

UNCLASSIFIED

**REPORT OF THE INVESTIGATORY POWERS
COMMISSIONER
(GUERNSEY)**

REVIEW PERIOD: JANUARY – DECEMBER 2018

**LORD ANDERSON OF IPSWICH K.B.E. Q.C.
JUNE 2019**

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 second annual report, covering the calendar year 2018.

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.

Interception of communications (RIPL Part I Chapter I)

7. 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).
8. The interception of such communications in the course of their transmission is normally a criminal offence in Guernsey (RIPL s1).
9. 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).
10. 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)).
11. 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)).

12. 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.
13. 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, 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.
14. 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)

15. 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.
16. 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.
17. 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).
18. 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)).
19. 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)).
20. 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.
21. Provision is made in RIPL for the form and duration of authorisations and notices (s19).
22. 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)

23. 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.

24. 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)).
25. Because of its capacity to intrude into private spaces, authorisations for intrusive surveillance may be granted 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 shall not take effect until approved by HM Procurer or Comptroller, who also have a power to quash or cancel (ss 30-31).
26. 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.
27. 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.
28. 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 (Schedule 1), through individuals of offices, ranks or positions specified by regulations under s25, is wide. The usual requirements of necessity and proportionality apply.

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

29. 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.
30. 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)

31. RIPL s 39 renders lawful "entry on or interference with property or with wireless telegraphy", if authorised by HM Procurer 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 Procurer or HM Comptroller to issue combined authorisations under RIPL Part II Chapters I and II.
32. Property interference may be authorised only where HM Procurer 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)

33. 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.

34. 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).
35. 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

36. 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.
37. 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.
38. 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]** is currently taking over the authorisation of communications data acquisition in the UK.

CONDUCT OF THE ANNUAL REVIEW

Appointment of Assistant Commissioners

39. 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. In the same way as I have prepared this report, the annual report of the Investigatory Powers Commissioner's Office [IPCO] in the UK is prepared under the supervision of the Commissioner (until October 2019 Rt. Hon. Sir Adrian Fulford, a serving Judge of the Court of Appeal).
40. The conduct of effective review at police forces, customs and other users of investigatory powers is however recognised in the UK to require additional skills to those 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].
41. 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; and
 - d. the operation of the various available systems for data management.
42. 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.
43. 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 relevant authorities in Guernsey have profited enormously from them, as they have made clear to me.
44. I should like to place on record my gratitude to Sir Adrian Fulford and to IPCO for their generous assistance in lending me the services of these Assistant Commissioners. Happily, IPCO 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.

Briefings

45. 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 briefed in some detail on current conditions regarding crime and immigration, and the role of investigatory powers in supporting investigations, operations and prosecutions.
46. Those briefings were supplemented during my inspections of April 2018 and April 2019. On 1-3 April 2019, my Assistant Commissioners and I were given detailed written accounts of the use of each of the relevant powers by Guernsey Border Agency, Guernsey Police and Social Security. Those accounts were supplemented by conversations with relevant

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.

personnel, and by the opportunity to inspect relevant files showing the procedures that were followed in each case.

SCOPE OF THIS REPORT

47. 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.
48. The trend in recent years in the UK and across northern Europe has been towards fuller disclosure of the use made of investigatory powers. IPCO constitutes an outstanding example.²
49. 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 categories have been granted during the review period.³ I adopted that course in my first report for most of the powers under review, and do so again this year.
50. 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 in specific operations or investigations.
 - b. The lengthy Annex B to the March 2019 IPCO report sets out the facts of 24 error investigations in considerable detail. Once again, to take a similar course would risk the identification of specific individuals and operations.

² See most recently IPCO, *Annual Report – 2017*, HC 1780, March 2019.

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.

51. As in my first report, I have sought (above) to describe a little more fully the nature of the powers under review, and also 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.

52. Further detail is reserved to the confidential reports prepared by my Assistant Commissioners after discussion with me and provided to the Bailiff. Those reports may be provided at his discretion to those who apply for and authorise investigatory powers so as to inform their training and pursuit of best practice.

INTERCEPTION

53. A total of 24 warrants for interception were issued during 2018 (down from 33 in 2017), relating to the subjects of 11 investigations (up from 6 in 2017). Most of the investigations concerned drug trafficking into Guernsey and associated money laundering offences.

54. There were, in addition, 163 applications for communications data on numbers linked to warranted numbers. 126 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.

