[redacted]

Report on computer-based electronic evidence

Duncan Campbell

CONTENTS

		Page
1	**Credentials and experience**	1
2	**Instructions and responses**	3
3	**Issues, contexts and approach**	7
4	**Research and forensic methods and sources**	15
5	**Operations Emma and Venetic data management**	19
6	**Operation Emma exfiltrated data package analysis**	28
7	**Overlapping Stage 1 and Stage 2 activity**	41
8	**Speed of interception and exfiltration**	43
9	**How EncroChat secure message interception worked**	44
10	**The effect of EncroChat Equipment Interference**	50
10	**Equipment interference technical processes**	56
11	**Analysis of NCA Operation Venetic Data Processing**	59
12	**NCA experience of Equipment Interference**	65
13	**Reliability of computer-based electronic evidence**	67

Figures

1	Operation Emma data flow	20
2	Operation Venetic data flow	22
3	Alice sends an EncroChat Message to Bob	48
4	The effect of EncroChat equipment interference	50
5	Interception of transmission inside Alice's phone	52
6	Interception of transmission inside Bob's phone	52

Tables

1	Equipment interference and interception actions	33-34
2	Realm file captures in Venetic data packages	42
3	Irregular CSV files in Schedule of Events	71

Annexes

A	Relevant experience	(i)
B	Judgments citing reports	(iii)
C	Instructions and cases	(iv)

Exhibits:

1	Exfiltrated Data Report	DC/1
2	Live Message Timing Analysis	DC/2

(Criminal Procedure Rules, r. 16. 2, r., 19; Criminal Justice Act 1967, s. 9)

Statement of Duncan CAMPBELL (Over 18)

This statement consisting of 73 pages is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have willfully stated anything which I know to be false or do not believe to be true.

1. I am an expert witness on electronics, computers, and telecommunications. I received a First Class Honours degree in Physics from Oxford University in 1973. I further trained in Operations Research at the University of Sussex in 1974 and 1975. I am a Doctor of the University (D.Univ) of the University of Sussex, *honoris causa*. I am a Senior Visiting Fellow to the School of Law, Politics and Sociology of the University of Sussex. I was formerly a Consultant to the Technology Faculty of the Open University (U.K.) (1974-1977), consultant to the European Parliament (1998-2001), a visiting Fellow at the University of Bournemouth (2000 – 2013), and at the Electronic Privacy Information Center, Washington D.C. (1999-2000)

2. My company is 2QQ Ltd. 2QQ Ltd registered in Scotland. My business partner is Mr Matthew Fowler. Mr Fowler and I married in 2017. Mr Fowler holds a Computer Science degree from the University of Reading and is employed by our company as a Programmer and Analyst.

3. I have provided expert evidence on scientific and technical forensic matters concerned with computers, communications, electronics and electronic equipment in over 200 civil and serious criminal cases since 1979. I have prepared over 200 expert reports over the past decade. From 2004 to 2016, I was registered on the former Law Society and Sweet and Maxwell Expert Witness Register and shown as "checked". I have given oral and written evidence to Crown Courts in England, to the High Courts of England and Scotland, to Sheriff Courts in Scotland and to the Court of Appeal, in civil and criminal cases. My reports have been cited at in judgments all levels of United Kingdom jurisdictions, including the Supreme Court of the United Kingdom, and in the European Court of Human Rights. Further details of relevant experience and forensic expert work are attached as Annexe A. A list of

citations in reported cases is attached as Annexe B. The list of cases in which I have been instructed is attached as Annexe C.

Instructions and responses

4. I have been asked by Kenyon McAteer Solicitors, Liverpool to interpret and report on computer-based electronic evidence concerning the EncroChat network supplied to the North West Regional Organised Crime Unit (NWROCU), by the UK National Crime Agency (NCA), and supplied to NCA by the *Centre de Lutte Contre les Criminalités Numériques (C3N)* (Cybercrime Centre), Pontoise, France, a division of the French Gendarmerie Nationale, as follows:

(a) **Question**: In relation to two stages of interference on mobile phones in the UK, described as Stage 1 (Historical Data Collection) and Stage 2 (Forward Facing Collection) is it accurate to describe either stage as collecting data stored on the device?

Response: Stage 1 collects data stored on a device and does not collect live information. Stage 2 collects live messages while being transmitted through the devices. Stage 2 also collects a large amount of additional information, other than messages, from the phone, such as live reports of mobile radio technical connections, location data or occasions when a user enters a lockscreen password.

(b) **Question**: If the stages differ in the processes they are carrying out, are you able to explain how they differ?

Response: I am able to explain and have tabulated how and why the Stage 1 (Historical Data Collection) and Stage 2 (Forward Facing Collection) processes differ. I have determined the distinct and different aspects of the Historical Stage and the Forward Facing Stage by

processing relevant information from all classes of data transmitted from infected UK phones during the course of Operation Emma.

(c) **Question**: From what you are able to discern, is either Stage causing modifications to the system by doing a "relevant act" to a communication at a "relevant time" while the communication is being transmitted (i.e. a "live" interception).

Response: So far as available evidence can be interpreted, modifications to devices resulted from a single act of infection with the C3N implant. It is possible but cannot be determined with certainty that additional modifications were also made at later dates. Stage 2 contains procedures embodying doing a "relevant act" to a communication at a "relevant time" while the communication is being transmitted. Stage 1 procedures do not appear to do so.

(d) **Question**: In your view is the interference with communications on phones in the UK during Stage 2 consistent with the description of Jérémy Decou and others that it is "live" interception?

Response: Yes. Extensive evidence supports the description given by M Decou.

(e) **Question**: Is there anything you have discovered specifically in the way the NCA have analysed the material you have analysed that is consistent with M. Decou's description of Stage 2 as live interception?

Response: Yes. All the material I have analysed is consistent with M. Decou's description of Stage 2 as live interception. None of the material I have analysed is inconsistent with M. Decou's description of Stage 2 as live interception. I observed that the programs comprising the NCA Operation Venetic Data Processing Suite, used in this case, process Stage 1 stored data internally within the suite using the source label "realm" or

"db", whereas it processed Stage 2 live intercept using the source label "live".

The Operation Venetic Data Processing Suite thus processed stored "realm" and "live" intercepted messages using two separate different and distinct sets of data inputs, programs and processes. This labelling was retained in disclosed "machine readable" data sets, such as I have analysed and reported on. This labelling has been omitted from "human readable" outputs used by police forces and in evidential products that I have examined.

(f) **Question:** In light of your other answers, is the description of Stage 2 that is relied on by the Prosecution accurate?

("Stage 2 (forward facing collection) communications (chat messages) on the EncroChat devices will then be collected on an ongoing basis. The messages are collected when they have been stored on the EncroChat devices.

Simultaneously the messages are sent via the chat server but they will not be collected in transmission, they will be collected from the devices")

Response: No. This description mixes the processes used in Stage 1 and Stage 2. It does not describe the Stage 2 live process. The statement that "The messages are collected when they have been stored on the EncroChat devices" is true of Stage 1 and false in relation to Stage 2.

(g) **Question:** Noting that the Schedule of Events (SOE) relating to EncroChat material used in Operation Subzero appears to contain inconsistencies, anomalies and potential inaccuracies are you able to determine whether the transcription of the Raw data of the EncroChat

material into schedules is an accurate and reliable presentation of the EncroChat material?

Response: It is impossible to determine if any or all of the original Raw EncroChat data is complete and accurate, for reasons of unreliability and paucity of information about provenance. I am not able to propose any means of verification or certification that would be likely to be possible or successful in that respect. With that qualification, the processes used to handle EncroChat material to and through the Europol system and within NCA do not appear to have caused, or be likely to have caused significant further inconsistencies, anomalies or potential inaccuracies. Handling and analytic procedures used inside NWROCU to present and support evidence have been inadequate and inadequately explained and appear unreliable.

(h) **Question:** If not, are you able to determine how, and in what way it is inaccurate and unreliable?

Response: It is impossible to determine if any or all of the original raw EncroChat data is inaccurate and/or unreliable, including because there is no underlying or different information currently available to use to check.

(i) **Question:** What more information, if any, would you require to ensure that the information that has been presented is an accurate and reliable representation of the EncroChat material?

Response: It is impossible to determine if any or all of the original raw EncroChat data, or final processing and presentation is complete and accurate, for reasons including failure to comply with the Principles of Computer Based Electronic Evidence promulgated by the National

Police Chiefs Council (formerly ACPO). Intermediate processing of EncroChat data by NCA does not appear to raise serious issues.

Issues, contexts and approach

5. My understanding is that:

(a) The stated and clear position of the French and Dutch police officers who jointly investigated EncroChat, and of Europol and Eurojust, who supplied data and evidence to the United Kingdom, is that under French national defence secrecy law they are prohibited from providing information or explanations as to how data used in NCA Operation Venetic - and thus in the case of *R v Coggins and ors* - was collected and processed as the result of acts of equipment interference taking place in the United Kingdom. I understand that this exclusion also applies to other police officers and services, without exception;

(b) The French component of the investigation was Operation Emma. The Dutch component of the investigation was Operation Lemont. Dutch and French police officers together formed a Joint Investigation Team (JIT). The United Kingdom was not a member of the JIT. The NCA was invited to be a recipient of information obtained by the JIT from Operation Emma and Operation Lemont;

(c) Members of Europol had access to live feeds of information from the operation. The United Kingdom did not. Except where real time filtering checks in Europe indicated a potential imminent threat to life or of serious violence, the UK and NCA only received collated and collected daily assemblies of information relevant to devices within the UK;

(d) On commencement of equipment interference activity on 2 April 2020, live message intercepts, location information and other data began to stream to a French run collection server, amounting to millions of events being reported daily from tens of thousands of infected EncroChat devices;



(e) On 2 July 2020, Europol published a diagram (above) [1] illustrating participant countries and describing the operations as "interception and analysis of millions of messages exchanged between criminals planning serious criminal acts. Announcing the results of the joint operation Europol, Eurojust, the French Police, the Dutch Police, the French Ministry of Justice, and the Dutch prosecution service jointly issued a detailed statement describing the work of the JIT as "intercept", adding

[1] https://www.eurojust.europa.eu/sites/default/files/2020-07/2020-07_Infographic-Encrochat-Case.pdf

"For an important part, these messages were read by law enforcement in real time, over the shoulder of unsuspecting criminals".[2]

6. My understanding is that an alternative view of relevant facts, proposed by the Prosecution, is that Stage 2 Live activity was accurately described in the terms put in question 2 (f) above. The key sentence is "The messages are collected when they have been stored on the EncroChat devices." If this statement is factually accurate, it requires evidence that the live messages were collected from a storage area forming a normal part of the device's functioning, before interference.

(a) The first sentence of the passage quoted is "Stage 2 (forward facing collection) communications (chat messages) on the EncroChat devices will then be collected on an ongoing basis." In isolation, this statement is true.

(b) The final sentence of the passage quoted is "Simultaneously the messages are sent via the chat server but they will not be collected in transmission, they will be collected from the devices". In isolation, this statement is confused and could be misleading. If it is read after the second sentence, it is misleading, particularly because of the way it is constructed in three sections:

(c) The first part of the final sentence, "messages are sent via the chat server" is correct;

(d) The second part "they will not be collected in transmission" is not clearly defined as to what transmission means in this context. If transmission in this context specifically means only transmission through the chat server, or transmission over the Internet or radio systems, or both, it is accurate.

[2] The Europol reference to "an important part" appears to be a reference to the Stage 2 Live phase.

(e) The third part "they will be collected from the devices" is also accurate, but only in isolation. When juxtaposed with the second part, the effect is to set up a false antithesis between "transmission" and "the device". Transmission also occurs within the device, as described fully below. As crafted, the sentence is misleading, for the reason that the antithesis is false. Each of the three clause can be true, simultaneously; i.e., a message can be "collected from the devices" and also "not collected in transmission [through the chat server or on the Internet]" and also "simultaneously ... sent via the chat server"

7. The core issue is whether or not Stage 2 Live messages are "collected when they have been stored". I have investigated this issue carefully from multiple technical perspectives, including :

(a) How does an Android device of the make and model used by EncroChat phone operate, in relevant ways?

(b) How did an EncroChat device store messages normally?

(c) How did the EncroChat chat app work when sending and receiving and storing messages?

(d) Does data in the Operation Venetic Data Package provide information about whether equipment interference during Stage 2 collected messages from storage and/or as they were being transmitted through the device?

(e) Is the timing and speed of data transmission discernible or calculable from Operation Venetic Data Package data more consistent with the assertion that "the messages are collected when they have been stored" or is the data seen more consistent with the statement by the investigators responsible for the activity that messages "were read by law enforcement in real time".

8. Multiple detailed statements about technical issues concerning equipment interference and interception are included in the witness statement of NCA Deputy Director of Investigations Matthew Horne of 8 October 2020. Mr Horne states that he is not a technical expert on interception or equipment interference.

9. A Europol meeting on Operation Emma was held on 19-21 February 2020. NCA officer Emma Sweeting attended the Europol meeting as an NCA delegate. Mr Horne states that prior to the meeting he required delegates, of which Ms Sweeting was one, to report back to him after the meeting and:

> "Confirm that the data collected falls within the UK's definition of Targeting Equipment Interference (TEI) [3]rather than Targeted Intercept."

Horne also stated what he said was the position of the United Kingdom

> "The current UK understanding is that this will be TEI and not TI but this needs to be established for the purpose of authorities."

10. I have examined disclosed notes, memoranda and reports made by NCA and CPS officials when and after attending the February meeting, and also the earlier similar meeting in January 2020, so as to determine if they had apparently obtained any technical information or details or guidance bearing on the issue of whether or not Operation Emma (in Stage 2) was based on live interception as opposed to copying data from storage. The relevant notes I found either stated that was interception or was likely to be so, possibly even also so in Stage1,

11. I have read the witness statement from Ms Sweeting dated 28 September 2020. She states that, following the meeting, she sent an email to the NCA at 12.56

---

[3] The correct term, used in IPA 2016, is Targeted Equipment Interference

containing the description of the Stage 2 process in the same terms as on question 2(f), .

12. Mr Horne states that "the NCA delegation informed me that their conclusion was that this [Stage 2 collection] fell into the category of TEI, in summary because the data would be collected from stored data on the EncroChat handset devices and not in the course of transmission." This statement by Mr Horne provides a clearer and more scientifically testable articulation of the Prosecution position. In scientific terms, it is a hypothesis which can be supported or refuted by examination of evidence.

13. On page 12 of his statement, Mr Horne states that "my team assessed [the collection operation] to be TEI upon which as the Gold Commander for the operation I formed the same belief". Evaluating evidence for and against Mr Horne's hypothesis, or belief, is a central task in this report. Evidence bearing on the accuracy of Mr Horne's understanding of encryption and knowledge of equipment interference methods is described in Section 12 below.

14. NCA technical specialist Luke Shrimpton attended the same Europol meeting. Mr Shrimpton was also responsible for developing the Operation Venetic Data Processing Suite. I have reviewed the operation of the suite for this report. Mr Shrimpton's Europol notebook for the meeting has been disclosed. The first line of the first page of the notebook reads "looks like it's intercept".

15. Lower on the same page, an entry reads "Is the DB dumps intercept??". I presume that in this context "DB" stands for "database. If so, it would appear that Mr Shrimpton may have been considering the means of the copying complete databases of messages from storage on the EncroChat, and which would or could be information stored in or by the system before or after transmission. I address the questions raised in Mr Shrimpton's notes below.

16. Mr Horne's statement describes technical matters in support of his belief, over four pages. He states that he is providing "context" based on personal policing experience, having had "operational roles" in investigations that involved other criminal use of secure communications (CDSC), and that his experience includes occasions on which Targeted Equipment Interference (TEI) methods were employed.

17. Mr Horne states, twice, that "in my judgment" and based on personal knowledge, the systems used for Stage 2 Live phase of Operation Emma were equipment interference (TEI) and not interception, on the bases that:

    (a) "the collection of 'clear text' human readable unencrypted communication content data was entirely inconsistent with any other method of Technical Operation known to me";

    (b) "I was not aware at the time, nor am I aware now, of any other tactic that would enable the acquisition of unencrypted content data, due to the 'end to end' encryption factor".

18. To my knowledge and in my experience the collection of human readable unencrypted communication content data is routine to technical operations in policing and intelligence work, and has been so for decades. Technical tactics to enable the acquisition of unencrypted content data where an 'end to end' encryption factor is in place have also been used for decades. British authorities responsible for cybersecurity have reported on multiple methods of this kind, including recently. I describe processes and reports of this type below.

19. I am aware that s56 IPA sets out a general prohibition on the use of or reference to interception or to intercept-related conduct in proceedings, and also that this prohibition is limited by Schedule 3 (2) (1) (a) if the interception was lawful in accordance s6 (c) (i), which deals with a "communication stored

in or by a telecommunications system", when in accordance with a targeted interference warrant.

20. I am also aware that s4 IPA defines interception as requiring that a "relevant act" (including interference) is performed such that the content of a communication is made available to an unintended recipient at a "relevant time", which means "any time while the communication is being transmitted". While preparing this report, I have attempted to assist by providing information which might be relevant in relation to the meanings of "relevant act", "relevant time" and/or the context of "any time while the communication is being transmitted".

