REPORT OF THE INVESTIGATORY POWERS COMMISSIONER

(GUERNSEY)

REVIEW PERIOD: JANUARY – DECEMBER 2019

LORD ANDERSON OF IPSWICH K.B.E. Q.C.
JULY 2020

INTRODUCTION

1. The Investigatory Powers Commissioner **[the Commissioner]** is a judge of the Guernsey Court of Appeal, appointed by the Bailiff under the Regulation of Investigatory Powers (Bailiwick of Guernsey) Law 2003 **[RIPL]** s53 to keep under review the exercise and performance of the powers and duties conferred and imposed under certain parts of RIPL.

2. Those powers and duties relate to the following investigatory techniques:

    a. Interception of communications (RIPL Part I Chapter I, ss 1-10 and 12)

    b. Acquisition and disclosure of communications data (RIPL Part I Chapter II)

    c. Directed surveillance, intrusive surveillance and covert human intelligence sources **[CHIS]** (RIPL Part II Chapter I)

    d. Interference with property (RIPL Part II Chapter II)

    e. Investigation of electronic data protected by encryption etc. (RIPL Part III).

    RIPL confers limited powers on specified persons to authorise the use of those techniques for stated purposes. It also regulates the use that can be made of material gained as a result.

3. It is not the function of the Commissioner to keep under review the exercise of any power of the States of Guernsey, the States of Alderney, the Chief Pleas of Sark or any committee thereof to make, amend or revoke any legislation (RIPL s53(4)).

4. The Commissioner is obliged to make an annual report to the Bailiff with respect to the carrying out of the Commissioner's functions (RIPL s54(4)). That report is to be made as soon as practicable after the end of each calendar year, and a copy of it laid before the Royal Court together with a statement as to whether any matter has been excluded from it because it appears to the Bailiff, after consultation with the Commissioner, that publication of that matter would be (RIPL s54(7)):

    a. contrary to the public interest, or

    b. prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the Bailiwick, or the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Commissioner.

5. I was appointed as Investigatory Powers Commissioner in 2017, in succession to Sir David Calvert-Smith who retired from the Court of Appeal upon reaching the statutory retirement age of 72. This is my third and final annual report, covering the calendar year 2019.

THE POWERS UNDER REVIEW

6. Legal definitions of the powers under review are to be found in RIPL and are not repeated here. But for the benefit of those without detailed expertise in these matters, I describe in this section what the use of these powers tends most commonly to involve in practice, and summarise the nature of the constraints placed by RIPL upon their exercise.

7. Before doing so, I would make three points of a general nature concerning the powers under review.

    a. ***Utility:*** The use of investigatory powers is generally (and correctly) associated with the detection and investigation of crime. They were used for that purpose during the period under review by Guernsey Police, Guernsey Border Agency and Guernsey Social Security. Use of the powers can help exonerate as well as implicate suspects. Communications data in particular can be very useful also outside the criminal context, notably in missing persons investigations.

    b. ***Cumulative benefit:*** *S*erious crime investigations will often, over time, make use of a range of covert powers, whether used by Guernsey Law Enforcement or by partners such as the National Crime Agency in the UK. Such powers contribute in different ways to an effective operation: their benefit is cumulative and cannot easily be attributed to the use of one rather than another. Accordingly, while it has been possible for illustrative purposes to quantify the arrests and seizures in operations where interception was used (Figure 1, below), other covert techniques were also usefully deployed in those operations as in others.

    c. ***Internal safeguards:*** Internal scrutiny mechanisms are applied before use of investigatory powers is authorised. Thus:

        i. In relation to acquisition of communications data, a Single Point of Contact ("SPOC") ensures that that the application is legally compliant and of the necessary standard to be recommended to the Authorising Officer. The SPOC is a member of staff who has completed an accredited training course and who is able to advise also whether it is technically possible to obtain the data that is wished for.

ii. In relation to interception, directed and intrusive surveillance and property interference, an equivalent function is performed by a Gatekeeper: normally, an experienced Higher Executive Officer/Sergeant or Senior Investigating Officer/Inspector.

iii. Authorising Officers (including the Law Officers, where the more intrusive powers are concerned) are themselves under a duty to reject requests or to request resubmissions where they are not satisfied that the conditions for granting them have been made out.

