling outside the expert's own field of expertise;

(f) the completeness of the information which was available to the expert, and whether the expert took account of all relevant information in arriving at the opinion (including information as to the context of any facts to which the opinion relates);

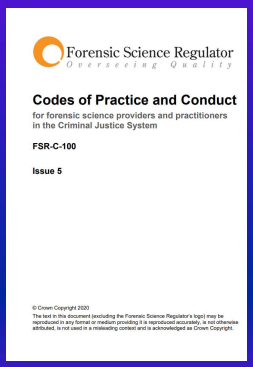
(g) if there is a range of expert opinion on the matter in question, where in the range the expert's own opinion lies and whether the expert's preference has been properly explained; and

(h) whether the expert's methods followed established practice in the field and, if they did not, whether the reason for the divergence has been properly explained.

Dove J never applied these to the "reverse engineering" evidence

Reliability Tests (3)

Forensic Science Regulator


Forensic Science Regulator
Overseeing Quality

Codes of Practice and Conduct
for forensic science providers and practitioners in the Criminal Justice System

FSR-C-100

Issue 5


Forensic Science Regulator
Overseeing Quality

Codes of Practice and Conduct

Appendix: Digital Forensic Services

FSR-C-107

Issue 2

The general requirement is that all technical methods and procedures used b a forensic unit shall be validated. This section details the principles of the requirement for validated methods, the next section, **21.2 Validation of methods**, details the required processes.

Even where a method is considered standard and is in widespread use, scientific validity will still need to be demonstrated. The topic of verification of the validation of adopted methods is discussed below although many of the other validation steps are likely also to apply. If a method is being newly included in the forensic unit's scope of accreditation and validation has not been conducted at the laboratory site where it is to be implemented, the forensic unit will have to follow the adopted methods procedure, which ends in the production of a validation library and statement of completion as well as demonstrating the method works in their hands.

Method Validation
Verification
ISO 17205

NPCC
Transforming Forensics

Reliability Tests (4)

ETSI Standards for Telecommunication Evidence

ETSI
World Class Standards

ETSI TR 101 943 V1.1.1 (2001-07)
Technical Report

Telecommunications security;
Lawful Interception (LI);
Concepts of Interception in a Generic Network Architecture

Audit trails:

- **Show warranting authority**
- **Tamper proof records**
- **All activities and procedures**

Not followed!

Why are these tests necessary and important?

- **Digital data is highly volatile – changes take place all the time on computers, laptops, mobile phones: we must freeze the scene** at a specific date and time
- **Two classic methods of digital data acquisition / scene freezing:**
  - → **Controlled report from database** – eg bank records, telecommunication records
    - Supporting witness statement
  - → **Forensic image copy** – formal use of hardware, software, procedures
    - Supporting witness statement + result disclosed to defence

NCA Data Processing

- **Once data is in the hands of the NCA we get proper continuity of evidence**
  - → **Physical, Logical**
- **But note that NCA passed data on to local ROCUs, who then carried out further processing**
  - → **To draw attention to what they thought significant**

Reliability: Visible Anomalies in CSVs

Typical findings:

- Duplicated lines
- Separate messages with separate correspondents apparently occurring simultaneously
- Many separate messages between parties apparently bunched up
- Missing messages?

BUT Pros may give you a "filtered" exhibit

- Local IO may have decided CSVs too complex and offers a "clearer" version
- (Nothing wrong with this in principle provided you can test against the source)

Reliability and Admissibility

We need to know:

- **Traffic data captured in the course of transmission ?**
  - → **Requires interception warrant, Part 2 IPA – intelligence use only, not admissible**
- **Data captured from storage ?**
  - → **Requires equipment interference warrant, Part 5 IPA – admissible**

We need to understand the technical environment:

- **Is data captured from handset transient or permanent?**
- **At point were messages available for viewing by the recipient?**

What we don't have

- **Full disclosure, detailed technical explanations from French**
- **Test environment – server + handset + implant**
- **Copies of programs, coding**
- **Forensic images of:**
  - → **Server**
  - → **EncroChat handset *before* implant**
  - → **EncroChat handset *with* implant**

What we do have

- *Output* of Operation Emma
  - As delivered via Europol to NCA
- Generalised knowledge of Android operating system

Evidence & Conclusions of Court

- Work of defence and prosecution experts relied on the above available material
  - Including the CPR 19.6 experts' meeting
- Defence expert concluded interception
- Dove J concluded storage
  - Dove J did not use/follow Practice Directions tests on "sufficiently reliable scientific basis"
- Court of Appeal followed Dove J

Did anybody have enough material to form a firm view?

Evaluating the Evidence

- Unreliable evidence may be corroborated against other types of evidence
  - Copies of messages on other EncroPhones
  - Photographs
  - Cellsite co-location with regular smartphones (IMEI corroboration)
  - ANPR
  - Physical surveillance
  - Discovery of Class A narcotics / unexplained wealth
- Evidence may be challenged by alibi

Evaluating the Evidence: Expert Instruction

- You must obtain the phone files as described by Luke Shrimpton
  - Search for anomalies
  - Compare against any "filtered" exhibit
  - Decide if you wish to pursue "admissibility" agenda
- Consider any potential corroborating material
  - or absence thereof
- Check the detail of attribution claims
- Consider the content of text messages against alleged activities in any alleged conspiracy etc