21. In preparing this report I have been assisted in carrying out data extraction and conversion and loading of Raw and JSON data file information and metadata, and of JAVA scripts by Mr Fowler.

22. Dr Ian Brown, currently visiting CyberBRICS professor at FGV Law School in Rio de Janeiro, has acted as a peer reviewer of the information technology and cyber-capabilities sections of this report. Professor Brown was formerly Professor of Information Security and Privacy at the Oxford Internet Institute and a Knowledge Exchange Fellow with the National Crime Agency. I have taken full account of and dealt with all matters raised in Professor Brown's reviews. I am responsible for all analytic data included in this report. I am solely responsible for all conclusions reached or opinions expressed in this report.

Research and forensic methods and sources

23. My central forensic task appeared at first to requiring researching a void - a context in which there appeared to be no information. I addressed this initial difficulty by a variety of means, described below. The most important part of this work has involved many weeks of detailed data analysis, testing and re-

testing, including submitting analytic work for peer review by a senior information scientist (Professor Brown).

24. To address the issues, I examined sets of documents and exhibits, conducted technical and literature searches, searched Internet databases and registries, and carried out forensic tests on the computer-based electronic evidence provided to the UK by C3N and its Dutch counterpart, working as the Joint Investigation Team (JIT) and sent to the UK via a Europol data transfer system located in The Hague.

25. Some evidence and productions in this case contain limited agreed basic disclosures about French technical methods of data capture, such as the start date, details of an "infection" operation, a "live" phase using captured data as confidential intelligence only, followed by a disruptive and well publicised takedown of the EncroChat system. Following the publicised Europol and Eurojust takedown of EncroChat on 2 July 2020, UK NCA officers began processing the information they had previously been sent for intelligence purposes to use in evidence.

26. I found that significant detail about technical operations, and about French research into the EncroChat network preceding the infection operation was included in multiple legal applications by French prosecutors, and in the warrants the Lille Court then issued. These are exhibited in French and in English. They include details of historical steps starting in 2019. These warrants, and the sequence in which they were issued, throw significant light on the planning and operational capabilities used in Operation Emma. For example, they reveal the method used to infect or implant EncroChat phones, and the physical and Internet location of an impostor server used for the infection operation. Open source registry information records attempts to reroute traffic going to EncroChat. Statements in applications by French prosecutors, combined with public records, mapped out the EncroChat server and control network

27. I confirmed that EncroChat devices used standard freely available and/or open source programs and systems, including the Android operating system, a cryptographic system called Signal, and a storage system called Realm, among others. This meant that EncroChat phones worked mainly using commonplace and openly available programs. Codes and components for these programs were available if needed at no cost and could be tested. EncroChat's designers made special purpose alterations to some standard functionality. The majority of these changes were advertised or well understood, and did not impede understanding. Many were acts of disablement intended to enhance users' security and privacy.

28. According to the JIT,[4] "EncroChat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port). It also had functions intended to ensure the 'impunity' of users (automatic deletion of messages on the terminals of their recipients, specific PIN code intended for the immediate deletion of all data on the device, deletion of all data in the event of consecutive entries of a wrong password), functions that apparently were specially developed to make it possible to quickly erase compromising messages, for example at the time of arrest by the police. In addition, the device could be erased from a distance by the reseller/helpdesk."

29. This information assisted in considering which features of the devices might appear normal on forensic investigation, and which might not.[5]

---

4 https://www.eurojust.europa.eu/sites/default/files/2020-07/2020-07_Infographic-Encrochat-Case.pdf *ibid*.

5 The statement that both cameras and microphones were disabled appears inconsistent with reports and evidence that users could take and send and store images and that they could make limited VOIP (Voice

30. EncroChat phones are adapted from the Spanish-produced BQ brand model Aquaris X2 Pro devices. The source code for the Android operating system used for these phones, or Kernel, has been published on the Internet [6] for over two years. At the start of infection, and during the Live phase, the C3N app routinely reported on the version of the operating system being used. This was version O.Z.218.20190622, the version available for download from the Internet

31. I was able to analyse and have here been able to report in detail on how the C3N implant (or "technical device" or "infection") [7] operated by studying the information it extracted or "exfiltrated". Exfiltrated information is generally called "Exfil". The Exfil data streams from infected EncroChat phones were rich in forensic information about times, locations, internal processes and events. They revealed many different capabilities and actions. They provide and indicate how the implant control system may have functioned. I have thereby been able to describe processes and times and steps involved, and to estimate how fast live intercepted messages were available to be displayed to police investigators, in "real time". I found that intercepted messages could generally be available at C3N within about 20 seconds, and often much less.

32. I have studied about 250 historical technical, legal and operational documents, mails and memoranda provided in evidence, disclosed as unused material, or provided in evidence for related Judicial Review proceedings, including French warrant applications and operational reports. I have examined, and reviewed the Venetic Data Processing Suite created by NCA and exhibited by NCA technical officer Luke Shrimpton. Under my direction and with my

---

Over Internet Protocol) calls, As there is no immediate issues of this type in this case of which I am aware, I have not investigated this aspect further.

[6] https://github.com/bq/aquaris-X2-Pro

[7] In this report I use the French descriptions "infection" and "infected" synonymously and interchangeably with alternative British terms, "implant" and "implanted". This alternate usage is also reflected in the evidence. "Implanting" or "infecting" in this context is an act of equipment interference, as defined by law. An implant or an infection can be method of lawful equipment interference, or it can be a consequence of lawful equipment interference.

assistance Mr Fowler constructed Venetic Data Loader (VDL) programs to ingest and sort aggregate raw files of EncroChat data supplied to NCA into components, placing these in a relational database for subsequent analysis. I then used relational database queries (Microsoft SQL) to analyse the provenance, pathways, metadata, content and timing of information exfiltrated from EncroChat users' devices during the investigation. I also researched the structure and use of "Realm" databases used by EncroChat on the Android platform to store user data, including messages.

33. Our VDL and Mr Shrimpton's suite had common functionality, but used different programming languages to derive distinct but overlapping results. The purpose of the NCA suite was to process a few selected information items from the data so as to pass this on in simple formats to other law enforcement organisations. The purpose of VDL was forensically to examine every aspect of the Exfil streams that could be relevant to the technical questions put to me. My use of VDL also served to see if Mr Shrimpton's suite delivered the same results from data as would be expected. A merit of two specialists undertaking some identical tasks using different technical tools is that the strength of any shared conclusion or result is enhanced.

34. I have read and considered the witness statements of and documents concerning Luke Shrimpton, Gregory Elliot, Emma Sweeting, Matthew Horne, Claire Meehan, Wayne Johns (NCA), Riaz Jakhura (CPS), Wilhelmus van Gemert, and Jérémy Decou.

Operations Emma and Venetic data management

35. Figures 1 and 2 below show how live messages and other information gathered from infected devices in the UK flowed through multiple countries, processes and relay systems so as to reach investigators and, ultimately, legal proceedings.

36. After 2 April 2020, when users of infected EncroChat phones exchanged messages via the EncroChat message server, copies of the intercepted messages were also rapidly transmitted over the Internet to C3N's app (application) server computers in France.

37. The first part of the data flow, shown in Figure 1 overleaf, was from devices to C3N. From the reported scale of Operation Emma implant activity, affecting tens of thousands of EncroChat devices in multiple countries, and from my examination of exfiltration rates seen in the Operation Venetic data for this case, it appears likely that once infections began the volume of data sent to the C3N server would have exceeded a million objects and uploaded files daily.

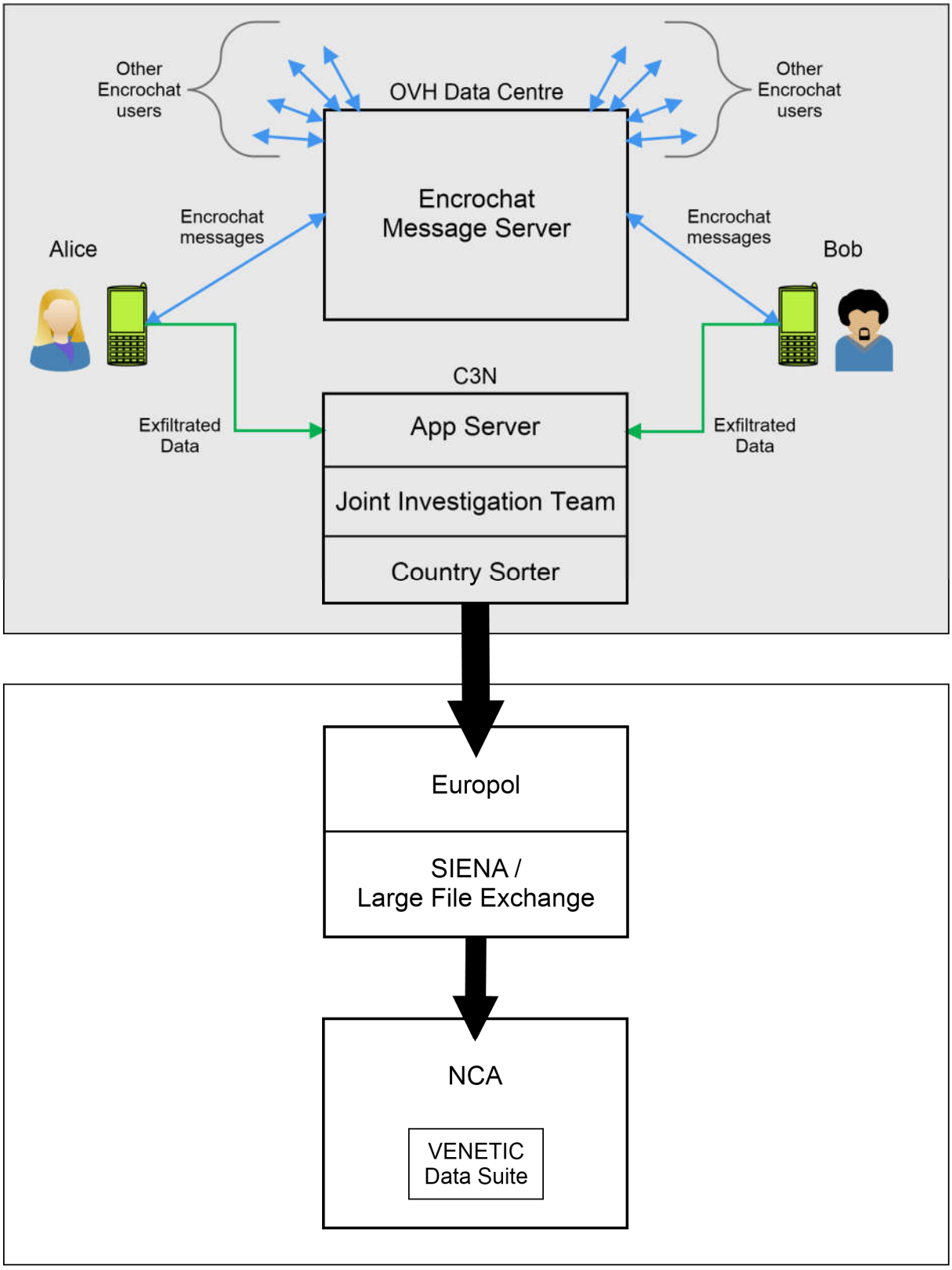
38. On receipt, processes on the C3N server first determined which specific device had sent the information, and the country in which it was then located. Although every Internet communication always includes the Internet protocol (IP) IP address of the sending device, this is not a reliable means of identification. IP addresses change as a user moves location, or from radio to wifi, or between networks, and for other reasons.

39. C3N's implant code caused each EncroChat devices to send the IMEI and IMSI at the start of every communication. These numbers were in effect a signature, permitting devices and accounts to be distinguished. A country code was also included. My understanding is that at C3N, the primary means of sorting incoming data was by using the IMEI at the start of the communication. Information was then sorted by country.

[This area has intentionally been left blank]

1

Operation Emma Data Flow



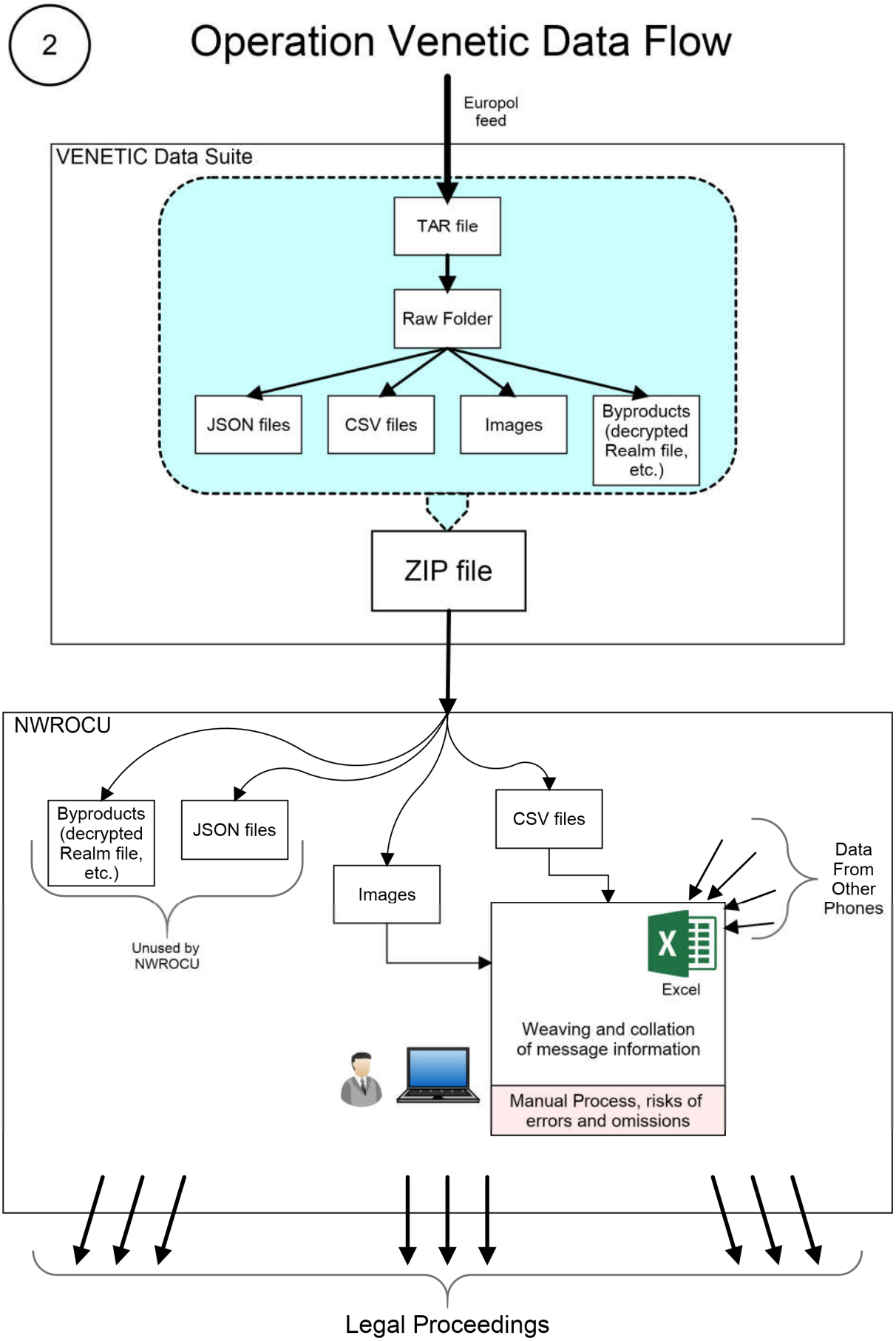
40. The second stage of the data flow was from C3N to French police forces, its Dutch partner organisation, and other organisations in Europol. Throughout Operation Emma, C3N in effect also acted as a post office, sorting and sending the relevant exfiltrated data to each co-operating country and national law enforcement agency concerned, providing that lawful exchange agreements were in place.

41. For the United Kingdom as set out in disclosed instruments negotiated between CPS, NCA and the French authorities, the method of delivery was that each day's data for devices identifying as being in the United Kingdom was collected into a single large file. Each daily file for the UK was sent to Europol headquarters in The Hague. The files were then stored on the Europol Large File Exchange system. The Exchange in effect served as an electronic mail drop for bulky items. NCA then collected the file, causing it to be transferred to London. At this stage, all the information was being transferred as intelligence, not for evidential purposes.

42. In addition to daily bulk information transfers, the French and Dutch JIT also managed processes intended rapidly to identify messages which might concern imminent threats to life. These were identified as potential "Threats To Life" (TTL). My understanding from the explanations given in evidence is that all intercepted messages first passed through a layer intended to identify possible threats, including threats to children, by searching for and then warning about relevant words or phrases, or argot or slang terms.