SPOCs, Gatekeepers and Authorising Officers are not box-tickers: their function is to speak up should they have reservations about any proposed use of covert investigatory powers. It speaks well of Guernsey Law Enforcement, and of the ethos surrounding the use of investigatory powers in Guernsey, that each was prepared to do so during the period under review. Equally important is the system by which administrative errors are recorded and, if potentially serious, notified to the Investigatory Powers Commissioner for comment and further action as may be required. I comment further on errors at paras 74-76 below.

Interception of communications (RIPL Part I Chapter I)

8. The interception of communications in the course of their transmission traditionally refers to the opening of mail but more commonly now takes the form of listening in to telephone conversations (phone-tapping).

9. The interception of such communications in the course of their transmission is normally a criminal offence in Guernsey (RIPL s1).

10. Interception is however lawful when authorised by an interception warrant issued personally by a Law Officer (s5: the reference to HM Procureur is deemed by s67 to include HM Comptroller). Warrants may be applied for by the Chief of Police, the Chief Officer of Customs and Excise, and competent authorities of other countries or territories with which Guernsey has a mutual assistance agreement (s6).

11. A warrant may only be issued if a Law Officer believes it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the Bailiwick or to give effect for serious crime purposes to the provisions of international mutual assistance agreements (s5(3)). The

conduct authorised by the warrant must also be proportionate to what it is sought to achieve (s5(2)(b)).

12. Serious crime is defined, for the purposes of RIPL, as offences which involve the use of violence, result in substantial financial gain or constitute conduct by a large number of persons in pursuit of a common purpose, or for which a person over 21 with no previous convictions could reasonably be expected to be sentenced to imprisonment for three years or more (s67(3)).

13. Detailed provision is made in RIPL for the contents of warrants (s7), their duration, cancellation and renewal (s8), their modification (s9) and their implementation (s10). Safeguards relating to the dissemination, retention and disposal of intercepted material are set out in ss 12 and 13.

14. Disclosure of the issue of a warrant, the interception of a communication or the content of an intercepted communication (intercepted material or "intercept") is generally prohibited (ss 14-16). As in the UK and Jersey, but in contrast to most of the rest of the world, intercept is therefore inadmissible as evidence in criminal trials in Guernsey. This means that when intercept is sought in Guernsey, the intention is generally to find not evidence but intelligence which can help build a picture of the criminality involved, or assist in planning a disruption or further intervention from which admissible evidence may be acquired.

15. The very limited circumstances in which interception is lawful without a warrant are set out in RIPL s3.

Acquisition and disclosure of communications data (RIPL Part I Chapter II)

16. Communications data are data about use made of a telecommunications service, excluding the contents of the communications themselves. They are sometimes described as the "who, how, when and where" of a communication. Communications data are generally obtained retrospectively from a communications service provider **[CSP]** that retains that information, such as a mobile phone company or broadband provider. When intercept is collected in the course of transmission pursuant to RIPL Part I Chapter I, the related communications data are also collected.

17. There is no power in Guernsey law to compel CSPs to retain communications data: accordingly, the availability of such data depends on the practices of the various CSPs, which vary considerably as between themselves.

18. The different types of communications data, defined in RIPL s67(3), are grouped for operational purposes under the following heads:

    a. ***subscriber information*** held by Communication Service Providers **[CSPs]** in relation to their customers, e.g. address, phone number or email address and bank account data; and

    b. ***call data*** held by CSPs in relation to the use made of their telecommunications (or postal) system, including data identifying the apparatus, location or address to or from which a communication is transmitted, and location data provided by mobile phones on the move, as they communicate with base stations or phone masts (cell-site data).