55. Intercept was instrumental in securing the arrest of 22 individuals (up from 19 in 2017), four of whom were charged, convicted and sentenced in 2018 with other cases still in progress. In operations where interception was used, drugs were seized to the value of £181,122.00 (down from £307,092.90 in 2017). The majority of those drugs (£139,900) were cannabis. Cash used in related money laundering offences was also seized to a value of £140,571.52 + €3,280 (down from £168,270.12 in 2017).

56. Assistant Commissioner Drummond under my supervision made a detailed examination of 14 interception warrants, all of them granted for the statutory purpose of preventing or detecting serious crime. He also interviewed key staff and teams involved in the

authorisation, management and oversight of covert investigations. He also made enquiries into the processes for retention, sharing and destruction of intercept.

57. There was found to be an overall good standard of compliance with the legislation and the Code of Practice. Applications contained a relevant intelligence case, outlining the nature of the criminal conduct under investigation and an explanation of why the proposed activity was considered necessary and proportionate. We identified some areas where further detail would be beneficial, and some where quality would be improved by a more succinct and focussed approach.
58. Three errors relating to interception warrants were recorded during the period under review. All related to administrative human error by the relevant CSP, and resulted in the interception data not being made immediately available. None of the errors resulted in an impact on privacy or human rights, or caused significant detriment to the investigation. Steps have been taken by GLE and the relevant CSP to minimise the risk of reoccurrence.

COMMUNICATIONS DATA

59. As in the United Kingdom, communications data requests were the most widely used of the investigatory powers in Guernsey. There were 129 authorisations (down from 175 in 2017), of which 16 were for subscriber information, 70 for call data information and 43 for both categories of information.⁴
60. 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.
61. 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.
62. 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,

⁴ 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.

location data or an IP address. They are made orally, and then in written form at the earliest opportunity after the event.

63. 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.
64. 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.
65. The inspection 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 take pride in their work and are committed to high standards.

INTRUSIVE SURVEILLANCE / PROPERTY INTERFERENCE

66. No authorisations for intrusive surveillance were granted in 2018 (as against 2 in 2017). Eight applications for interference with property were applied for and granted in 2018 (up from 5 in 2017), all for the purpose of preventing or detecting drug trafficking and money laundering offences.
67. Three of the property interference applications were reviewed by my Assistant Commissioner Clare Ringshaw-Dowle, under my supervision. Each application was found to have been well put together and appropriately authorised.

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. Five of the authorisations were reviewed by my Assistant Commissioner, who noted that some very good results had been achieved in terms of both seizures and arrests. The quality of the applications was generally good: suggestions were made for further improvement.
70. A further 10 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). In two cases, prosecution and conviction resulted. The inspection concluded that Social Security was rightly making use of the powers. However a number of suggestions and a recommendation were made, aimed at ensuring that current best practice standards are followed.

COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

71. During the reporting period Guernsey Law Enforcement (Police and Border Agency) used the services of registered CHIS.
72. As last year, 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.
73. During the last annual review, my Assistant Commissioner was able to use her practical knowledge of CHIS operation to make a number of recommendations aimed at the improvement of practice. Those recommendations were acted on in a satisfactory manner during the period under review.

INVESTIGATION OF DATA PROTECTED BY ENCRYPTION

74. Twelve section 46 notices requiring passcodes for mobile telephones were applied for during the period under review, the same number as in 2017. Two individuals complied with the notices and five were charged with non-compliance. Other charging decisions are pending. Sentences imposed were up to six months' imprisonment for the first offence and four months concurrent for the second.
75. Assistant Commissioner Ringshaw-Dowle inspected two of the section 46 applications, which she believed to be representative of those made over the year, and found both to be of a high standard.

CONCLUSION

76. The investigatory powers under review were, so far as my Assistant Commissioners and I were able to observe, exercised in a compliant, proportionate and conscientious way. They made a significant contribution to the prevention and detection of crime, in particular serious crime, in Guernsey. Though scope for improvement was identified in some respects, levels of compliance were never less than good, and it was particularly pleasing to see that improvements had been made as a result of the detailed inspection that took place in 2018.
77. The inspection team was once again made to feel welcome in Guernsey. We found Guernsey Law Enforcement, Social Security and Law Officers to be frank and helpful, both in the pre-briefing that they provided and in their responsiveness to our questions and requests for access.
78. Despite the difficulties inherent in policing relatively small communities, considerable successes have been achieved through the use of a variety of covert tactics. GLE and Social Security should feel confident in their appropriate use, and the people of Guernsey can be confident that these intrusive powers were used in 2018 lawfully and productively on their behalf.

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

21 June 2019