43. The third stage of the data flow was within the National Crime Agency. This is shown at the top of Figure 2, below.

[This area has intentionally been left blank]


2
Operation Venetic Data Flow
Europol feed
VENETIC Data Suite
TAR file
Raw Folder
JSON files
CSV files
Images
Byproducts (decrypted Realm file, etc.)
ZIP file
NWROCU
Byproducts (decrypted Realm file, etc.)
JSON files
CSV files
Images
Unused by NWROCU
Data From Other Phones
Excel
Weaving and collation of message information
Manual Process, risks of errors and omissions
Legal Proceedings

44. In his witness statement of 10 July 2020, Mr Shrimpton states that he was tasked on that day by NCA officer Greg Elliot to copy the original data received from Europol and used in Operation Venetic to a hard drive. The data was held on and copied from NCA servers. Shrimpton's statement implies that on unspecified dates prior to 10 July 2020 the entirety of the original Operation Venetic Data was "passed through "the NCA developed software". This may be a reference to the Operation Venetic Data Suite described in his later statements. His 10 July 2020 statement is unspecific and unclear as to what processes were followed.

45. From my examination of disclosed Operation Venetic Data Packages, as explained below, it appears that NCA processing operations causing new files to be created and inserted within the Europol data took place on dates including (but which may not have been limited to) 5 July, 6 July, and 7 July 2020. This effect of this processing activity has not been described or explained. I may not have detected other undisclosed processing activities when using only the specific forensic analyses described below.

46. Shrimpton states that he copied the "working copy" data resulting from NCA processing to a computer hard drive identified as LS/01/100720/HD/WC. He also states that he copied unprocessed master copy data sent from Europol to a second computer hard drive identified as LS/01/100720/HD/M.

47. Shrimpton further states (page 2 of his 10 July statement) that he was directed to remove data from LS/01/100720/HD/WC according to instructions in "a document" he was given. The document is not further described or identified in his statement. A possible inference from the statement is that the document contained details about 11 Operation Venetic Data Packages which were believed to hold suspected LPP material, but his statement does not make this clear. He states that he then copied the processed and redacted information from this working copy to hard drive LS/03/100720/HD/M. He then made a further working copy, exhibited as LS/03/100720/HD/WC.

48. The processed and redacted information on either copy of LS/03/100720/HD is therefore arguably the central exhibit in the chain of evidence for all Operation Venetic investigations and proceedings. As neither copy holds original evidence, should any issue arise in future in any fora, it would have to be resolved by comparing the contents of LS/01/100720/HD/M, the original master, with the contents of LS/03/100720/HD/M or LS/03/100720/HD/WC. For the sake of brevity, I refer to below to the information held on LS/03/100720/HD/M and the copy LS/03/100720/HD/WC LS/03/100720/hard drive as the "Source drive" *(sic)*.

49. Each Operation Venetic Data Package was prepared from information held or also present on the Source drive. Each package contains one zip file. Inside each zip file are one or more folders, labelled according the International Mobile Equipment Identity (MEI) of the device concerned. If a user of an EncroChat had caused their IMEI to be altered over time, the zip folder in the package holds an IMEI labelled folder for each number that was detected to have been used.

50. Within the folder, Mr Shrimpton placed the processed and redacted data from Europol into subfolder labelled "Tars". Within the Tars folder were compressed collections of information in files each labelled with the country code "GB", then the IMEI number, then the IMSI number, then the calendar date. Using this naming system, a file containing all exfiltrated data for 2 April 2020 for a device located in the UK with the IMEI 358098092001058 was called GB_358098092001058_204080812541354_2020_04_02.tgz. The second long number before the date is the IMSI.

51. The file extension "tgz" indicates that data in multiple computer files has been packed and compressed into a single file. Tgz files are compressed or "zipped" "tape archives". "Tape archives" are also known as tar files. The terms "tape archive", "tar" and "tgz" all originated at the time when large

computers stored and archived information and programs on reels of magnetic tape. Physical tapes are not now usually part of these processes.

52. In data packages provided by the NCA for this and other cases, information packages were prepared using the data suite. The first stage, described by Mr Shrimpton, and shown in figure 2 was to unpack the archive file so as to create "Raw" folders. Each Raw folder contains all the files of information collected on the specified day for a particular device.

53. For example, the folder GB_358098092001058_204080812541354_2020_04_02 contains 15 files. In this instance one of the files was an image. Four were security keys. Five were databases. One was a configuration file. One file was called json_data.

54. Each and every "Raw" folder contains at least one file called json_data. This single file contains every data object exfiltrated from the target device on the day concerned. Files such as the images and databases mentioned above were uploaded separately.

55. This data was analysed and processed by the Operation Venetic Data Processing Suite, devised by Mr Shrimpton and described by in his witness statements. He describes how the information available to NCA, plus relevant additional processed information he created and added, was compiled into distribution packages that NCA used internally, or sent to regional and national police forces and organised units, including NWROCU.

56. At NCA, according to statements by Mr Shrimpton and Mr Elliot, multiple stages of sorting, filtering, data extraction and format manipulation were carried out to produce easily human readable end product files, called "CSVs" (Comma Separated Variable files). This and other information flows in Operation Venetic are depicted in Figure 2 above.

57. By "manipulation" in this context I do not mean or intend to imply the use by NCA of processes intended to change the content or likely interpretation of any piece of data. For example and in general, to manipulate a word from lower case to UPPER CASE would change its format but not its meaning or significance.

58. In producing evidential materials in this case, NCA state they altered time stamps in evidential materials so as to be displayed as Coordinated Universal Time (UTC), without any time offsets. Offsets are the difference between UTC and the time displayed to a user from a computer clock. Offsets are applied because of geographical position (for example, Central European Time (CET) and/or because of daylight saving measures (for example, British Summer Time (BST)).

59. The standard use of UTC is good practice. It avoids confusion, complexity and difficulty for witnesses and the Court in making relevant time comparisons. An important proviso is that any offset adjustments to time data used in evidence should be clearly disclosed and explained on each occasion an offset is removed from formatted time information. In this report, I have followed the same practice as NCA staff by removing offsets to show UTC times only.

60. Mr Shrimptons's programs and codes have been disclosed, in three versions, as Exhibit LS/02/17/08/2020. With the assistance of programmer Mathew Fowler, and in a very brief period of time, I have examined their operations to the best of my ability. The time available to me to complete this report has ruled out any systematic attempt to audit, check or certify the programs, to any standard. Nevertheless, in inspecting Mr Shrimpton's work products and in creating and operating alternative processes with some of the same endpoints, I did not see grounds for substantial forensic concern (but see §64, below). If future or later or additional work reveals a matter or matters of concern, I will so report.

61. Mr Shrimpton describes how he prepared programs to inspect every "Raw" folder so as take desired and selected uploaded files and desired and selected parts of json_data files to prepare evidential packages in user friendly or "human readable" formats. As shown in Figure 6, all images found were selected for evidential use. Shrimpton then selected eight categories of information – "Contacts", "Deleted messages", "Geo", "Messages", "Notes", "Passwords", "Selectors", and "WiFi". These were drawn with from collected files.

62. The names of most of the categories are self-explanatory. "Geo" means geographical or location information. "Notes" refers to EncroNotes, a secure bespoke notepad app on EncroChat phones. "Selectors" means information about the devices. "WiFi" means information about local WiFi networks detected by the device.

Operation Venetic exfiltrated data package analysis

63. I have forensically examined the "Raw" folders of data supplied in Operation Venetic Data Packages so as to reach conclusions about the information sent from and the manner of operation and function of the C3N implants. For this purpose I mainly inspected json_data files and Encrochat.realm files. Json_data files contain live data and were compiled daily.

64. I found an issue of concern regarding the forensic integrity of the data suite. My inspection of three user packages, described below, identified 23 files which specifically were not exfiltrated from the relevant devices. Each of the 23 files had been created and prepared on 6, 7 and 8 July 2020, after the operation had ended and while being handled by NCA.

65. The files are either decrypted "realm" data stores, or files merely called "data". In his statements, Mr Shrimpton describes the methods he used to decrypt original Realm files, so as to extract and exhibit historical stored

messages. That process is clear and does not raise difficulty of itself, in my view.

66. It appears unwise and forensically improper to insert new and/or processed files into original exhibited material. There is no need to do so. At best such actions merely undermine the forensic integrity of the chain of evidence. At worst, such conduct could and does expose Mr Shrimpton or colleagues to inferences of tampering (even if there may be a valid available excuse). It could cause uncertainty for defendants or their representatives or the Court as to authenticity, creating concerns which would then have to be examined forensically. A better and safer course, in my opinion, would have been to place all and any decrypted or derivative or manipulated files in a separate and clearly marked folder.

67. I initially inspected and analysed json_data files using the Microsoft program Visual Studio Code. I noted that each Operation Emma/Operation Venetic exfiltrated json_data object had three distinct sections.

68. The first section of each json_data file is a timestamp called "server_time". I have not seen the name "server_time" used, referred to or explained in any French Operation Emma technical material in evidence. Nor have I seen the name "server_time" in NCA materials, nor in other evidence, exhibits, and unused material.

69. In each json_data file, the "server_time" label and the timestamp appears before the exfiltrated data. It appears to have been added after the data was transmitted to C3N over the Internet. I therefore infer that "server_time" means the clock time recorded by the C3N server in France when the incoming exfiltrated json_data object was saved to C3N's data collection.

70. The second section of each exfiltrated json_data object is labelled "metadata". The section labelled metadata includes information identifying the sending

device for the object and the SIM card within it. The metadata section includes the International Mobile Equipment Identity (IMEI) and the International Mobile Subscriber Identity (IMSI)

71. Absent deliberate falsification[8] each IMEI is unique to a single hardware device. In general use, a device is usually but need not be a mobile phone. Similarly, absent falsification, each IMSI is unique to a single SIM card. According to statements made to the Lille Court, lawful searches on OVH servers used by EncroChat found details of 66,314 SIM cards registered to EncroChat, all purchased from Dutch telecommunications provider company KPN.[9]

72. The form of the full information in the metadata section of the json_data file for each exfiltrated object is shown in the chart below.

Imei	358098090779879.00
Imsi	204080812115701.00
country code	Gb
Ota	O.Z.218.20190622
creation	1587128489180.00
creationTimestamp	1587128489180.00
timezone	Greenwich Mean Time
version	1.00
Path	Metadata
Size	3026.00

73. Country code has the obvious meaning. The name "ota" stands for "Over The Air". "Over The Air" is a method used in Android phones for distributing software, apps, programs, configurations, encryption keys, and operating system updates by means of radio connections between the device and the Internet. This specific entry identifies the EncroChat operating system, in use as the version used in BQ Aquaris X2 Pro devices, as explained above.

---

8 EncroChat phones reportedly included an app for changing IMEI numbers sent from the device.

9 https://www.kpn.com/algemeen/english.htm

74. The "creation" and "creationTimestamp "fields are both numerical values recording the then current time on the EncroChat device using a variation of a long-established format called "Unix time". Unix time was developed during the 1960s as part of the Unix computer operating system. It is a count of the number of seconds since 1 January 1970. The variation of Unix time used in these timestamps is a count of the number of milliseconds since 1 January 1970. [10] The numbers in the sample above resolve to the date and time of 7 April 2020, 1.01pm UTC. The timezone "Greenwich Mean Time" means that the time recorded is UTC and that no time zone offset has been applied.

75. I have not seen the json_data name "creation" used, referred to or explained in this context or as such in any French Operation Emma technical material. Nor have I seen the name "creation" in this context in NCA materials, nor in other evidence, exhibits, and unused material.

76. As it is within information sent by the C3N implant, I infer that the "creation" timestamp within a json_data object means the time on the sending EncroChat device at the time when the current data object was complete, packaged and encrypted prior to being transmitted over the Internet to C3N.

77. The clock time set on each EncroChat device is subject to error, inaccuracy and "drift". Once set by a user or the supplier, the internal computer clock runs continuously, subject to battery power being available. As with any mechanical clock, internal computer clocks can and do run fast, or slow, or both fast and slow at different times. It follows that any two computer clocks will not fully be synchronised to each other, unless synchronisation is carried by reference to a common external source. This affects results when comparing the times on any two clocks, if they are known or suspected not to be synchronised.

---

10 The presumed C3N server "server_time" time stamp is recorded in standard Unix time.

78. Computer systems called "Internet time servers" provide remote time synchronisation services for mobile devices and computers. An Internet time server is a server computer that continually obtains an extremely accurate time from a national or international standard reference service, and then distributes this information to clients over the Internet. Time services may also be supplied and operated by network service providers

79. During Stage 1, the Historical phase, messages and information about messages were captured only from copied Realm data stores, called Encrochat.realm. Each Realm store contains records of up to seven days of historic messages. Collection operations began on 2 April 2020. If a realm store was copied on 2 April, it might contain messages as early as 26 March 2020.

80. British Summer Time began on 29 March 2020. It follows that in individual cases, a small number of stored messages sent from or received on EncroChat devices within the United Kingdom before that date would record timestamps as Greenwich Mean Time (GMT). GMT is the same as UTC in this context.

81. After 29 March 2020 and until the conclusion of Operation Emma, the United Kingdom was on BST, one hour in advance of UTC. All Live message captures took place on or after 2 April 2020, meaning that only BST was in effect during the Live stage of Operation Venetic

82. Within the metadata object shown above, "version" might mean the version of the implant code then operating. The "path" "metadata" is the name of the listed data about the exfiltrated object. The "Size" element appears to be the number of bytes of information being sent. The third element of each json_data object sent to C3N, labelled "filedata", is the file of data copied and removed from the infected phone. In this context, if does not mean data about a file. From analysis, I found at least 12 distinct types of data object were sent to the C3N server, many times daily. These are listed in Table 2 below.

83. In Table 2, "action name" is the name I selected so as to describe the action by the phone performed as a result of equipment interference by the C3N implant. Each action exfiltrates or attempts to exfiltrated one or more types of data. The heading "Android process or storage areas accessed" refers to locations, storage areas or applications in or run on the EncroChat devices. The heading "Interpretation of purpose or intended purpose" is my explanation and interpretation of each action and its effect in exfiltrating items or collections of information from an infected device. Some of the actions appear to have failed, on occasions or systematically. This could indicate that the C3N implants did not function as its designers' intended or planned, on occasions.

84. In the limited time available, I have not been able fully to document the full and precise function and actual effect of each and every observed action by the C3N implant and listed in Table 1. As noted above, for the stated reason of French national defence secrecy, NCA and other British authorities, and the Court, have been given no information about the how the implant operated. When we (I and Mr Fowler) received and examined Mr Shrimpton's scripts (programs) they provided assistance in understanding the data. They showed how he had approached the same task as addressed here in the same way as we had. My understanding of the operation of the implant has therefore been built from the ground, founded on original evidence, as explained in this report, buttressed by understanding Mr Shrimpton's more guided and limited approach.

[This area has intentionally been left blank]

Table 1 Equipment interference and interception actions Part 1

Action name	Android process or storage areas accessed	Interpretation of purpose or intended purpose
Beacon	android/beacon	Sending IMEI, IMSI, a field called "phone" (this may have been intended to report the subscriber's telephone number. This appears not to have been used in EncroChat phones), SIM number, SIM operator, Mobile Country Code, Mobile Network Code, Network Operator Name; then sending Android Wifiscanner information, which should list the identity (SSID) of local wifi systems; but Wifiscanner collection appears to have failed to run in "beacon" exfil objects examined. This action might have failed in part because the EncroChat system did not use or access standard Android storage areas, by design.
Calendar	com.android.providers.calendar	Accessing or sending calendar information. Calendar is a db (database) file which uses the standard android sqlite format. This action may have failed because the EncroChat system did not use or access this standard Android storage area, by design.
Cell information	android/cellinfo	Presumably Intended to send mobile phone cell information. All cell information entries examined in Venetic data seen to date were empty. The implied function of the Cell Information action may be the same as for the Cell location action (below). This action might have failed because the EncroChat system did not use or access standard Android storage areas, by design.
Cell location	android.telephony.gsm.GsmCellLocation	Sending Location Area Code, Cell Identity, Primary Scrambling Code (used in G3/UMTS networks), Country Code, Mobile Country Code, Mobile Network Code, Network Operator Name
Contacts	com.android.providers.contacts	Accessing or sending contacts information. Contacts is a db (database) file which uses the standard android sqlite format. This action might have failed because the EncroChat system did not use or access standard Android storage areas, by design.
Files	android/files	Access Android general file storage area
Lockscreen	Lockscreen	Sending lockscreen password
Messages	com.esocrypt.chat.app.im/message	Sending intercepted message as transmitted, and message metadata

Table 1 Equipment interference and interception actions Part 2

Action name	Android process or storage areas accessed	Interpretation of purpose or intended purpose
Message files	com.esocrypt.chat.app.im/files	Sending message app files (not messages) (usually or always received or sent images). Message app files are copied and sent This does not include sending a copy of the Encrochat.realm data storage file, stored at the path (file location) com.esocrypt.chat.app.im/files/Encrochat.realm.
Notepad	network.encrochat.notepad	Sending Notepad file (encrypted)
SIM	apps.utility.virtualsim	Sending Virtual SIM (vSIM) information
Update	network.encrochat.updater	May indicate sending or receiving software or app updates
Multiple actions	**Actions included**	**Scope**
Sweep (1)	Contacts, Notepad, vSIM, Files, Message Files (not messages), Update, Calendar	This sweep action included seven discrete actions
Sweep (2)	Contacts, Notepad, vSIM, Files, Message Files (not messages), Calendar	This sweep action included six discrete actions
Sweep (3)	Contacts, Notepad, Files, Message files, Update, Calendar	This sweep action included six discrete actions
Sweep (4)	Contacts, Notepad, Files, Message files, Calendar	This sweep action included five discrete actions
Sweep (5)	Contacts, Notepad, vSIM, Files, Message files, Calendar	This sweep action included five discrete actions
Update and lockscreen	Update, lockscreen	This sweep action included two discrete actions

85. Many of the exfiltration events we observed included multiple actions at one time. I have labelled these as "Sweep" actions. The second part of Table 1, headed "multiple actions", lists and enumerates groups of combined actions found in the evidence. The Sweep actions also confirm and validate the distinction between Stage 1 (Historical) and Stage 2 (Live) of Operation Emma. From the analysis of the evidence as described below, the first action on infection of every device was to perform a sweep collecting multiple items. The items copied included passwords, stored images, device data, EncroNote entries (if any), contacts, and the Encrochat.realm file containing stored messages.