19. The acquisition of communications data is treated by the law as less intrusive than the interception of content, even though it is possible to tell a good deal about a person's movements and contacts through analysis of communications data. Accordingly, the range of purposes for which communications data may be obtained (s18(2)) is considerably wider than in the case of interception. For example, communications data may be requested if necessary "*for the purpose of preventing or detecting crime or of preventing disorder*" (s18(2)(b)), not merely for the purpose of preventing or detecting *serious* crime (s5(3)). It may also be requested in the interests of public safety or public health, for the purpose of assessing or collecting taxes or, in an emergency, for preventing death or injury (s18(2)(d)-(g)).

20. The range of public authorities permitted to access communications data is also wider than in the case of interception (s20). Police and Customs may issue their own authorisations (s20(1)(a)(b)), after the application of internal safeguards; other public authorities must obtain authorisation from the Law Officers (s20(1)(c)).

21. Communications data can be obtained by the giving of notices to a postal or telecommunications operator, requiring the operator to obtain and/or disclose relevant data (s18(4)). As in the case of interception warrants, such notices may be issued by a designated person only when the requirements of necessity and proportionality are satisfied.

22. Provision is made in RIPL for the form and duration of authorisations and notices (s19).

23. Communications data, unlike intercept, are admissible as evidence in legal proceedings in Guernsey, and indeed often form a significant part of the prosecution case in relation to organised crime or conspiracy.

Directed and intrusive surveillance (RIPL Part II Chapter I)

24. Surveillance is defined by RIPL s69 as including "monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications", and recording the product. For the purposes of RIPL, surveillance does not include the use of CHIS or warranted interception.

25. To be classed as ***intrusive surveillance***, it must be covert (s21(9)), and carried out in relation to anything taking place on any residential premises or in any private vehicle (s21(3)). Though it may involve the presence of an individual, it classically takes the form of a technical surveillance device: for example a "bug" placed in a vehicle or a dwelling. Surveillance carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle is not intrusive (s21(4)(a)).

26. Because of its capacity to intrude into private spaces, intrusive surveillance may be authorised only for the same limited purposes as interception, and on satisfaction of the same conditions as to necessity and proportionality (s26(2)(3)). Authorisations for intrusive surveillance may also be issued by the Chief Officer of the Police and Customs and Excise (s26(1)(6)), but save in cases of urgency they may not take effect until approved by HM Procureur or Comptroller, who also have a power to quash or cancel (ss 30-31).

27. General rules about grant, renewal and duration of authorisations are in RIPL s34. Provisions relating to applications for intrusive surveillance by the UK intelligence services and armed forces are in ss 33 and 35.

28. Covert surveillance that is not intrusive but that is undertaken for the purposes of a specific investigation or operation, in such a manner as is likely to result in the obtaining of private information about a person, is known as ***directed surveillance*** (s21(2)). A classic form of directed surveillance is static, foot or mobile surveillance in the street. The use of tracking devices, and targeted open source research (including online research), may also class as directed surveillance. Directed surveillance assists in the prevention and detection of a wide range of crimes, from drugs offences to harassment. Though generally targeted on a particular suspect, it can and does identify the associates of known targets, as well as criminal activity not already known to law enforcement. Like other forms of surveillance, it may also help decide the most propitious moment to launch executive action.

29. Directed surveillance is controlled in a manner analogous to the acquisition of communications data. The range of grounds on which the obtaining of communications data may be authorised are the same (s23(3)), and the range of public authorities permitted to

authorise it, through individuals of offices, ranks or positions specified by regulations under s25, is wide (Schedule 1). The usual requirements of necessity and proportionality apply.

Covert human intelligence sources (CHIS) (RIPL Part II Chapter I)

30. A person is deemed to be a CHIS if they establish or maintain a personal or other relationship with a person for the covert purpose of obtaining information, or if they covertly disclose information obtained from such a relationship (RIPL s21(8)). CHIS can be, but are not always, paid small amounts of money for their work by the public authorities that use them.

31. The public authorities entitled to use CHIS are the same as those authorised to use directed surveillance (Schedule 1). The system for authorisation, and the range of grounds for which CHIS may be authorised, are also the same (s24). Additional requirements are spelled out in s24(5). In particular:

    a. An officer (known as the handler) must have day-to-day responsibility for contact with the CHIS and for his or her welfare.

    b. A different officer (known as the controller) must oversee the use of the CHIS.

    c. Records must be kept of such use.

    d. There must be restricted access to details of the source's identity.

Interference with property (RIPL Part II Chapter II)

32. RIPL s 39 renders lawful "entry on or interference with property or with wireless telegraphy", if authorised by HM Procureur or HM Comptroller in accordance with the Law. The concept of interference with property is not closely defined. It includes, for example, the interference with the fabric of a dwelling that may be required to insert a surveillance device: with this in mind, RIPL s27(3) provides for HM Procureur or HM Comptroller to issue combined authorisations under RIPL Part II Chapters I and II.

33. Property interference may be authorised only where HM Procureur or HM Comptroller believes that it is necessary for the purpose of preventing or detecting serious crime or in the interests of national security, and that the taking of the action is proportionate to what it seeks to achieve (RIPL s40(2)).

Investigation of data protected by encryption (RIPL Part III)

34. The law of the Bailiwick of Guernsey (like that of the UK, but not that of Jersey) allows for the issue of notices requiring the disclosure of the key to encrypted information that is lawfully within the possession of the authorities. Typically, it is used to obtain passwords allowing access to electronic devices such as mobile phones.

35. Such notices may be given where a person permitted under RIPL Schedule 2 reasonably believes it to be necessary on the restricted set of grounds applicable also to interception and intrusive surveillance, and to be proportionate: s46(2)(3).

36. Failure to comply with a notice under s46 is a criminal offence, punishable by up to two years' imprisonment after conviction on indictment and six months after summary conviction (s49). It is conceivable therefore that suspects facing long prison sentences if they are convicted of the index offence may choose to take their chances by disobeying a s46 notice. Part III has however proved its utility in Guernsey, as detailed further below.

Codes of Practice and Guidance

37. RIPL ss 61-62 provides for the issue of codes of practice. Five such codes – on accessing communications data, CHIS, covert surveillance, interception of communications and interception of communications (postal) – were brought into operation pursuant to the Regulation of Investigatory Powers (Codes of Practice) (Bailiwick of Guernsey) Order 2004.

38. Guernsey's codes of practice have drawn heavily on those produced in the UK under the Regulation of Investigatory Powers Act 2000 **[RIPA]**. That remains the governing statute in the UK for directed and intrusive surveillance, CHIS, interference with property and investigation of data protected by encryption.

39. However, where the interception of communications and the acquisition and disclosure of communications data are concerned, RIPA has been replaced in the UK by the Investigatory Powers Act 2016 **[IPA]**. New codes of practice under IPA have been produced in the UK on the exercise of both these powers. Those codes have much in common with the old RIPA codes, but they reflect a few significant statutory differences. The most notable of these relates to the acquisition of communications data, where (in response to a 2016 judgment of the Court of Justice of the EU) a new, independent Office for Communications Data Acquisition **[OCDA]** has taken over the authorisation of communications data acquisition in the UK.

CONDUCT OF THE ANNUAL REVIEW

Appointment of Assistant Commissioners

40. As stated at the start of this report, the conduct of the annual review is conferred by law upon a judge of the Guernsey Court of Appeal, appointed by the Bailiff as Investigatory Powers Commissioner. The statutory scheme in the UK, both under RIPA and IPA, makes similar provision. Thus, the annual report of the Investigatory Powers Commissioner's Office **[IPCO]** in the UK is prepared under the supervision of the Commissioner (since October 2019 Rt. Hon. Sir Brian Leveson, a recently-retired Judge of the Court of Appeal of England and Wales).