86. The data storage area or database inside each EncroChat phone is called Realm. The Realm storage file, called Encrochat.realm is encrypted. It uses a different and distinct encryption process and keys to the encryption on the message transmission path. Mr Shrimpton is aware of this. He deals with the problem in the Venetic Data Processing Suite which he developed and exhibits. This includes special processes and programs to decrypt Realm files so as to access stored data. Realm storage is not part of the transmission process. It is an additional function, which can be altered or reset by a user.

87. I have examined multiple copies of Encrochat.realm files taken from infected devices. These files were stored on the device. Programs or apps such as com.esocrypt.chat.app.im (the EncroChat messaging app), are executed or performed by the device. I found that EncroChat Realm data stores had been structured to hold eleven different classes of data object. These were "Account", "Capabilities", "Contact", "IdentityState", "Invitation", "Media", and "Message". The four final fields, associate with Signal, were "SignalConfiguration", "SignalIdentity", "SignalPreKeyRecord", and "SignalSession".

88. The Realm "Account" class includes the Username (such as "moonlitboat"), the AccountID, an encrypted password and a flag (indicator) possibly showing whether or not an account was activated. Realm "Message" data objects hold the texts of both incoming and outgoing messages, and metadata information about the message, such as sending times.

89. Metadata is data about other data. The metadata in the message objects are about the message. The message class metadata includes "contactID", "packetID", "type "(OUTGOING or INCOMING)", "dateCreated", "burn", "burnDate", "Status" (RECEIVED or DELIVERED), "dateRead ", and "Media". Realm "Media" files store images, including images recieved from other users.

90. Within the Realm data storage areas within the EncroChat app, the data object classes called SignalIdentity, SignalPreKeyRecord, SignalConfiguration and

SignalSession are distinct and recognisable parts of the Sesame encryption system used in the Signal Protocol. This evidence strongly supports Mr Shrimpton's statements (Section 9, below) that EncroChat uses the Signal Protocol.

91. After this examination and under my direction and supervision, Mr Fowler wrote and provided a series of scripts to systematically extract information from Raw files. The scripts are programs in the C# ("C-sharp") high level general purpose computer programming language. The scripts prepared by Mr Fowler are contained in a compressed file package called Venetic_Data_Loader.zip (VDL). [11]

92. VDL loads data from the original Raw exfiltrated material initially sent from infected EncroChat devices to the C3N server, then from C3N, via Europol, and then to the NCA, and provided to us. VDL created data tables for analysis using Structured Query Language (SQL). Structured Query Language (SQL) is a programming language used to extract data from relational databases, and/or for data management.

93. For the sake of speed and less complexity in preparing this report, all the analyses I have provided here are taken from a combination of three Operation Venetic data packages that have been provided to me. These are for the users and accounts identified as bladehedge, moonlitboat and kingwasp.

94. With the assistance of Mr Fowler, I prepared an SQL query Report_Exfil.sql so as to examine and report on all exfiltrated data for a user or a group of users.

---

[11] The Venetic Data Loader package was created as a Windows Forms application written in C#, targeting .Net (pronounced "dotnet") Framework 4.7.2, using the common Newtonsoft.Json library (version 12.0.3) for interacting with JSON data. Standard LinqToSQL run time infrastructure, part of the .Net Framework was used to connect to the database. I searched, inspected and analysed the VDL database on a local instance of Microsoft SQL Server 2012 (Developer Edition).

95. Using Report_Exfil, I identified, characterised and tabulated 27,194 exfiltration events which removed data from the three devices and sent it to C3N from April to June 2020. Of these, 26,499 are Json_data exfil objects. A further 695 events are occasions when files were copied from devices. A further 23 files which were never present on the devices were added to the original data in July 2020 as the result of processing actions taken by NCA described above. These are also listed in the Report Exfil table

96. Including files added during NCA processing, Report_Exfil identifies and provides information about 27,217 events. I transferred this information to an Excel file, Exfil_Report.xlsx. From Exfil_Report.xlsx, I created a PDF file Exfil_Report [BH-KW-MB].pdf. I produce this file as DC/1. I have used the suffix "BH-KW-MB" to connote that this exhibit is the combined Exfil Report for users bladehedge, kingwasp, and moonlitboat. The suffix distinguishes this Exfil Report from any other similar reports I may be asked to produce.

97. In DC/1, the first column identifies the user to which the row relates. Stage refers to Stage 1 (Historic data collection) or to Stage 2 (Live collection). Each Stage 1 event is a "sweep" action that includes copying stored messages by copying the Encrochat.realm data store. All other events are Stage 2 (Live). I entered the Stage information manually.

98. "Action time" is the time the action was completed and data ready for exfiltration, based on the clock time on the EncroChat device. "Exfil time" is the time between the "Action time" and the C3N receiving "Server time", as described above. "Implant functions" refer to the functions listed in Table 1 above. "Exfiltrated object" is the name of the file uploaded, when the implant action listed is "File upload".

99. The full Excel table contains three additional columns. The additional columns contain additional information about uploaded files only. These columns are not included in the PDF printout, DC/1. The extra columns in

the Excel file are the file size, the "hash" value and the name of the Operation Venetic folder containing the file. A "hash" value is a mathematical authentication technique. The technique used for these file hashes is called SHA-256. A hash is an integer computed from the entire content of the file using algorithms whose effect is that no tampered or altered file could have the same hash value, except at an exceptionally low probability.

100. The progress of each implant and every action it performed is set out in DC/2. Stage 1 "sweep" actions are shown in bold red on a yellow background. Stage 2 live message interceptions are shown in bold red on a light green background. All of the processes caused by equipment interference in the UK and also caused messages to be intercepted. They may be "relevant events". The events occurred between 2 April and 9 June 2020, at the times specified. These may be "relevant times".

101. The Exfiltrated Data Analysis, DC/1 is based and derived entirely from Europol provided information in the Data Packages examined, using repeatable processes.

102. For the user bladehedge, Stage 1 effects start at 18.42.35.35, i.e. 35 milliseconds after 18.42.35 UTC. Because of BST, this time would be seen by the user as 19.42. The first event is a sweep group of actions, as listed in the "Implant functions" column. This event includes an instruction to start sending the Encrochat.realm containing historic messages.

103. The first Stage 2 Live events affecting for bladehedge occur within in the same millisecond. The Cell Information action runs, fails, and sends no data. The Cell Location action then sends information about the country the device is in, and identifies the current serving mobile radio cell. This identifies the user's location. Two milliseconds later, the implant started sending files and images found on the device to C3N.

104. Stage 1 uploading affecting bladehedge continued until 18.48.39.39, six minutes later. This is when an Encrochat.realm exfil object was created on the device. Server times are not available for file uploads. This Realm file did not load correctly on this occasion. Possible reasons for this could be that the user was interfering by using the phone at the same time in order to conduct a text conversation. The C3N server could be expected also to be receiving very high volumes of traffic at this time, as thousands of devices reported in to say that they had been infected successfully, becoming "owned" and then sending back collections of files.

105. Twelve seconds after infection, user bladehedge is engaged in a text message exchange. The first intercepted message to be exfiltrated from the bladehedge device was created at 18.42.47.47 and reached C3N's server 23 seconds later. By the time the Stage 1 historical data collection phase is complete for this device, Stage 2 had already intercepted and relayed 13 text messages,

106. This Exfiltrated Data Analysis also shows that very frequent location tracking reports were sent, sometimes in the same second. I cannot currently offer any suggested explanation as to why location messages were sent so frequently. Because of this, during Operation Venetic, the position of the bladehedge device was reported on at least 6,240 occasions.

107. The device for user kingwasp was infected 8 minutes after bladehedge. The device for user moonlitboat was infected at 8.51 the following morning.

108. It appears that the designers and planners of Operation Emma would have expected a rich daily record of location and movement data, as well as clues from photographs, and the content of messages, and could use these to form or refute suspicions or conclusions about potential users of devices at particular times. For Europol members, the data positioned them both to electronically track criminal suspects as they went about their business, and to read their messages at the same time. Because of the Covid-19 pandemic, both

operations' intelligence-led phase fell within the period of UK and European lockdown, meaning that the observed range of travel (shown by the changes of radio cell sites or "masts" accessed) was unsurprisingly limited.

109. I wrote a second SQL query Report_Realm_Files.sql in order t**o** find every Encrochat.realm file uploaded from each user. I found 14 uploaded Realm files (called Encrochat.realm). Each realm file contains a single table of stored historical messages. This query also identified 13 additional files called Encrochat.realm.decrypted. These are the decrypted Encrochat.realm files created by Mr Shrimpton and then added to the exhibits.

110. All the original Encrochat.realm files found using this query are listed in Table 3 below. This list is a complete account of all occasions on which historic stored messages were copied (Stage 1), as opposed to live interception of messages (Stage 2) while they were being transmitted through devices. I have omitted the decrypted versions of these files created by the NCA. The NCA produced decrypted realm files are listed on the final page of exhibit DC/1.

Overlapping Stage 1 and Stage 2 activity

111. Technical evidence, data analysis and information in this report fully confirms and supports the description of the Live phase of Operation Emma by the police officers running it as fast live, real time interception. It refutes the belief promoted by Mr Horne.

112. Further refutation of his position also arises from my discovery that Stage 1 and Stage 2 processes operated side by side for up to seven days after infection, for the three users whose information we analysed. The initial infection sweep action was repeated multiple times: 4 times for bladehedge (2, 3, 5, and 8 April), 5 times for kingwasp (2, 4, 6, 7, and 8 April) and 4 times for moonlitboat (3, 6, 7, and 8 April).

113. This discovery came as a surprise. It came to light because of the detailed work I had carried out with the assistance of Mr Fowler. I have not seen any documents or evidence reporting or explaining this type of event. On detecting this, I re-checked the output "message" CSV files for these users created by Mr Shrimpton's Venetic Data Processing Suite. I found that his suite had, like our VDL, recognised and then parsed and grouped multiple calls from live interception and from multiple Encrochat.realm files, all exfiltrated from a single device.

Table 2 Realm file captures in Venetic data packages (listed by username)

EncroChat User	File Name	File Date and time	File Size	Sent in Europol container file name
Bladehedge	Encrochat.realm	02 Apr 2020 19:48:39	0	\GB_358098093363556_204080813446649_2020_04_02
Bladehedge	Encrochat.realm	03 Apr 2020 19:20:03	1200128	\GB_358098093363556_204080813446649_2020_04_03
Bladehedge	Encrochat.realm	05 Apr 2020 07:15:02	1200128	\GB_358098093363556_204080813446649_2020_04_05
Bladehedge	Encrochat.realm	08 Apr 2020 08:39:30	1200128	\GB_358098093363556_204080813446649_2020_04_08
Bladehedge	Encrochat.realm _1586372338533	08 Apr 2020 19:59:07	1200128	\GB_358098093363556_204080813446649_2020_04_08
Kingwasp	Encrochat.realm	02 Apr 2020 19:56:24	233472	\GB_358098092001058_204080812541354_2020_04_02
Kingwasp	Encrochat.realm	04 Apr 2020 19:45:07	233472	\GB_358098092001058_204080812541354_2020_04_04
Kingwasp	Encrochat.realm	06 Apr 2020 07:36:56	233472	\GB_358098092001058_204080812541354_2020_04_06
Kingwasp	Encrochat.realm	07 Apr 2020 19:41:12	233472	\GB_358098092001058_204080812541354_2020_04_07
Kingwasp	Encrochat.realm	08 Apr 2020 19:38:49	233472	\GB_358098092001058_204080812541354_2020_04_08
Moonlitboat	Encrochat.realm	03 Apr 2020 09:51:21	233472	\GB_358098092785213_204080812711363_2020_04_03
Moonlitboat	Encrochat.realm	06 Apr 2020 10:07:48	233472	\GB_358098092785213_204080812711363_2020_04_06
Moonlitboat	Encrochat.realm	07 Apr 2020 19:27:46	233472	\GB_358098092785213_204080812711363_2020_04_07
Moonlitboat	Encrochat.realm	08 Apr 2020 19:55:54	233472	\GB_358098092785213_204080812711363_2020_04_08

114. On inspection of Mr Shrimpton's CSV files, I found that up to 8 April 2020, the files contained multiple message entries. This was because the same message is found in live intercept, and also four or five additional times in Realm storage files. From re-examination of the suite programs, as described below, I saw that Mr Shrimpton's processing code correctly labelled calls seen in

Realm files as "realm" or "db" (database), and calls found in live traffic json_data files as "live". Regrettably, this information is omitted from the resulting CSV files provided and examined to date.

115. The reason for originally writing program code to omit data is not clear, as discussed below.[12] Had Mr Shrimpton's correct file parsing script of 6 August 2020 been used, the reason for multiple messages entries would have been clear to all involved in the process (including analysts working for NWROCU) as the messages would then be labelled "Live" for one copy and "Realm" for the other copies.

116. In summary: identical duplicate records were found both by our VDL application and by Mr Shrimpton's suite. We both extracted the same information from the same data sources while using different computer languages and programs. The common result provides compelling proof that any belief that the live messages came from storage would be false.

117. In theory, the designers of the C3N "rogue app" could have chosen to have copied new messages from inside the Encrochat.realm file on every occasion a message was sent or received. Had they done so in this case, each message would unambiguously have been collected only from the storage area on the device. The evidence found, and labelled, and reported, by Mr Shrimpton and myself confirms that, save for the occasional early overlapping described here, they did not do so.

118. Based on this analysis it should have been apparent to the NCA team no later than 10 April 2020 (when Realm file collection stopped according to the available evidence) that the incoming message data stream was not being collected from storage on the phone.

---

[12] See Section 11, Analysis of Operation Venetic Data Processing. I note in that section that Mr Shrimpton was instructed to write new Java code that disclosed all the information he had copied to JSON files, and that he did then create correct new code for that purpose. To date, I have seen no evidence that the revised code was used.

Speed of interception and exfiltration

119. With the assistance of Mr Fowler, I prepared a third SQL query Report_Message_Flow.sql so as to examine and report on the speed with which users' messages were copied and sent on to C3N from infected devices. This analysis provides further forensic evidence bearing on whether intercepted live messages might been have deliberately stored by the EncroChat application before being transmitted.

120. This information was exported to an Excel file, Message_Flow.xlsx. From Message_Flow.xlsx, I created a PDF file "Live Message Timing Analysis.pdf". I produce "Live Message Timing Analysis.pdf" as Exhibit DC/2. In DC/2, the first column identifies the user to which the row relates. "Message time GMT" is the date and time created, and is the same as the dateCreated field in the message metadata.

121. The original time has been corrected from BST to UTC/GMT, for the reason explained previously. "Exfile time GMT" is the time the intercepted message was completed, packaged with its metadata as an object for exfiltration. It cannot be determined from this data if by this stage the user's message and metadata had already been encrypted using codes and keys managed by C3N. It is a also a possibility that encryption inside the C3N app took place after this time. It would be extraordinary if the intercepted message were not sent encrypted. To do otherwise would carry a considerable risk that the fact of interception could be established by a competent technical person who was, or worked for, a user.

122. "C3N server time GMT" is the "server_time" timestamp added to the start of an exfiltrated data object after receipt at C3N. "From" is the name of the EncroChat sending user. "To" is the name of the EncroChat receiving user.

123. The final three columns in DC/1 calculate and report time differences. "Time to capture" is the time between the message being created by the user, and the time when the intercepted, packaged (and possibly already encrypted) copy was completed and ready for exfiltration from the device. Both times are derived from the same clock on the EncroChat device, so the comparison can be expected to be accurate.

124. The column "Time to exfiltrate" calculates the time between when the intercepted message package was ready for exfiltration and the time when it was received by the C3N server. This is the elapsed time the data package took in transmission over the Internet. In this case, the clocks cannot be assumed to be synchronised. The final column, "Time to reach C3N" is the time between a user completing or receiving a message and the time when a copy of the message was available at C3N.

125. Just under 100 of the intercepted messages are shown to have been captured and ready for exfiltration within the device in less than 100 milliseconds (0.1 seconds). The comparison of clock times on the EncroChat device also suggests that 85% (5,752 out of 6,484) messages were captured and packaged for sending within one second. Over 95% of user messages (6,478 out of 6,484) were packaged ready for exfiltration in less than two seconds.

126. The time then taken for an intercepted message to be available, read and processed at C3N appears from the final column of Exhibit DC/2 usually to have been matter of seconds. It also appears that the server and device clock times were nearly but not exactly synchronised, as some messages are implied by the difference calculation to have been sent up to one minute before they were ready to be sent. This suggests that the device clocks may for these users may have been running slightly ahead of the server clock.