41. The conduct of effective review at police forces, customs and other users of investigatory powers is however recognised in the UK to require additional expertise, different from that conventionally possessed by Judges. Accordingly, such inspections are normally conducted not by the UK Commissioner himself but by specialised inspectors from the Investigatory Powers Commissioner's Office **[IPCO]**.

42. Often from a law enforcement, intelligence or civil service background, these inspectors have a close familiarity with the relevant capabilities and procedures. They are skilled in interrogating the electronic systems on which records are kept. Because they spend the entire year inspecting law enforcement and other bodies which use investigatory powers, they also have a deep knowledge of constantly-evolving good practice. Much of this practice relates to matters outside the normal experience of a judge: for example

    a. the procedures for investigation of criminality within public authorities;

    b. the optimal methods of deploying a variety of covert means at different stages of an investigation;

    c. the considerable complexities and risks that attend the handling of CHIS;

    d. systems and procedures designed to prevent errors in accessing communications data; and

    e. the operation of the various available systems for data management.

43. Since coming to know IPCO (and its predecessor bodies) in the UK, I have been conscious of the significant value that their inspectorate would be able to add to the inspection process in Guernsey. Accordingly and at my request, the Investigatory Powers Commissioner agreed

to make available to me (without charge to the Government of Guernsey, save as to travel and subsistence) the services of the IPCO inspectorate for each of my first two inspections, as follows:[1]

a. For my April 2018 inspection (reviewing the 2017 calendar year), I was accompanied as Assistant Commissioner by Clare Ringshaw-Dowle, an IPCO Chief Inspector specialising in intrusive and directed surveillance, CHIS and property interference.

b. For my April 2019 inspection (reviewing the 2018 calendar year), I was accompanied as Assistant Commissioners by Clare Ringshaw-Dowle and by Alex Drummond, an IPCO Chief Inspector with equivalent expertise in the interception of communications and acquisition and disclosure of communications data.

44. Both Assistant Commissioners brought knowledge and understanding to the task that no senior Judge could be expected to possess. Their detailed recommendations, drawn from their expert knowledge of current best practice in UK law enforcement, were made both in oral briefings to relevant personnel and in the confidential reports which are submitted to the Bailiff alongside this Report. The management of investigatory powers in Guernsey has benefited significantly from their involvement.

45. I place on record my gratitude to IPCO for lending me the services of these Assistant Commissioners. IPCO through its Chief Executive, Amanda Jeffery, indicated to me in June 2019 that it is prepared to continue supporting future inspections in the Channel Islands, by offering one or two inspectors, who may include a Chief Inspector, with the relevant expertise. If this offer is made good in years ahead, it can only be to the benefit of Guernsey.

46. The inspection visit to Guernsey booked with IPCO for w/c 18 May 2020 had to be called off because of the COVID-19 virus, which has also made exceptional claims on the time of IPCO inspectors. I have accordingly prepared this report without the assistance of IPCO inspectors on the ground, though they have been generous with their advice both during the year under review and in connection with the preparation of this report. I hope that their help will be available to my successor as required.

Briefings

47. After my appointment as Commissioner, I held a day of preliminary meetings in September 2017 with Law Officers, Police and Customs and Social Security. At those meetings I was

[1] That was in turn facilitated by the passage of the Regulation of Investigatory Powers (Bailiwick of Guernsey) (Amendment) Ordinance 2018, which amended RIPL s55(2) to allow for the appointment of an Assistant Commissioner who has not held judicial office.

briefed in some detail on current conditions regarding crime and immigration, and the role of investigatory powers in supporting investigations, operations and prosecutions.