127. My analysis detected groups of anomalous very large transmission delays. I found long calculated delays appeared on two dates only, 21 April 2020 and 2

June 2020, and only in relation to the user moonlitboat. In respect of users bladehedge and kingwasp, only one message is reported as having taken an exceptional time (more than one hour) to be copied. The reason for interception traffic for one user being delayed in this way is not immediately clear.

128. Outliers and exceptions are always expected to be observed for no immediately apparent cause in any complex large scale data analysis of this type. Other than some likely systematic errors affecting moonlitboat, there were a trivial number of outliers (5 periods greater than 100 seconds while being transmitted from device to C3N on the Internet). So, for the users bladehedge and kingwasp, only 20 out of 6084 messages took more than 20 seconds to be available to Gendarmerie officers.

129. This analysis further confirms and fully supports clear statements by Dutch, French, JIT and Europol police officer at the press conference held in the Hague on 2 July 2020 on the conclusion of Operation Emma and Operation Lemont (the Dutch name for the joint operation) [13]. Eurojust stated that the "joint investigation made it possible to intercept, share and analyse millions of messages", as mentioned in §4 above.

130. The Eurojust statement added that the French team put a "technical device in place to go beyond the encryption technique and have access to the users' correspondence ... a large dedicated team at Europol investigated in real time millions of messages and data that it received from the JIT partners". This description is also completely fully consistent with my analysis of the operations and effects of the "device" (implant or infection).

131. The Gendarmerie taskforce was stated by Eurojust to have been "monitoring the communications of thousands of criminals" Eurojust also stated that the

---

13 https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves- through-organised-crime-groups-across-europe

Netherlands JIT team had "followed the communications of thousands of criminals day and night since the operation began to unravel and act on the intercepted data stream." This statement is also shown to be accurate by the evidence here.

132. Jannine van den Berg, Chief Constable of the Netherlands Central Police Unit is reported as saying "It was as though we were sitting at the table where the criminals were chatting among themselves, really. What makes this investigation unique is that at a large scale we managed to read all of these criminal messages live."[14] This is not overstatement, on the basis of the detailed timing analysis above.

133. My assessment of each of these statements is that they are correct, based on the detailed and extensive forensic study of data collection and exfiltration from EncroChat devices reported here. I found no evidence of any type that could or does support Mr Horne's belief and Ms Sweeting's confirmatory report, as expressed in February 2020, that "messages are collected when they have been stored on the EncroChat devices" during the Live phase of the operation. From measuring the speed at which information was sent, it appears that the Eurojust description of the live interception of messages was being carried out in real time.

How EncroChat secure message interception worked

134. In customary academic and commercial descriptions of cryptography and secret messages, it is usual to depict A as a user wishing to send a secret message to another user, B, such that no party except B can read and understand A's message. EncroChat was designed and sold to provide this service. Historical evidence shows that their security approach was successful, from the point of view of the EncroChat user group, until the start

[14] https://www.nytimes.com/2020/07/02/world/europe/encrypted-network-arrests-europe.html

of the infection operation managed by the French and Dutch law enforcement Joint Investigation Team (JIT).

135. In standard cryptography diagrams, "Alice" is the "A" party and "Bob" the "B" party to a secret communication. NCA technical officer Luke Shrimpton also uses this convention in the diagram in his witness statement of 2 October 2020 (page 4). The communications paths are also described in the same terms by the French JIT team leader, Jérémy Decou.[15]

136. Mr Shrimpton's diagram is broadly correct. It includes minor errors. The lower left hand box of the diagram refers to Alice's phone and an "Unencrypted message" when it should refer to Bob's phone and a "Decrypted message". It is also not correct that original unencrypted messages - called "plaintext" – and/or decrypted messages are stored unencrypted in the storage database inside the EncroChat phones.

137. I have not been provided with evidence as to how EncroChat's message server programs worked in relaying messages between users. I am not aware of any information of this type being available. The "Message Queue" function on the server Mr Shrimpton describes and illustrates in his diagram therefore appears speculative. I nevertheless agree that it is a reasonable and probable inference. In any case, within such a queue and within the EncroChat message system generally, all messages remained encrypted and unintelligible. This is an inescapable consequence of the use by EncroChat "end-to-end encryption", as described by M. Decou.[16]

138. It follows, as Mr Shrimpton also states, that any attempt to understand EncroChat messages by breaking in on lawful authority to the server in Roubaix would be bound to fail. Lawful Interception[17] of the messages being transmitted though OVH would also be found to fail, if tried, as the

---

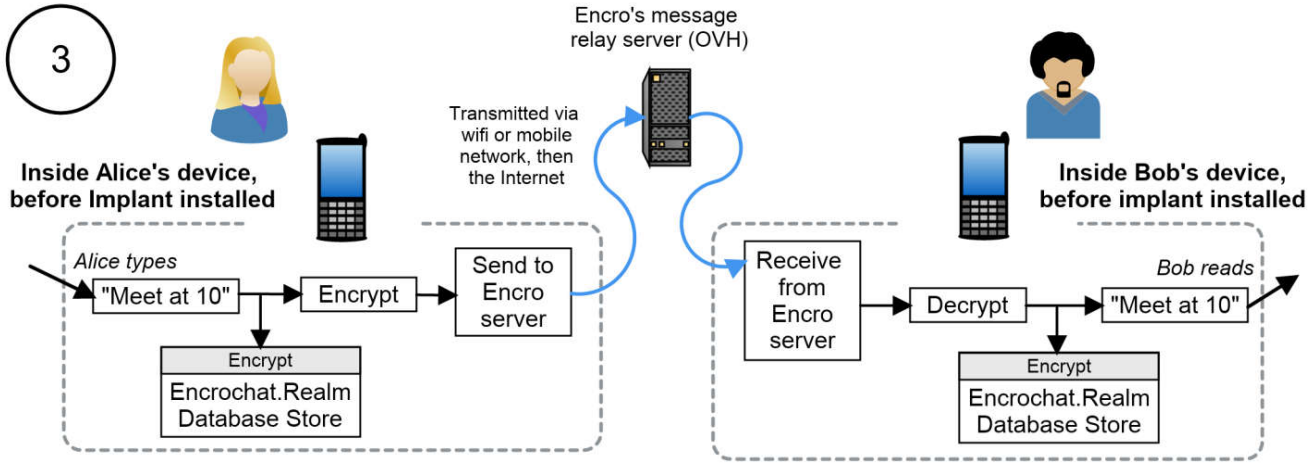
15 Responses to EIO questions, 5 September 2020

16 Page 1638

17 "Lawful Interception" is standard term of art in telecommunications engineering, not a legal definition.

cryptosystem (code) was not breakable by any known method. Evidence from the Gendarmerie suggests that both approaches were indeed tried, and failed, even when supplemented by potent lawful authorities to covertly copy content, data and programs directly from EncroChat's servers at OVH.

139. In Figure 3 below, Alice transmits a message to Bob, before interference.



140. The communications path from Alice to Bob begins when human agency and actions are transformed to electrical signals within computing machinery. At Alice's end, the path starts when her fingers touch a key, creating an electrical signal representing the key. The signals are then digitised, and so become represented by electrical states composed of binary digits or "bits", which are either 1 or 0. The data signal created by taps from Alice's fingers is then transmitted though inside a short term "working memory" or "buffer" inside the phone. As she types more letters they become a message in that location.

141. When Alice types Enter, the EncroChat program interprets this as a "send" instruction. Still being transmitted inside Alice's phone, the encrypted message passes to the onboard radio transmission system. Her message also includes address identification information for Bob, used only inside the EncroChat network. The address format used appears to be either an email style format, such as alice@encrochat.com, or the longer identity ID key for each user known to and used by EncroChat.

142. The EncroChat server then sends Alice's message to Bob, via the Internet and Bob's radio connection. If Bob's phone appears not to be connected to the Internet when Alice's message arrives, Bob's message is held, encrypted, on the message server, until Bob's phone reconnects and asks for his waiting messages.

143. All modern digital communications systems, including data sent using the Internet Protocol, relay data in very many stages, using physical distances or steps which can be miniscule or immense in length. Each step takes a discrete period of time to moved data from one point to another. Inside a microprocessor, the time intervals may be nanoseconds (one thousand millionths of a second) and the distances involved much less one centimetre. If identical digital signal then travel internationally or intercontinentally (at, or close to, the speed of light), distances may be in thousands of kilometres, and the time period in transmission one or a few seconds. The physical and technical processes are identical, despite the difference in scale.

144. The data storage area or database inside an EncroChat phone is called Realm. The Realm storage file, called Encrochat.realm is encrypted. It uses a different and distinct encryption process and keys to the encryption on the message transmission path. Mr Shrimpton is aware of this. He deals with the problem in the Venetic Data Processing Suite which he developed and exhibits [18]. This includes special processes and programs to decrypt Realm files so as to access stored data. Realm storage is not part of the transmission process. It is an additional and separate function. The duration of message storage can be altered by an EncroChat user. A copy Alice's message is sent on a different path to the Realm file. It is encrypted and stored there.

145. On the signal (transmission) path, the message is encrypted using the Signal Protocol, before being sent through her phone's built-in radio transmitter. The

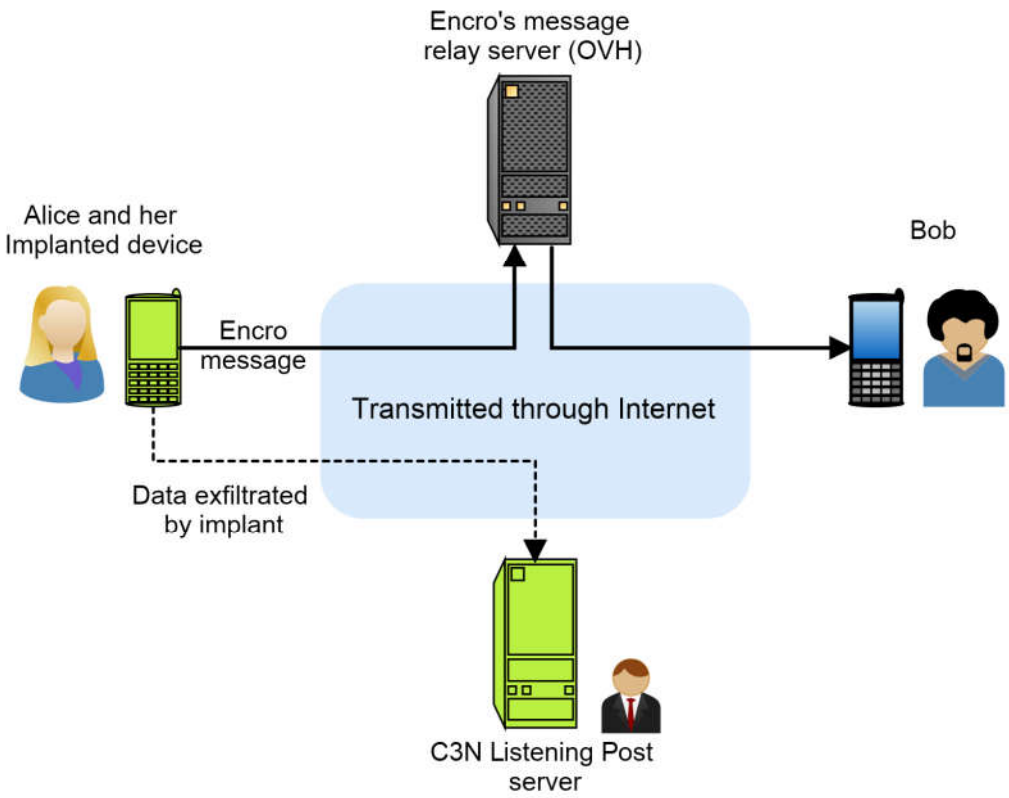
[18] LS/01/17/08/2020

radio connection can be made either to a serving mobile phone network cell or "mast", or a nearby WiFi access point. The transmission path then continues over the Internet and via the EncroChat message server provided by OVH.

The effect of EncroChat equipment interference

146. Figure 4 below illustrates the situation effect after equipment interference. The C3N app has infected Alice's phone in this example. It has created a hidden path, also on the Internet to send data to C3N. Alice is not warned that copies of her messages are being sent to C3N in real time, as she sends them. Other data is also sent regularly.

4



147. As before Alice's connection to the Internet could be cellular radio (to a mobile telephone network) or use local WiFi. It does not matter which. The radio connection takes Alice's message into the Internet. Its Internet destination is the EncroChat message server, located at the OVH Data Centre, Roubaix. Having passed through the encryption module inside Alice's phone, her

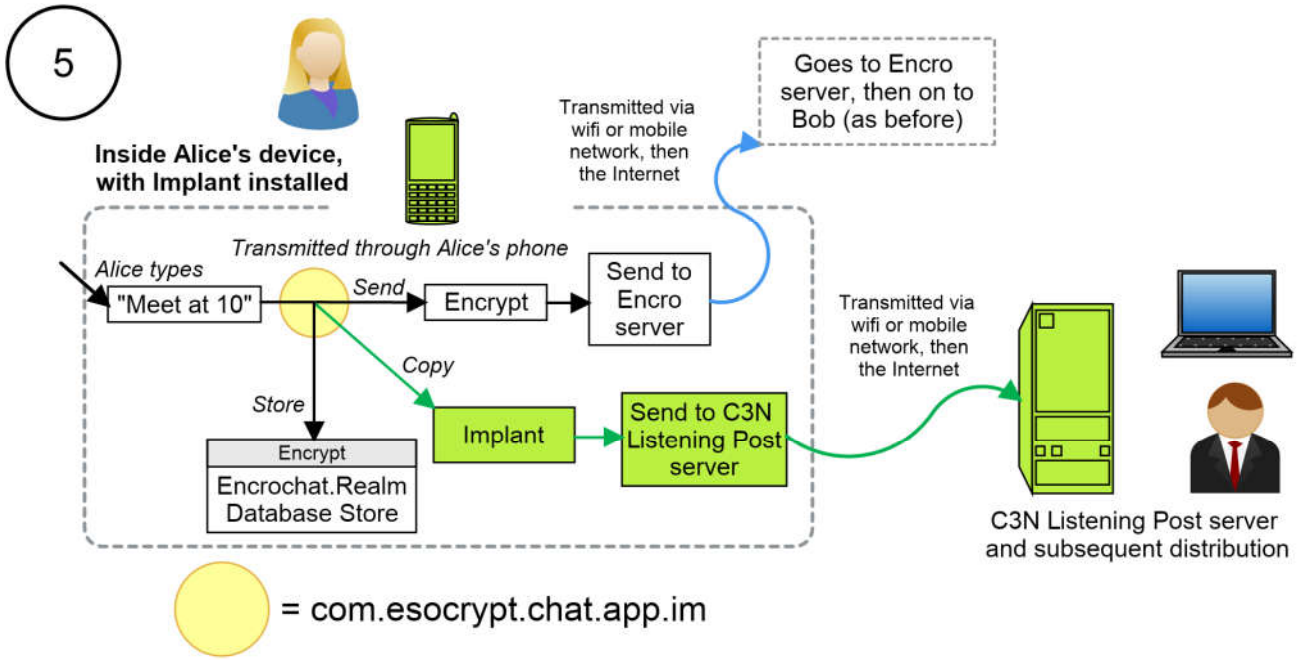
message is unintelligible and unreadable to anyone attempting to copy and then read it, including as it passes through EncroChat's chat or message server. When the separate copy of Alice's message passes to the Realm store inside her phone, it is locked by being encrypted

148. In EncroChat phones, the name of the chat application is com.esocrypt.chat.app.im. "Esocrypt" was the original name used by the company developing and selling EncroChat from 2013 onward. "IM" presumably refers to the app being an "instant message" system. The chat app is shown in Figures 5 and 6 as a yellow circle. Equipment interference and the effects of equipment interference both happen within the yellow circle.

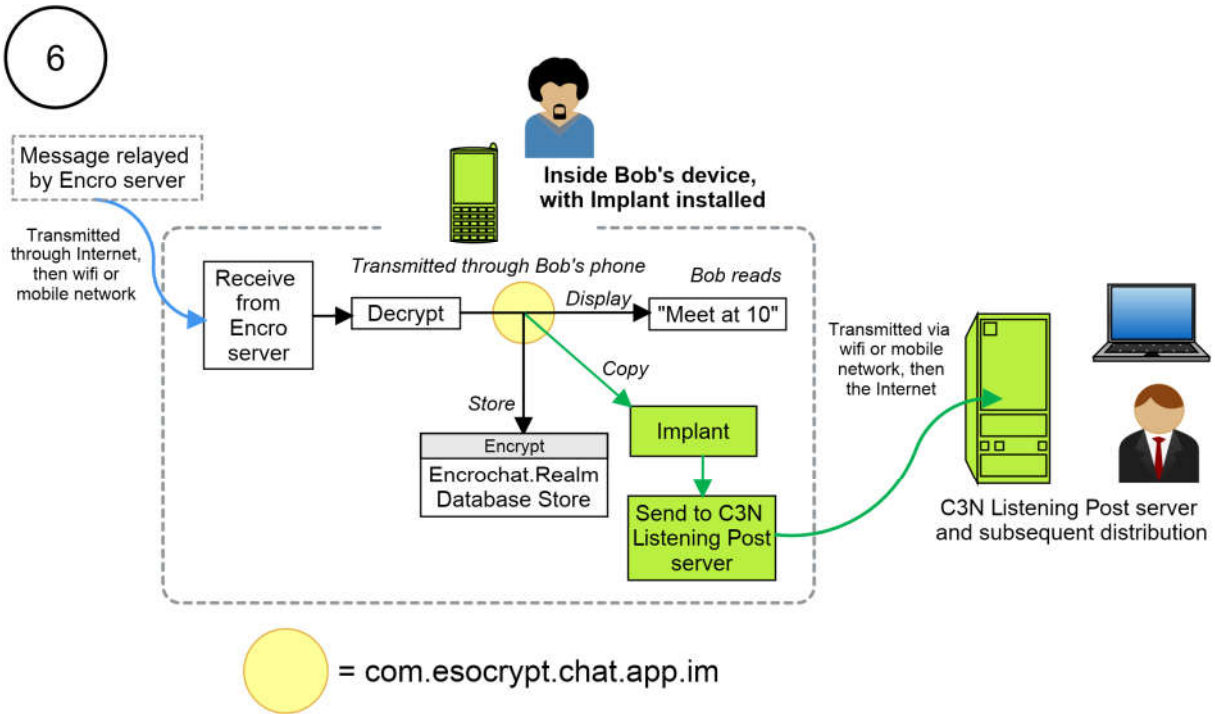
149. Figure 5 overleaf shows in detail the stages inside Alice's phone, after interference. When Alice presses "Send" on her infected phone, her message is transmitted as before to the encryption module within the EncroChat application on the phone. A copy is made to the Realm, encrypted, as before infection. As the direct result of the interference, an additional copy of Alice's message is sent to the C3N implant (from inside the yellow circle, the chat app). For security purposes, the C3N implant would be expected to encrypt the copy of the message, using another encryption system.

150. C3N's copy of Alice's message is then also transmitted though the onboard radio transmission system, and the Internet, to C3N's server. The effect of the equipment interference is that Alice's message, and the intercepted copy of her message are both transmitted over the Internet simultaneously or nearly simultaneously, to Bob and to the interception server.

[This area has intentionally been left blank]



151. If Bob's EncroChat phone has also successfully been infected, then another copy of Alice's message will be captured after it has been recieved and decrypted. Inside Bob's phone, as in the previous example, the message passes from the receiver part of the phone to the EncroChat decryption module com.esocrypt.chat.app.im, again shown within the yellow circle. The process is illustrated in Figure 6, below.



152. Normally, before infection, the decrypted message would be transmitted to the Encrochat.realm data store, and shown to Bob on his screen, on demand. After interference in the Stage 2 Live phase, his copy of the message from Alice is taken from the com.esocrypt.chat.app.im (EncroChat mesage app).

153. Mr Shrimpton states (page 3) "EncroChat encrypt their messages with the Signal Protocol. This is a commonly used encryption protocol that is freely available. I am unaware of any capability to decrypt messages encrypted using the Signal protocol." I accept these statements. I am also unaware of any capability to decrypt messages encrypted using the Signal Protocol.

154. The Signal Protocol has been developed and in use since 2013.[19] It is intrinsic to the widely used Signal[20] secure messaging application. Since 2017, the Signal Protocol has also been used by WhatsApp, an application owned by FaceBook, and which has over two billion users globally. The Signal Protocol has been built in different versions to operate in different types of computers, devices and operating systems. The computer code and programs designed to run the Signal Protocol version for Android type phones, including EncroChat phones, is available at and can be downloaded from Github,[21] an international software development repository owned by the US Microsoft Corporation.

155. I downloaded and examined the Signal Protocol source code to examine how messages are transmitted through a phone using the Signal protocol, from the moment of being typed by the user to the moment of passing from the phone in the form of a radio signal. The code is written in a general purpose programming language called Java.

156. On examining the Realm data storage areas within the EncroChat app, I located data object classes called SignalIdentity, SignalPreKeyRecord, SignalConfiguration and SignalSession. Features such as SignalPreKey are distinct

19 https://en.wikipedia.org/wiki/Signal_Protocol

20 https://signal.org

21 https://github.com/signalapp/libsignal-protocol-java

parts of the Sesame[22] encryption system used in the Signal Protocol. They enable a so-called "double-ratchet" key system, which provides for exceptionally strong cryptographic features called "perfect forward secrecy" and "perfect backward secrecy". Compared, for example, to well known wartime codebreaking achievements – where finding the code to one enemy message allowed codebreakers immediately to open or decode other messages - the Signal Protocol does not permit this. It currently appears impregnable when attacked directly.

157. Provided EncroChat engineered its network and device software to use the Signal Protocol correctly, only Bob would ever be able to read any message addressed to him. EncroChat staff could not read or understand Alice's encrypted message as it was transmitted though their message relay server, even if the message had to be held temporarily while Bob's phone was turned off or not connected. Other users of EncroChat could not read or understand the message.

158. By arranging to intercept messages being transmitted while inside Alice's phone, the "rogue app" developed by the French C3N agency was able fully to defeat this strong encryption. That is because it could copy live messages without needing to know the secret key used to decode it on Bob's phone.

159. Although the processes described above appear remote, complex and mysterious, they can easily be comprehended if tangible technologies are considered instead. In 1920, if Alice wanted to send a message to Bob, she would go to a Post Office and hand the postmaster her message to be sent by telegram. The postmaster would type her message on a form, simultaneously creating a carbon copy for the record. He puts the carbon copy in the Post Office safe (supplied by Realm Ltd) and locks the safe shut. Britain's GPO (General Post Office) has created a world-beating and uncrackable code

---

22 https://signal.org/docs/specifications/sesame/

system to protect telegrams going through its telegraph service. The postmaster then sends the message to the Post Office telegraphist to send. Alice's message is completely secure, for these reasons.

160. The postmaster is then induced by Charlie, a rogue, to cause an additional carbon copy of Alice's message to be created, by adding an extra layer of carbon paper to the telegram form. When the postmaster types Alice's message, an extra copy is created. He sends the second copy to Charlie. Charlie is thus able to intercept Alice's secret message, before coding, even if the British Post Office had then been deploying a world-beating encryption system to protect telegrams from snoopers.

Equipment interference technical processes

161. The equipment interference operation C3N launched in April 2020 is known in academic, security and cryptographic literature as a "Man in the Middle" (MITM) attack. With the reported co-operation and assistance of OVH engineering staff, the fake C3N EncroChat run server appears to have been electronically inserted into Internet communications paths between users and EncroChat's update server. A judicial order required OVH to divert incoming traffic to and the C3N server on police command.

162. The use of MITM as an attack method placed C3N in the most powerful position possible with respect to each phone, provided that they fully understood EncroChat's systems and operations. C3N anticipated, correctly, that after cutover at OVH, when devices asked for or were sent updates, the update sent would be the rogue app, which would then be installed.

163. Because, according to evidence, the fake update server was constructed essentially by copying the original, and for other reasons, the software on the devices and fake server might be expected allow the rogue app to be seen as a "superuser" and to have "root privileges". This would gave it unrestricted

access to read and copy all data anywhere inside the device, whether in storage or in operating memory, including passwords, codes and computer keys. In computer operating systems, a superuser has no restrictions and every privilege. In the everyday argot of the Internet, once the rogue implant reached each EncroChat device, it was "owned" by C3N. Covert information gathering systems like the C3N rogue application normally include extensive facilities for modifying and instructing the operations both of the telephone and of the application itself.

164. For this purpose, remote law enforcement or intelligence agency operators connect covertly to the device, over the Internet. They can then issue enquiries or give instructions. For example, they may set how often a cell location report is sent, or install additional software to carry out other functions. As they have acquired full control of, and "own" or "pwn"[23] the phone, the remote operators are able to cause messages and images to be transmitted, and/or to edit or delete or insert stored messages to the Realm file. They would also have the technical ability to control and use the camera and microphone (if working) to listen to local sounds or take images. NCA staff were advised before the start of the operation that C3N did not propose to use this exploitation technique.

165. The means of infecting each the phone was to cause the C3N "rogue app" to be sent as a data package from the fake EncroChat server at OVH's Roubaix data centre, operated and controlled by C3N. I infer that as part of previous authorised lawful intelligence operations, C3N had copied or intercepted all necessary cryptographic certificates and programs used by EncroChat to certify to their clients' phones that new data packages coming from the update server were authentic and should be installed. Further, since messages to and from the EncroChat update server were being covertly diverted and rerouted

---

[23] "Pwn" had the original meaning in computer games that a player had been owned, if they became dominated or controlled by another. In the modern cybersecurity context, to "pwn" is to remotely take full control of a target by means of cyberattack.

to C3N's fake update server, physically close by, the phones would have no means of detecting that they were being sent instructions by an impostor.

166. When the full update data package had been downloaded, it would be installed automatically. M. Decou described the infection as an "app" (i.e. application program). It is possible that he is also using this term to include additional interference with the operating system used by EncroChat. It is therefore a possibility that the C3N infection made changes to the phones' modified Android operating system, so as to assist intended activities. Decou states that disclosure of any information about this would be an offence under French defence national security law.

167. The installation and possible related "relevant events", and any subsequent installations, any further interference or remote command execution, including the act or conduct of creating an interception system took place on the territory and in the jurisdiction of the location of the device at the time of installation, notwithstanding that the infection data package was sent from Roubaix, in northern France.

168. After download and then installation of the infection, according to my analysis of exfiltrated data sent from newly infected phones, the Historic Data Collection phase began. The application normally first swept up the phone's encrypted Realm data file, the encrypted "EncroNotes" notepad file, the Android contacts file, the Android calendar file, standard SIM and telephone information (including IMSI and IMEI numbers unique to the phone and its SIM), stored images and media files (which were also encrypted), and other update files. It also located and sent back any keys it found for decrypting the Realm file, the EncroNotes file and the media files. EncroChat's storage encryption systems, used the "AES" (Advanced Encryption Standard) cryptographic algorithm, in contrast to its use of the Signal Protocol to send encrypted messages. Each standard sweep-up collected 15 different items of

data, as shown in the table of exfil functions (Exhibit DC/4, attached) under the heading "sweep-up".

169. The "cellLocation" and "cellinfo" data would show where the phone was located. The information included fields called MCC (Mobile Country Code), MNC (Mobile Network Code), LAC (Location Area Code) and CID (Cell Identity).

170. The Mobile Country Code, a three digit number, shows the country in which the phone is then located. The MCC for the UK is 234. The Mobile Network Code shows which network operator in that country was providing communications services to the phone. For example, the MNC for the Vodafone network in the UK is 15, EE is 18 and O2 is 20.

171. The Location Area Code identifies a broad service area for the given network in the country identified, within which a collection of cells provide radio service to mobile customers. By using information supplied by communications service providers such as Vodafone, or measured in the field, knowledge of the Cell Identity (CID) and LAC will indicate the approximate current location of the phone. Typically, in an urban area, this would be estimated to an accuracy of approximately half a mile; in country areas the accuracy could be less, up to several miles

172. M. Decou's response to the Crown Prosecution Service's EIO of 11 September 2020 states that messages are captured when "(IV) The message is transmitted (in an encrypted format) from telephone A to the server;" and/or "(VIII) The message arrives on telephone B where it is decrypted."[24]

173. I agree with these answers provided by M. Decou. The meaning and consequence of his description is easily deducible, clear, and is not in my understanding capable of being ambiguous. M. Decou and I agree that in the

[24] Page 1688.

technical processes, messages are not captured after encryption inside Alice's phone, or before decryption inside Bob's, because decryption of the ciphertext at these stages is not possible and has not been achieved. Therefore, M. Decou is saying (as I am) that the capture of the message from A (Alice) is when it is being transmitted inside her telephone, before being encrypted. He is also saying (as I am) that the capture from B (Bob) is while her message is being transmitted inside his telephone, after decryption. He makes no mention of "storage" playing any role. I confirmed this by research. His answers further refute the hypothetical belief espoused by Mr Horne.

Analysis of NCA Operation Venetic Data Processing

174. I have examined a set of 17 Python scripts (computer programs) prepared by Mr Shrimpton and colleagues as the Operation Venetic Data Processing Suite.[25] These are written in the Python high level general purpose computer language. These programs show that the NCA processed Live intercepted data entirely separately from the stored Realm data, using different programs and processes. This was necessary because the data structures, locations, format and content are different between Live material and Realm material. In particular, the Realm data was supplied as a single encrypted file [26] of stored messages, whereas the Live data arrived unencrypted and was processed as a stream of many thousands of individual messages. There is no grey area of ambiguity or uncertainty as to the distinction between the two types of data or how they were handled.

175. I requested copies of the computer programs created by Mr Shrimpton at the start of my investigation. I was provided with copies on 20 October 2020. I was sent three versions, held in files labelled v1.zip, v2.zip and v3.zip. I unzipped (decompressed) these to subfolders for examination.

---

25 Version 1, 5 July 2020.

26 Shrimpton, Operation Venetic Data Processing Suite, page 1638

176. Inside v1.zip, I found scripts (programs) written in the Python general purpose computer language. One group of scripts was constructed to handle live intercepted messages sent in the form of JSON data objects. These were GetLiveMessages.py, ProcessLiveMessage.py and ProcessLiveFile.py. Each script appeared written to perform the functions implied by their names.

177. A second and distinct group of Python scripts were constructed to collect and process stored messages and data received by C3N in the form of Android Realm databases. These included "ProcessRealmFile.py", "GetDBMessages.py" and "ProcessDBMessage.py". Other scripts were designed to decrypt and process images and other files, including EncroNotes files.

178. Inside v3.zip, I found a TAR type archive file caller DockerImagev3.tar. Docker images are a form of virtual computer. Technically, they are called "containers". The use of a container or a virtual computer means that all users can have the same experience and work in the same way, while using multiple types of computer. The user also does not have to set up special programs, such as a program to run instructions written in Python. My understanding is that Mr Shrimpton prepared Docker containers for circulation in order to simplify the steps recipient law enforcement agencies would have to take to run his Venetic Data Processing Suite.

179. Docker containers comprise multiple folders, which include "layers" to be assembled to run the intended virtual computer. I did not attempt to run the Docker software as such. I looked for the location where the new version of Mr Shrimpton's Python scripts was stored. I found the Python scripts in folder 329f1d0f8624640fc204f9aeb4bfec1d203544a1cf32dd38a6b34daebf6043a7. Within that sub-folder I found another TAR type archive file caller layer.tar. The file layer.tar contained a folder called "Code". I found and examined the third version (v3) of Mr Shrimpton's Python scripts from there. I found that the v3 scripts were substantially the same as v1. Specifically, Version 3 contained the same three Live scripts and three Realm (or DB) scripts as in v1.

180. Although the complex processes I describe above sound akin to opening a Russian doll, and could appear obscure or obstructive, they are not and that is not the issue. They script names and functions show that Mr Shrimpton was always at all times of the fundamental and meaningful difference between the two types of message evidence, Live and Realm.

181. Part of the Venetic Data Processing Suite is a Python program called ParseMessages.py. This program brings together message information taken from the Realm storage files and, separately, from Live messages, and then merges them to a single data table. Within a data table then produced inside the ParseMessage.py program, the source of every message is identified as coming either from "Realm" or "Live".

182. In his witness statement describing the material he caused to be produced for evidential use, Mr Shrimpton explains[27] that he first created files in a format called JSON, as "the result of the script [program] parsing the data in the Raw folders". JSON stands for JavaScript Object Notation. It is a means of characterizing and storing different sorts of data object within a single file format.

183. Mr Shrimpton then produced a folder of files called CSV. CSV stands for "Comma Separated Variable". It is a simple data file format in which items are grouped in columns and separated by lines, with each column entry having a single meaning. For example, a simple CSV file for a greengrocer's business could appear as

Fruit, amount, supplier, date
Oranges, 200, Sombrero, October
Apples, 140, Robinsons, September
Grapes, 350, Romanica, August

[27] Shrimpton, Operation Venetic Data Processing Suite, page 1638

184. Mr Shrimpton produced eight CSV files, including Messages.csv. He states that CSV files present data (in the style above) in a "simplified, human readable format. In order to achieve this format, some of the json data entries have not been included".

185. Mr Shrimpton has exhibited three numbered versions of the Venetic Data Processing Package and its components, with dates shown overleaf

Version	ParseMessages.py date	CSVOutput date
1	05 July 2020	05 July 2020
2	06 August 2020	24 August 2020
3	06 August 2020	03 September 2020

186. Mr. Shrimpton created Python scripts[28] including CSVOutput.py and ParseMessages.py. Within ParseMessages.py (Version 1, 5 July 2020) the instruction shown below tells the computer which specific data items about each message should be sent to the CSV output evidence file to be provided:

```
MakeCSV (WorkingDirectory, Messages ,"Messages", ["id", "dateCreated",
"dateRead", 'From', 'To', 'burn', 'body', 'IsMedia', 'MediaID']);
```

187. In this Python instruction, the list of types of data to disclose about the message content are shown between quotes, such as "dateCreated", 'body' or 'From'. The choice of which data types to include, and the order and style of presentation of each item in the CSV output is an explicit choice made by the programmer when coding. I presume but do not know that the programmer concerned would act on instructions and/or task specification set out in documents supplied by a line manager, team manager or similar senior.