48. In past years, my inspections have been based upon detailed, classified written accounts of the use of each of the relevant powers by Guernsey Law Enforcement. Those accounts have been supplemented by the opportunity to inspect files showing the procedures that were followed in each case, and by interviews in a secure space with personnel at all levels of both organisations involved in the authorisation, management and oversight of covert operations. Based on the case files, I have also been able to discuss with the Law Officers the manner in which they discharged their authorising functions.

49. Since no inspection visit was possible in 2020 because of the COVID-19 virus, this report has had to be prepared without detailed examination of case files or interviews based on those files with key staff and teams involved in the authorisation, management and oversight of covert operations. Guernsey Law Enforcement and Social Security were however able to send me a series of detailed reports and appendices via secure email, and I was able to discuss aspects of this material remotely. I am grateful to all involved for their painstaking work on this.

SCOPE OF THIS REPORT

50. There is an obvious public interest in legislators, and indeed the people of Guernsey, understanding at least in outline how the intrusive powers conferred by law upon the public authorities translate into capabilities which are exercised on their behalf. That is the means by which those entrusted with these intrusive powers are rendered accountable to those whom they serve. Accordingly, in the body of this report, I have endeavoured to publish as fully as possible the conclusions of my review.

51. The trend in recent years in the UK and across the democratic world has been towards fuller and more transparent scrutiny of the use made of covert investigatory powers. IPCO constitutes an outstanding example of such scrutiny.[2]

52. In advising the Bailiff on what material should and should not be placed in the public domain, I have been guided by the practice of my predecessor Sir David Calvert-Smith, and by the developing practice of other oversight bodies. I have noted, in particular, that reports of the Interception of Communications Commissioner and the Surveillance Commissioner for the Isle of Man specify how many warrants and authorisations under the various different

[2] See most recently IPCO, *Annual Report – 2018*, HC 67, March 2020.

categories have been granted during the review period.[3] I adopted that course in my first two reports for most of the powers under review, and do so again this year.

53. I am also conscious, however, that there are special factors in a small jurisdiction such as Guernsey that make it difficult to disclose information as comprehensive as that which is released by IPCO in the UK. To take two examples:

    a. IPCO breaks down national figures for requests relating to criminal activity by crime type. Bearing in mind the low level of serious criminality in Guernsey and its small size, this is not a course that could safely be taken without giving at least a hint of the extent to which investigatory powers may have been used (or not used) in specific operations or investigations.

    b. The lengthy Annex C to the March 2020 IPCO report sets out the facts of 22 error investigations in considerable detail. Once again, to take a similar course would risk the identification of specific individuals and operations.

54. In this open report and its two predecessors, I have sought to describe the nature of the powers under review, and to give an indication of how much each power has been used. I have not given a detailed breakdown for the use of investigatory powers by the different public authorities in Guernsey, so as to avoid any risk of the use of powers in specific operations being identified, but note that the overwhelming majority of authorisations and warrants requested and granted were:

    a. in support of the activities of Guernsey Police, the Guernsey Border Agency and Social Security; and

    b. for the purpose of preventing or detecting crime.

55. Further detail is reserved to the confidential reports to the Bailiff, which in past years have been prepared by my Assistant Commissioners under my supervision. Those reports may be provided at the Bailiff's discretion to those who apply for and authorise investigatory powers, so as to inform their training and pursuit of best practice. This year I have directed that the classified reports supplied to me be conveyed to the Bailiff as confidential appendices to this report.

[3] See most recently the annual reports for 2018 of the Interception of Communications Commissioner and of the Surveillance Commissioner for the Isle of Man, March 2019.

INTERCEPTION

56. A total of 37 warrants for interception were issued during 2019, relating to the subjects of 10 operations. Most of the operations concerned drug trafficking into Guernsey and associated money laundering offences.

57. There were, in addition, 152 applications for communications data on numbers linked to warranted numbers. 96 of these were "*short form*" applications, used to obtain subscriber information and call and traffic data on numbers that have been in direct contact with a warranted number. The remainder were "*long form*" applications, similar to those that must be made to acquire communications data in other contexts. These figures are comparable to those for 2018.