[This area has intentionally been left blank]

[28] (In this context a "script" is a computer program written in the Python programming language.)

188. It would have been better, easier and quicker to have written this instruction in a straightforward fashion which did not suppress the 'source' or other fields, by writing instead the instruction:

```
MakeCSV(WorkingDirectory,Messages,"Messages");
```

189. This Python language instruction is basic, shorter, simpler and less likely to create errors. The instruction automatically follows principles of disclosure. It would create s full list of message data evidence, in the same way as was present in the machine readable JSON files created simultaneously. I have inspected the JSON files created. They include "live" and "realm" labels. The word in the JSON files are in human legible. I have read them.

190. It would be fair to say that some of the data items do not greatly add to understanding. For example, the entries found in the JSONs for "contactId" contain sequences such as "00c5e8c7-4fd6-49ee-94fc-77e2666a1c39", which is the "ContactId" for the user bladehedge.

191. Mr Shrimpton's statements do not explain or mention the exceptions he wrote into his script for creating the CSV output files. He does not explain why the type distinction between "live" messages and "realm" (stored) messages was suppressed from view in the CSV files. If the purpose of his omitting data from was a *bona fide* attempt to make the products more manageable for a Court and jury, this could have easily been done by changing a single word of his first script, as shown below:

```
MakeCSV(WorkingDirectory,Messages,"Messages", ["id", 'source' "dateCreated",
"dateRead", 'From', 'To', 'burn', 'body', 'IsMedia', 'MediaID']);
```

192. The variation is the addition of the word 'source', such that in the CSV files, the source of the message, be it stored data or live intercept, would appear in a new column to the left of the "dateCreated" entry. In the interests of transparency in disclosure, it would also have been possible to provide both a full output table and a "simplified" table omitting items such as "ContactId"

which do not have a clear meaning unless a directory of ContactIds and names is available.

193. For the above reasons, I am unable to comprehend Mr Shrimpton's explanation that he edited the CSV records to remove the source identification in order to make the resulting tables "human readable". I also cannot understand how removing the crucial distinction for the Court of knowing whether a message was from storage or was live can accurately be described as "simplification".

194. In his statement of 17 August 2020, Mr Shrimpton says that he had later been instructed to make changes to his scripts including to cause "CSV spreadsheets to include all json data". I therefore then examined the revised version of the ParseMessages.py script, dated 6 August 2020. It contained the correct Python instruction for full disclosure of all data explained above, specifically:

```
MakeCSV(WorkingDirectory,Messages,"Messages");
```

195. I then rechecked all disclosed output data available to me or those instructing me at the time of preparing this report, including CSV files, Excel tables, PDF documents produced from Excel tables, or other written documents or statements, to determine when and if Mr Shrimpton's revised script of 6 August 2020 had been used. None of the documents I examined contained references to live and realm (or "db") entries, which would have occurred if the revised script had been used.

196. Mr Shrimpton's programs created a folder of JSON files at the same time as creating CSV files. Source identification information was included in the matching JSON files. JSON files are, as he suggests, hard to analyse and understand manually, even with the use of a specialist viewing program.

197. Mr Shrimpton's also says that in August, he had to amend his program because of a systematic error in incoming information from Europol. He then made changes including causing "CSV spreadsheets to include all json data."

198. Despite this claim, source information identifying Live copies of messages in CSV files is absent from all evidential products I examined. These including in particular the large and compendious 1,477 page Operation Subzero Exhibit 75 Spreadsheet.

199. If time and circumstances permit between the date of service of this report and the date of hearing, or after the date of hearing, I can if asked by the Court or by those who instruct me extend the reach and thereby the strength of the conclusions in this section by including and analysing evidence from one or more or many additional Operation Venetic Data Packages.

NCA experience of Equipment Interference

200. In his statement of 8 October 2020, NCA Deputy Director of Investigations Matthew Horne states that he is not a technical expert on interception or equipment interference. He offers "context" based on personal experience. He describes having held "operational roles" in investigations of the criminal use of secure communications (CDSC), or in operations in which Targeted Equipment Interference (TEI) methods were employed. On this basis Mr Horne asserts that "in my judgment" the systems used in the Live phase of Operation Emma data collection were Equipment Interference ("TEI") and not Interception ("TI").

201. At §17 above, Mr Horne founds belief and offers "judgment" because he knows from personal experience (i) that it is technically impossible to obtain human readable unencrypted communication content data (called "plaintext" by cryptographers) and (2) that no technology exits to do so if "end to end" encryption is in use.

202. Both statements are wrong. The distinction between plaintext and ciphertext is elementary and fundamental to cryptography and cryptanalysis. By necessity, encrypted communications always also pass through plaintext links and stages. The methods Mr Horne says he is unaware of have been generally known for more than 50 years. "Equipment interference" was not invented in 2016. Unlawful equipment interference - commonly called "hacking" – goes back to the 1960s for computers and IT systems, and earlier for electronic communications.

203. During the 1950s, Soviet Intelligence Services developed techniques for intercepting plaintext electronic signals leaking from communications equipment, and/or causing such signals to be sent by using powerful radio illumination beams. To defeat these forms of interception, NATO allies developed a standard set of defensive methods known as TEMPEST.

204. It then became mandatory for government, military, police and intelligence organisations in the west to use "TEMPEST shielded" equipment when needed to prevent interception of sensitive secret information during the plaintext stages of a communications. Guidance and standards for equipment requiring TEMPEST shielding is provided to HMG customers including police services by the National Cyber Security Centre (NCSC), a division of the intelligence agency GCHQ.

205. One of the longest established, simplest and best known methods of equipment interference so as to obtain plaintext before it is encrypted is the installation of a "keylogger". A keylogger can be a computer software program or a hardware device, mechanically fitted to a computer or device. Keyloggers are a standard part of the equipment interference repertoire available to agencies in the UK. Keyloggers automatically capture every message sent from a device while the message is typed in the course of transmission. It is very widely known that keyloggers have particular value to attackers when used to copy passwords for accessing services such as

online bank accounts. Keyloggers have also been used for at least 50 years by adversary intelligence agencies. They are used by serious and organised crime groups for cyberattacks.

206. Warnings that the UK faces repeated cyberattacks using keyloggers are routinely published by NCSC , for example:

https://www.ncsc.gov.uk/report/weekly-threat-report-13th-january-2017, reporting the "EyePyramid" attack method.

https://www.ncsc.gov.uk/report/weekly-threat-report-16th-march-2018, reporting the "Shadowpad" attack method.

https://www.ncsc.gov.uk/report/weekly-threat-report-29th-june-2018, reporting the Mylobot and "fake Fortnite" attack methods.

207. On 20 March 2020, NSCS jointly with the US Homeland Security Cyber-Infrastructure Agency issued a warning that "an increasing number of ... cyber criminals are exploiting the Covid-19 pandemic as part of their cyber operations". NCSC warned that they had detected many scams relating to Covid-19 include fake e-mail messages appearing to be sent from the World Health Organisation and deploying "Agent Tesla" keylogger malware.[29]

Reliability of computer-based electronic evidence

208. The manner of producing the EncroChat evidence violates all the long established and internationally recognised UK Principles of Computer Based Electronic Evidence prepared under the auspices of ACPO (now NPCC). [30] The "Good Practice Guides for Digital Evidence and their four governing

---

29 https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

30 https://athenaforensics.co.uk/wp-content/uploads/2019/01/National-Police-Chiefs-Council-ACPO-Good-Practice-Guide-for-Digital-Evidence-March-2012.pdf

principles for evidence handling are amongst some of the most cited pieces of digital forensic best practice advice."[31] The four principles are listed below.

(a) **NPCC Principle 1:** That no action take is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

(b) **NPCC Principle 2:** Where a person finds it necessary to access original data held on a digital device that the person must be competent to do so and able to explain their actions and the implications of those actions on the digital evidence to a Court.

(c) **NPCC Principle 3:** That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third party forensic expert should be able to examine those processes and reach the same conclusion.

(d) **NPCC Principle 4:** That the individual in charge of the investigation has overall responsibility to ensure that these principles are followed.

209. Further (§2.2.7) "It is essential to display objectivity in a court of law, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court."

210. None of these essential and necessary checks appear to be possible in these cases. Concerning NPCC Principle 1, the process of creating and installing an implant gives the implant designers, installers and operators *carte blanche* to operate any enabled physical or computational process possible on the Android device, including but not limited to recording speech from the microphone or images from the camera, generating and/or sending messages,

[31] https://www.sciencedirect.com/science/article/pii/S2665910720300220

changing the contents of data stores, as well as the acknowledged and documentable activities seen in the Raw folders for each device.

211. "Changing data", proscribed by the First Principle, can and does mean altering or adding to or operating programs as well as altering, adding to or removing content. "Changing data" is fundamental to and the basis of equipment interference, even when and if change is effected purely by means of physical hardware interference.

212. Because of robust French legal requirements, there is no evidence available nor, *prima facie*, the possibility of evidence being available to the Court concerning customary issues of provenance, authenticity, reliability, completeness and integrity. There are no witnesses identified to the Court who can describe the technical means, and be cross-examined as to flaws or inadequacies at the start of the chain of evidence. As far as I am currently aware, these issues are unprecedented in nature as well as in scope and significance.

213. There is also no official evidence available, other than in the vaguest outline, as to what the technical processes involved in the French and Dutch joint operation were. French witnesses say that they must refuse by law to identify the agency and/or persons undertaking this work. The involvement of unknown and unidentified third parties, or even further and undisclosed third party activities within the implant design or operational activity cannot be excluded.

214. My further concerns about this evidence are:

(a) There is no information about any disruptive (disruption enabling data changing) capabilities which could be part of the implant, or its use;

(b) The range of commands an operator could send to the implant and their capabilities have not been disclosed.

(c) Exfil from the implant may have been filtered or changed at multiple stages before being transferred to Europol, including by unknown and unknowable parties, with no risk of detection.

215. These violations of the NPCC Code all appear egregious in that there is, for the reasons set out in statements by Jérémy Decou of C3N, no reliable available technical possibilities for "workarounds" which could even partially test, validate and/or authenticate this evidence. This is also novel and unprecedented in my experience.

216. In relation to the second to fourth NPCC Principles of Computer Based Electronic Evidence, there is no witness available to the Court who is competent to explain actions of interference that were undertaken, or their effects.

217. If wholly undocumented equipment interference actions, such as the C3N "rogue app" are permitted, inevitable effect is to destroy entirely the reliability of digital evidence produced to a tribunal. That is because there is no audit trail or records of providing the normal and mandatory chain of evidence. No person has been nor can be identified who will be willing to testify that they are responsible for and in charge of rogue app activity and management, and answer questions.

218. Excel based exhibits derived from NCA Operation Venetic data packages, prepared by NWROCU for this case appear to have been incompetently prepared and are in my view unreliable, for multiple reasons. In particular the origins and provenance of the Operation Subzero Conspiracy to Murder SOE V2, produced by intelligence analyst Emma Southall on 14 October 2020 are indeterminate. Her witness statement gives no details of the processes followed or tools used. The source evidence is not available. Documents were served in a form in which they could not be analysed electronically.

219. To identify the actual sources of information for Ms Southall's exhibit, we used an Optical Character Recognition (OCR) program to recognise and recover text information from this very large exhibit. At my request, Mr Fowler used a bespoke "scraper" program to extract sources of evidence by scanning and analysing the face of the document to pick out source information. This search generated the list of files in Table 3 below

Table 3 Irregular CSV files in Schedule of Events

Name of CSV file	No of entries
354362110006943 Figzoo.csv	1782
358098090779879 Bladehedge 1.csv	17
358098090779879 Bladehedge Messages.csv	907
358098090781552 Bladehedge 1.csv	26
358098090781552 Bladehedge Messages.csv	1555
358098092001058 Kingwasp 1.csv	1
358098092001058 Kingwasp.csv	879
358098092202201 Scalpstaff 1.csv	2
358098092202201 Scalpstaff.csv	693
358098092255563 Northknee 1.csv	154
358098092255563 Northknee.csv	11737
358098092785213 Moonlitboat 1.csv	51
358098092785213 Moonlitboat.csv	2853
358098092940354 Olivescooter 1.csv	19
358098092940354 Olivescooter.csv	3609
358098092960899 Sappystag 1.csv	7
358098092960899 Sappystag.csv	1687
358098092962945 Bestgolfer.csv	25063
358098093190918 Softherb 1.csv	32
358098093190918 Softherb.csv	5437
358098093363556 Bladehedge 1.csv	3
358098093363556 Bladehedge.csv	886

[This area has intentionally been left blank]

220. The search showed that (a) none of the source files listed in Ms Southall's statement were listed in her exhibit; and (b) none of the source files in the exhibit were listed in her witness statement. The scan also showed that many of the sources of data used by Ms Southall could not have been original data supplied to NWROCU by the NCA. That is because they do not confirm to the normal name styles generated for Operation Venetic data packages.

221. Most of the source files found, shown in red overleaf, should not have been used. That is because these names have been suffixed by "1", meaning that they appear to be copies, not originals. The two "Bladehedge Messages" files cannot be original for the same reason. To be considered as trustworthy, any similar table should be rebuilt only from original, specified and exhibited NCA Operation Venetic Data Packages, for every user whose name appears. It should also include the evidence for both parties to any message exchange.

222. Many other difficulties and inconsistencies are apparent from the face of the SOE document. I discovered a probably answer for one of the significant discrepancies purely by accident as an unexpected byproduct of the work described above. That is the observation that when multiple entries appear for a single message in the SOE, the probable reason is that one entry is from Stage 2 Live intercept, and the others are copies from Stage 1 Realm files.

223. Problems of this type are common when large data sets are mixed and joined and then manipulated using the popular software program Excel. In this investigation, Excel has apparently been used to merge and display message logs brought together for different communicators who are alleged to be part of one or more linked groups. Images and other items are added by manual processes of "cut and paste", which are not logged, and are prone to human error. Many errors created are not then easily detected, if at all. The lack of quality in producing this exhibit makes further tests to find and remove errors an unproductive use of time; the work should be re-done, properly, first.

224. The information in this statement is true to the best of my knowledge and belief. I fully understand that it is my duty as an expert to help the Court on matters within my expertise, and that this duty overrides any other obligations including my duty to the person(s) from whom I have received instructions. In preparing this report, I have complied with that duty.

Signature:  **6 November 2020**

ANNEXE A

Relevant experience and forensic expert work

1. My work has included serious terrorism and fraud cases involving forensic analysis of large data sets, as well as cases of major drug trafficking and of exploitation of child abuse images.

2. I have researched and reported concerning communications interception for 45 years. While studying at master's level, I designed and built a novel communications probe, and a device for detecting analogue telephone line interception. As a consultant to the Technology Faculty of the Open University, I co-wrote a course book on "The British Telephone System". During the 1980s and 1990s, I physically carried out and/or advised on detection of covert communications systems. In one instance in 1988, I physically and analysed located two clandestine secure radio linked interception devices.[32] In 1998, I was appointed a consultant to the Scientific and Technological Options Assessment (STOA) office of the European Parliament and was contracted to prepare reports on communications security.

3. The European Parliament published my report, "Interception Capabilities 2000" in 1999. I provided further reports to the European Parliament concerning international communications surveillance for intelligence purposes. I regularly lecture to British and overseas audience; recently at Cambridge University, Edinburgh University and the University of Warwick, and the Royal Institute for International Affairs (Chatham House). I have presented on electronic intelligence and security matters to the Foreign Affairs Committee of the Bundestag (Germany), to Committees of the Diet (Japan), to the Swedish, Danish and Dutch parliaments; and to the intelligence supervisory committee of the Belgian government. I have lectured on training courses for international

[32] The target was an exiled leading member of the African National Conference (ANC) of South Africa, creating a presumption that the attacker was likely to the then South African intelligence services, BOSS. I gave one of the devices to Special Branch for further examination.

military and diplomatic staff conducted by the Geneva Centre for Security Policy, and for academics at the Ecole Nationale Superieure des Telecommunications, Paris.

4. In May 2015, I was invited to open the Ditchley Park International Conference on Intelligence, Security and Privacy jointly with the then Director of Government Communications Headquarters, Mr Robert Hannigan. I gave evidence to the Joint Parliamentary Committee on the Data Communications Data Bill in 2012 and to the Committee on the Investigatory Powers Bill in 2016. In November 2017, I was invited by the Investigatory Powers Commissioner Sir Adrian Fulford (Lord Justice Fulford) to participate in a training panel for the first Judicial Commissioner Induction Seminar.

5. I am a Fellow of the Royal Society of Arts (FRSA) and a former member of the Institute of Telecommunications Professionals (ITP). During 2019 and 2020, I was a member and then the deputy chair of Police Scotland's External Reference Group on Cyber Kiosks.

ANNEXE B

List of Judgments citing expert evidence

1. R v Sayers, Judgment of Mr Justice Brown, Leeds CC, 10 December 2001
2. R v Winters [2008] EWCA Crim 2953; [2008] WLR (D) 387
3. R v Breton [2008] EWCA Crim 2935
4. Clifford v Herts [2008] EWHC 2549
5. Liberty and others v United Kingdom no 58243/00.
6. Clifford v Herts [2008] EWHC 3154
7. R v Iqbal [2009] EWCA Crim 1627
8. R v Austin & ors, Supreme Court [2009] EWCA Crim 1527
9. Clifford v Herts [2009] EWCA Civ 397
10. Clifford v Herts [2009] EWCA Civ 1259

ANNEXE C

List of Cases Instructed

No	Matter	Year	Court	Charges
1	R v Bennett, Mills and others	1979	Central Criminal Court	Conspiracy to cause explosions
2	R v Johnstone	1980	Central Criminal Court	Hoax 999 call
3	R v Watts	1980	Central Criminal Court	Hoax 999 call
4	R v O'Brien	1981	Central Criminal Court	Armed robbery and murder
5	R v Ainger	1982	Central Criminal Court	Hoax 999 call
6	R v Sanchez & Ramirez	1983	Central Criminal Court	Espionage (S1 OSA 1911)
7	R v Middlemast	1984	Croydon Crown Court	Hoax 999 call
8	R v Bartholomew	1985	Southwark Crown Court	Hoax 999 call
9	R v Trump	1985	Central Criminal Court	Armed robberies
10	R v Williams	1986	Inner London Crown Court	Hoax 999 call
11	R v Raja	1989	Southwark Crown Court	Conspiracy to supply Class A drugs
12	R v Effik	1990	Middlesex Crown Court	Sale of drugs
13	R v John & ors	1996	Leeds Magistrates Court	Criminal damage
14	R v Lee & ors	1997	York Crown Court	Criminal damage
15	R v Hanratty & ors	1997	Central Criminal Court	Conspiracy to cause explosions (Provisional IRA)
16	R v Rogers and ors	1997	Portsmouth Crown Court	Conspiracy to cause criminal damage
17	R v Hart	1997	York Crown Court	Criminal damage
18	R v Kebilene & ors	1999	Central Criminal Court	Prevention of Terrorism Acts
19	Prentice & Prentice v McPhilemy & ors	2000	Federal District Court of Washington DC	Libel (allegation that plaintiffs were members of protestant terrorist murder conspiracy)
20	R v James & Wenham	2000	Liverpool Crown Court	Conspiracy to damage a Trident submarine
21	R v Wylde	2000	Central Criminal Court	Official Secrets Act (1989, s4)
22	R v Sayers & ors	2002	Leeds Crown Court	Conspiracy to murder
23	R v Knaggs & ors	2002	Sheffield Crown Court	Conspiracy to supply Class A drugs
24	R v Allsopp & others	2002	Newcastle Crown Court	Conspiracy to supply Class A drugs
25	Liberty v UK	2008	European Court of Human Rights	Breach of convention; re Interception of communications
26	R v Burns & others	2003	Leeds Crown Court	Conspiracy to murder
27	R v Kearney & ors	2003	High Court, Belfast	Conspiracy to cause explosions
28	R v Shepherd	2003	Newcastle Crown Court	Assisting an offender

29	R v Ali	2003	Newcastle Magistrates Court	Threatening phone calls
30	R v Straw	2003	Leeds Crown Court	Rape and kidnap
31	R v Kerry, Watkin, Rowland and others	2003	Maidstone Crown Court	Prevention of Corruption
32	R v Dixon & ors	2003	Newcastle Crown Court	Burglaries
33	R v Jackson	2003	Sheffield Crown Court	Conspiracy to supply Class A drugs
34	R v Nasar & Loxley	2003	Stafford Crown Court	Conspiracy to supply Class A drugs
35	R v SS	2003	Newcastle Crown Court	Making indecent images of children (Operation Ore)
36	R v Shazad	2003	Bradford Crown Court	Arson and murder
37	R v Nazir	2002	Luton Crown Court	Conspiracy to supply Class A drugs
38	R v Dunne & others	2003	Durham Crown Court	Conspiracy to murder
39	R v Wolf	2003	Newcastle Crown Court	Conspiracy to burgle
40	R v Ahmed	2003	Wolverhampton Crown Court	Murder
41	R v Al	2003	Newcastle Crown Court	Sex with a minor
42	R v Vispo	2003	Kingston Crown Court	Conspiracy to supply Class A drugs
43	R v Ramsey	2003	Central Criminal Court	Attempted murder
44	R v Crumbie	2003	Leeds Crown Court	Conspiracy to supply Class A drugs
45	R v Jenkins	2004	Cardiff Crown Court	Conspiracy to supply Class A drugs
46	R V GC	2004	Newcastle Crown Court	Making indecent images of children
47	R v NM	2004	Crawley Magistrates Court	Making indecent images of children
48	R v Gaulston & others	2004	Central Criminal Court	Arson and murder
49	R v Houssein	2004	Birmingham Crown Court	Conspiracy to supply Class A drugs
50	R v Livingstone	2003	Middlesborough Crown Court	Conspiracy to supply Class A drugs
51	R v Sikander & others	2003	Bradford Crown Court	Kidnap and assault
52	R v Crumbie	2003	Leeds Crown Court	Offence not advised
53	R v McKay	2003	Newcastle Crown Court	Murder
54	R v Hanvey	2003	Bedford Crown Court	Rape and assault
55	R v Maybarskan	2003	Southampton Crown Court	Conspiracy to supply Class A drugs
56	R v Mustifa	2003	Southampton Crown Court	Conspiracy to supply Class A drugs
57	Jameel v Wall Street Journal (Europe)	2003	High Court (QB)	Libel (surveillance of bank records)
58	R v SO	2003	Newcastle Crown Court	Making indecent images of children

59	R v Walsh & others	2003	Kingston Crown Court	Conspiracy to cause serious public disorder
60	R v Baria & others	2003	Birmingham Crown Court	Conspiracy to supply Class A drugs
61	R v Jones and Jones	2003	Newcastle Crown Court	Theft (recovery of computer data)
62	R v Gill	2004	Court of Appeal	Murder (appeal)
63	R v Brett	2004	Middlesborough Crown Court	Conspiracy to supply Class A drugs (surveillance)
64	R v Thomas	2004	Liverpool Crown Court	Robbery
65	R v DC	2004	Hartlepool Crown Court	Making indecent images of children (Operation Ore)
66	R v GW	2004	Hartlepool Crown Court	Making indecent images of children (Operation Ore)
67	R v Powell & others	2004	Woolwich Crown Court	Conspiracy to supply Class A drugs
68	R v C	2004	Durham Crown Court	Sexual offences (child)
69	R v Patterson	2004	Gateshead Magistrates Court	Stolen goods
70	R v Swindon & Conway	2004	Bradford Crown Court	“Ram raid” thefts
71	R v Khachik & others	2004	Court of Appeal	Conspiracy to supply Class A drugs (appeal)
72	Davies v Commissioner	2004	High Court	False arrest (civil action)
73	R v O’Hagan	2005	High Court Belfast	Prevention of Terrorism Act
74	R v Pickering	2004	Middlesborough Crown Court	Conspiracy to supply Class A drugs (surveillance)
75	Al Rahji Bank v Wall Street Journal	2004	High Court (QB)	Libel (re bank accounts used for Al Qaeda Terrorism)
76	R v Curry	2004	Newcastle Crown Court	Harassment (appeal)
77	R v Waite & others	2004	Leeds Crown Court	Armed Robbery
78	R v JC	2005	St Albans Crown Court	Making indecent images of children (Operation Ore)
79	R v SR	2007	Stafford Crown Court	Making indecent images of children (Operation Ore)
80	R v Ciaran Kearney	2005	High Court, Belfast	Theft and Terrorism (Stormont)
81	R v J	2004	Norwich Crown Court	Making indecent images of children
82	R v Bourgass & ors	2005	Central Criminal Court	Terrorism
83	R v CS	2005	Norwich Crown Court	Making indecent images of children (Operation Ore)
84	R v Austin & ors	2006	Winchester Crown Court	Conspiracy to import class A drugs
86	R v SB	2008	Court of Appeal	Appeal (Operation Ore)
87	R v DM	2005	Leicester Crown Court	Making indecent images of children (Operation Ore)
88	R v Shergold and Iddon	2005	Preston Crown Court	Conspiracy to murder
89	R v Mullan	2005	Leeds Crown Court	Distribution of class A drugs

90	R v Shan, Dad and Ors	2005	Newcastle Magistrates Court	Assault and wounding
91	R v Fox & ors	2005	Woolwich Crown Court	Armed robbery
92	R v Rowe	2005	Central Criminal Court	Terrorism
93	R v MT	2006	Stafford Crown Court	Making indecent images of children (Operation Ore)
94	R v NH	2005	Norwich Crown Court	Making indecent images of children (Operation Ore)
95	R v Curran	2006	Southwark Crown Court	Fraud
96	R v DW	2006	St Albans Crown Court	Making indecent images of children (Operation Ore)
97	R v MD	2006	Norwich Crown Court	Making indecent images of children
98	R v DG	2006	Birmingham Crown Court	Making indecent images of children (Operation Ore)
99	R v Garcia and others	2007	Central Criminal Court	Terrorism
100	R v PH	2007	Birmingham Crown Court	Making indecent images of children (Operation Ore)
101	R v GK	2006	Middlesborough Crown Court	Making indecent images of children
102	R v GP	2006	Lewes Crown Court	Making indecent images of children
103	R v JF	2009	Belfast Crown Court	Making indecent images of children (Operation Ore)
104	R v Hoey	2007	Belfast Crown Court	Terrorism
105	R v SK	2007	Newry Crown Court	Making indecent images of children (Operation Ore)
106	R v GO	2006	Newry Crown Court	Making indecent images of children (Operation Ore)
107	R v MM	2007	Newry Crown Court	Making indecent images of children (Operation Ore)
108	R v SB	2008	Court of Appeal	Appeal (Operation Ore)
109	R v Kent Police *ex parte* A	2006	High Court	Judicial Review (Operation Ore)
110	R v Akbar	2006	Central Criminal Court	Terrorism
111	R v Kahar	2006	Central Criminal Court	Terrorism
112	R v Somers	2006	Belfast Crown Court	Murder
113	R v Yahya	2007	Central Criminal Court	Terrorism
114	R v Iqbal	2007	Birmingham Crown Court	Attempted murder
115	R v Davies	2008	Manchester Crown Court	Distribution of class A drugs, concealment of profits
116	R v Shaffi	2007	Central Criminal Court	Terrorism
117	JC v Bedfordshire Police	2011	High Court	Wrongful arrest (Operation Ore)
118	R v DM	2009	Newry Crown Court	Making indecent images of children (Operation Ore)
119	R v Harriman	2006	Hartlepool Crown Court	Theft
120	R v McEvoy	2007	Belfast Magistrates Court	Robbery (Irish Bank) and Kidnap

121	R v MD	2010	Lewes Crown Court	Making indecent images of children
122	R v Zafar	2007	Central Criminal Court	Terrorism
123	R v Al-Daour	2007	Central Criminal Court	Terrorism
124	R v Barker	2006	Leeds Crown Court	Corruption in public office
125	R v Sikander	2011	Court of Appeal	Appeal (kidnap and assault)
126	R v Abu Hamza	2006	Central Criminal Court	Terrorism
127	R v Iwegbu	2006	Central Criminal Court	Murder
128	R v Lindo	2006	Central Criminal Court	Murder
129	R v Nassari	2007	Central Criminal Court	Terrorism
130	R v Siddique	2007	High Court, Glasgow	Terrorism
131	R v Al Faqih	2007	Birmingham Crown Court	Terrorism
132	R v Ashgar	2007	Central Criminal Court	Attempted murder
133	R v Feroze	2007	Woolwich Crown Court	Terrorism
134	R v Crossan	2007	Belfast Crown Court	Kidnapping / extortion
135	R v DC	2007	Teesside Crown Court	Making indecent images of children (incitement)
136	R v MM	2008	Antrim Crown Court	Making indecent images of children (Operation Ore)
137	R v Brown	2008	Manchester Crown Court	Fraud
138	GMC v AE	2008	GMC Fitness to Practice Panel	Making indecent images of children (Operation Ore)
139	R v Tarmohamed	2007	Woolwich Crown Court	Terrorism
140	R v Gulzar	2008	Woolwich Crown Court	Terrorism
141	R v TM	2008	Bedford Crown Court	Making indecent images of children
142	R v John and Boyce	2007	Harrogate Magistrates Court	Unlawful trespass
143	R V Zaitschek	2008	Belfast Crown Court	Extradition
144	R v McRory	2007	Belfast Crown Court	Kidnapping and robbery
145	R v Sikander	2003	Court of Appeal	Appeal (Kidnap and assault)
146	R v Iqbal	2009	Court of Appeal	Attempted murder (appeal)
147	R v Patel	2008	Central Criminal Court	Terrorism
148	R v Ditta	2008	Woolwich Crown Court	Terrorism
149	R v Sulieman	2008	Blackfriars Crown Court	Terrorism
150	State v JC	2007	Nenagh District Court (Eire)	Making indecent images of children (Operation Amethyst)
151	R v RH	2008	Teesside Crown Court	Making indecent images of children
152	R v Chenery-Wickens	2009	Lewes Crown Court	Murder
153	R v Siddiqui	2009	Central Criminal Court	Terrorism
154	R v Elasmar	2009	Birmingham Crown Court	Terrorism
155	R v W	2009	Dewsbury Magistrates Court	Making indecent images of children
156	R v TR	2009	Lewes Crown Court	Making indecent images of children
157	A v Kent Police	2009	High Court	Wrongful arrest (Operation Ore)
158	R v Haji	2008	Manchester Crown Court	Terrorism

159	PY v Devon and Cornwall Police	2012	High Court	Malicious prosecution (Operation Ore)
160	County Autocall v Williams	2009	Brighton County Court	Civil action
162	R v Yusuf	2009	Blackfriars Crown Court	Terrorism
163	R v Thomas	2010	Central Criminal Court	Attempted murder
164	R v Nadeem & ors	2009	Central Criminal Court	Terrorism
165	R v W	2009	Kingston Crown Court	Grooming a minor
166	R v Craig	2010	Belfast Crown Court	Arson
167	R v De Silva	2009	Central Criminal Court	Murder
168	Mardas v IHT	2010	High Court (QBD)	Libel
168	State v Eccles	2010	State of Jersey	Indecent assault
169	R v Randall	2010	Leeds Crown Court	GBH
170	R v Kanmi	2010	Preston Crown Court	Terrorism
171	R V CS	2010	Kingston Crown Court	Making indecent images of children
172	R v NO	2011	Canterbury Crown Court	Making indecent images of children (Operation Sledgehammer)
173	US v Khan	2011	Federal Court NYC	Terrorism
174	R v Karim	2011	Woolwich Crown Court	Terrorism
175	R v PO	2012	Chester Crown Court	Making indecent images of children (Operation Sledgehammer)
176	R v Belle	2012	Luton Crown Court	Supply of firearms
177	R v MD	2012	Southwark Crown Court	Making indecent images of children
178	R v GMD	2012	Croydon Crown Court	Making indecent images of children
179	R v Faraz	2012	Woolwich Crown Court	Terrorism
180	R v Faraz	2012	Woolwich Crown Court	Terrorism
181	R v Afzal	2012	Preston Crown Court	Conspiracy to supply Class A drugs
182	R v Javed	2012	Central Criminal Court	Terrorism
183	R v DP	2013	Maidstone Crown Court	Making indecent images of children
184	R v Maroof	2012	Stafford Crown Court	Conspiracy to assist a prisoner to escape
185	R v TN	2013	Croydon Crown Court	Making indecent images of children
186	R v SW	2013	Croydon Crown Court	Making indecent images of children
187	R v MH	2013	Croydon Crown Court	Extreme pornography
188	R v Newall	2011	Kingston Crown Court	Conspiracy to supply Class A drugs
189	R v Driver	2013	Maidstone Crown Court	Making indecent images of children
190	R v Latif	2013	Woolwich Crown Court	Terrorism
191	R v Emde	2012	Woolwich Crown Court	Terrorism
192	R v Papachristos	2013	Blackfriars Crown Court	Fraud

193	R v Dixon	2015	Court of Appeal	Conspiracy to murder
194	R v Nicholas	2014	Court of Appeal	Conspiracy to murder
195	R v Parsons	2014	Manchester Crown Court	Theft and fraud
195	R v Abushofa	2014	Immigration Court	Immigration appeal
196	Dar al Arkan v Al Raji	2014	Commercial Court	Commercial Claim (Saudi Arabia)
197	R v MP	2015	Maidstone Crown Court	Making Indecent images of children
198	R v PO	2016	Court of Appeal	Making Indecent images of children
199	R v JH	2017	Clerkenwell Magistrates Court	Making Indecent images of children
200	R v Lank	2016	Central Criminal Court	Conspiracy to procure misconduct in public office
201	R v Ullah	2016	Central Criminal Court	Terrorism
202	U.S. v Khatallah	2017	Federal Court Southern District of New York	Terrorism
203	R v GJ	2018	Aylesbury Crown Court	Making indecent images of children, grooming
204	Sardarov v Sardarova	2017	Royal Courts of Justice	Divorce proceedings
205	Yukos v Foresman	2019	Commercial Court	Commercial Claim
206	R v Kamali	2019	Central Criminal Court	Terrorism
207	Rich v Butkowsky	2020	Federal Court, Washington DC	Libel
208	R v Earle	2020	Liverpool Crown Court	Conspiracy to murder