58. The interception of communications during 2019 was instrumental in securing the arrest of 25 individuals. 15 of those individuals were charged with criminal offences during 2019, and 12 convicted and sentenced with other cases still in progress. In operations where interception was used, drugs were seized to the value of £834,215.10, with cannabis accounting for more than 99% of that sum (£830,972.75). Cash used in related money laundering offences was also seized to a value of £146,876.

59. The equivalent headline figures for the past three years are shown in Figure 1, below.

Figure 1: interception warrants

Year	Warrants	Operations	Arrests	Drugs	Cash
2017	**33**	**6**	**19**	**£307,093**	**£168,270**
2018	**24**	**11**	**22**	**£181,122**	**£140,572**[4]
2019	**37**	**10**	**25**	**£834,215**	**£146,876**

COMMUNICATIONS DATA

60. As in the UK, communications data requests were the most widely used of the investigatory powers in Guernsey. There were 129 authorisations, of which 16 were for subscriber information, 70 for call data information and 43 for other categories of information.[5]

[4] Plus EUR 3,280.

[5] The meaning of subscriber information and call data is explained at para 19 above. These figures do not include the figures for acquisition and disclosure of communications data obtained in support of warrants of interception, as to which see para 58 above.

Figure 2: communications data

Year	Authorisations	Urgent	Subscriber info	Call data	Both
2017	**175**	**N/A**	**59**	**76**	**40**
2018	**129**	**19**	**16**	**70**	**43**
2019	**121**	**21**	**31**	**50**	**40**

61. Communications data is useful not just for linking individuals with electronic devices but for tracing their patterns of organisation, communication and movement. It can be of value for piecing together criminal networks and activities, for supporting the alibis of innocent suspects and for tracing missing persons. Another use is in "*resolving*" IP addresses, a technique which can be of value for example in identifying which of a number of possible devices has been accessing indecent images of children from a server.

62. Accordingly, communications data was used during the period under review not only to target drug trafficking networks but in support of investigations into other crimes including child sexual exploitation.

63. A total of 19 urgent authorisations were granted in 2018 in relation to missing persons who were perceived to be vulnerable (e.g. at risk of taking their own life, or missing children at risk of sexual exploitation). Such applications may be to obtain details of telephone calls, location data or an IP address. They are made orally, and then in written form at the earliest opportunity after the event.

64. Communications data are typically sought for periods ranging from a few minutes to a few months, depending on the demands of the operation in question.

65. Communications data formed part of so many investigations, in conjunction with so many other types of evidence and intelligence, that it would be a difficult or impossible task to attribute any particular number of arrests, convictions or seizures to its use.

66. My inspections in 2018 and 2019 concluded that as in the case of interception, GLE accessed communications data lawfully and for the correct statutory purposes. The processes and procedures in place were fit for purpose, and the personnel involved took pride in their work and are committed to high standards. Though a similar detailed inspection was not possible in 2020, with the result that no equivalent conclusion can be stated, I have no reason to believe that standards had slipped in 2019.

INTRUSIVE SURVEILLANCE / PROPERTY INTERFERENCE

67. Two authorisations for intrusive surveillance were granted in 2019. Seven applications for interference with property were applied for and granted in 2019, all for the purpose of preventing or detecting serious crime, specifically drug trafficking and cash offences. Four of those applications were urgent.

DIRECTED SURVEILLANCE

68. A total of 14 directed surveillance authorisations were granted in the period under review by Guernsey Law Enforcement (down from 38 in 2017), the majority of them relating to drug trafficking and others relating to a range of crimes. A total of five authorisations were granted orally, due to circumstances deemed to be of an urgent nature.

69. A further eight applications for directed surveillance were granted by Social Security for the purpose of investigating benefit fraud. Each operation was graded as successful (either because it resulted in the closure or adjustment of benefit, or because it enabled the case to be dismissed). Three cases were subsequently referred for consideration of prosecution. Operations in which direct surveillance was used were responsible during the period under review for the identification of £10,051.97 in overpayments and an estimated yearly benefit outlay saving of £92,989.26.

Figure 3: Intrusive surveillance, property interference, directed surveillance authorisations

Year	IS	PI	DS: GLE	DS: S/S	DS: total
2017	**2**	**5**			**38**
2018	**0**	**8**	**14**	**10**	**24**
2019	**2**	**7**	**20**	**8**	**28**

COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

70. During the reporting period Guernsey Law Enforcement (Police and Border Agency) used the services of registered CHIS.

71. In each of the past two years, Assistant Commissioner Ringshaw-Dowle was satisfied that the relevant sections of RIPL had been properly applied, that authorisations granted had been properly made and that the continuation or cancellation of such authorisations had been kept under proper review. She also made a number of recommendations in 2017, which were acted upon in a satisfactory manner during 2018. Though no such expert

guidance was available this year, I registered no cause for concern on the basis of the information provided to me.

INVESTIGATION OF DATA PROTECTED BY ENCRYPTION

72. Thirty-five section 46 notices, the great majority of them requiring passcodes for mobile telephones, were applied for during the period under review. Eight individuals complied with the notices and 21 were charged with non-compliance. Sentences were imposed of up to 10 months' imprisonment (consecutive to the sentence for other offences).

73. Section 46 applications have in the past been inspected and found to be of a high standard: Though their number was higher in 2019 than in the two previous years, I have no reason to believe that the standard was lower during the period under review.

Figure 4: Notices requiring disclosure

Year	Notices	Complied	Charged
2017	**12**	**N/A**	**N/A**
2018	**12**	**2**	**5**
2019	**35**	**8**	**21**

NOTIFICATION OF ERRORS

74. A number of recordable errors relating to communications data were identified during the period of review and notified to me after that period for the purposes of this report. Examples were an error in a notice sent to a CSP; the sending of notices to a CSP in respect of numbers that had been ported from that CSP; and administrative errors on the part of CSPs. In all but one case, these errors were picked up and remedied without excess data being collected or any adverse consequence being suffered by individuals. In the one case where excess data was collected, prompt action was taken to remove the data in question (ensuring that no dissemination occurred) and to ensure that the error will not be repeated.

75. It is incumbent both on the Guernsey public authorities and on the CSPs to maintain the highest standards of accuracy, and regrettable when those standards are not always reached. However, the fact that these errors were picked up and notified to the Commissioner for the purposes of my report is a sign that Guernsey Law Enforcement are properly alert to the possibility of error, and properly aware of their responsibilities.

76. On two occasions during the period under review, I was notified of reportable errors that were potentially more serious, because material was collected without proper authorisation. The first concerned the question of whether an operation met the criteria for directed surveillance when it had not been authorised as such. I advised that it did meet the criteria, and action was taken to prevent similar situations arising in the future. The second concerned the lapse of a direct surveillance authority for a few hours before the intended renewal was authorised. In neither case did the errors lead to arrests. Learning points were identified for the future, and I advised that the unlawfully-obtained product should be destroyed.

CONCLUSION

77. The investigatory powers under review made a significant contribution to the prevention and detection of serious crime in Guernsey. To the extent that I have been in a position to judge, they appear to have been exercised in a compliant, proportionate and conscientious way.

78. I once again found Guernsey Law Enforcement and Social Security to be frank and helpful, both in the very full confidential briefing that they provided and in their responsiveness to my questions.

79. Despite the difficulties inherent in policing relatively small communities, considerable successes have been achieved through the use of a variety of covert tactics. Though my inspection this year has been subject to unavoidable limitations necessitated by COVID-19, I am aware of no reason why the people of Guernsey should not be confident that these intrusive powers were used in 2019, as in previous years, lawfully and productively on their behalf.

Lord Anderson of Ipswich K.B.E. Q.C.
July 2020