STATES OF JERSEY

REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 2005 AND POLICE PROCEDURES AND CRIMINAL EVIDENCE (JERSEY) LAW 2003: REPORT OF THE INVESTIGATORY POWERS COMMISSIONER 1ST JANUARY TO 31ST DECEMBER 2018

Presented to the States on 30th August 2019

STATES GREFFE

FOREWORD

In accordance with the requirement in Article 44(6) of the Regulation of Investigatory Powers (Jersey) Law 2005 and Article 104(4) of the Police Procedures and Criminal Evidence (Jersey) Law 2003, I am pleased to lay before the States the attached Annual Report for 2018 of the Commissioner appointed under those Laws.

Article 44(6) of the Regulation of Investigatory Powers (Jersey) Law 2005 requires the report to contain a statement indicating whether any matters have been omitted from it. Article 44(7) allows the Bailiff to exclude any matter from the report laid before the States if it appears to him, after consultation with the Commissioner, that the publication of any matter in an annual report would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of Jersey; or the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Commissioner. I am able to inform Members that, on the advice of the Commissioner, I have omitted the confidential Annex referred to in the report.

Article 104(4) of the Police Procedures and Criminal Evidence (Jersey) Law 2003 contains a similar provision, requiring the report laid before the States to contain a statement indicating whether any matters have been omitted from it. Article 104(5) allows the Bailiff to exclude any matter from the report laid before the States if it appears to him, after consultation with the Commissioner, that the publication of any matter in an annual report would be prejudicial to the security of the British Islands or to the detection of crime. I am similarly able to inform Members that, on the advice of the Commissioner, I have omitted the confidential Annex referred to in the report.

I would like to thank Lord Anderson of Ipswich, K.B.E., Q.C., for all his work as Investigatory Powers Commissioner in 2018.

BAILIFF OF JERSEY

REPORT

INTRODUCTION

1. The Investigatory Powers Commissioner **["the Commissioner"]** is a judge of the Jersey Court of Appeal, appointed by the Bailiff under Article 43 of the Regulation of Investigatory Powers (Jersey) Law 2005 **[the "2005 Law"]** and Article 104 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 **[the "2003 Law"]** to keep under review the exercise and performance of the powers and duties conferred and imposed under certain parts of those Laws.

2. The relevant powers and duties relate to the following investigatory techniques –

   (a) interception of communications (2005 Law, Articles 5–15 and 19);

   (b) acquisition and disclosure of communications data (2005 Law, Part 2, Chapter 2);

   (c) directed surveillance, intrusive surveillance and covert human intelligence sources **["CHIS"]** (2005 Law, Part 3);

   (d) interference with property (2003 Law, Part 11).

   The 2003 and 2005 Laws confer limited powers on specified persons to authorise the use of those techniques for stated purposes. They also regulate the use that can be made of material gained as a result.

3. The Commissioner is obliged to make an annual report to the Bailiff with respect to the carrying out of the Commissioner's functions (2005 Law, Article 44(4); 2003 Law, Article 104(3)). 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 States 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 –

   (a) contrary to the public interest; or

   (b) prejudicial to national security, the prevention or detection of serious crime, the economic well-being of Jersey, or the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Commissioner.[1]

4. 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.

[1] 2005 Law, Article 44(7). The grounds for exclusion are formulated slightly differently in the 2003 Law, Article 104(5).

THE POWERS UNDER REVIEW

5. Legal definitions of the powers under review are to be found in the relevant Laws and are not repeated here. But for the benefit of those without detailed expertise in these matters, I describe in this section what these powers mean in practice, and the nature of the constraints placed by the 2003 and 2005 Laws upon their exercise.[2]

Interception of communications (2005 Law, Part 2, Chapter 1)

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

7. The interception of such communications in the course of their transmission is normally a criminal offence in Jersey (2005 Law, Article 5), and it may also give rise to a civil action (Article 6).

8. Interception is, however, lawful when authorised by an interception warrant issued personally by H.M. Attorney General (Article 10). In the event of his or her absence, that function may be discharged by H.M. Solicitor General.[3] Warrants may be applied for by the Chief of Police, the Agent of the Impôts and the Chief Immigration Officer in Jersey, certain Heads of Security Services and the Armed Forces in the UK, and competent authorities of foreign states with which Jersey has a mutual assistance agreement (Article 11).

9. A warrant may only be issued if the Attorney General 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 Jersey, or to give effect to the provisions of international mutual assistance agreements (Article 10). The conduct authorised by the warrant must also be proportionate to what it is sought to achieve (Article 10(2)(b)).

10. Serious crime is defined, for the purposes of the 2005 Law, as offences which involve the use of violence, result in substantial financial gain, or are conducted 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 3 years or more (Article 1(1)). Detecting crime is defined in Article 1(2).

11. Detailed provision is made in the 2005 Law for the contents of warrants (Article 12), their duration, cancellation and renewal (Article 13), their modification (Article 14), and their implementation (Article 15). Safeguards for intercepted material are set out in Articles 19 and 20.

[2] The law of Jersey (in contrast to that of the UK and of Guernsey) contains no power for the issue of notices requiring the disclosure of the key to encrypted information, a power typically used, where it is available, to obtain passwords allowing access to electronic devices such as mobile phones.

[3] Departments of the Judiciary and the Legislature (Jersey) Law 1965, Article 5(1).

12. Disclosure of the issue of a warrant, the interception of a communication or the content of an intercepted communication (intercepted material or "intercept") are generally prohibited (Articles 21–23). 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 Jersey. This means that when intercept is sought in Jersey, 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.

13. The very limited circumstances in which interception is lawful without a warrant are set out in Article 8 of the 2005 Law.

Acquisition and disclosure of communications data (2005 Law, Part 2, Chapter 2)

14. 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 Part 2, Chapter 1 of the 2005 Law, the related communications data are also collected.

15. There is no power in Jersey 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.

16. The different types of communication data, defined in Article 24 of the 2005 Law, 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 e-mail 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).

17. 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 (Article 26(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"* (Article 26(2)(b)), not merely for the purpose of preventing or detecting *serious* crime (Article 10(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 (Article 26(2)(d)–(g)).

18. The range of public authorities permitted to access communications data is also wider than in the case of interception (Schedule 1). Authorisations on behalf of the Income Tax Department, Social Security Department, Parishes and intelligence services may be issued only by the Attorney General. Authorisations for communications data required for police, customs and immigration purposes are issued by the Chief Officer of Police, Agent of the Impôts and Chief Immigration Officer without any requirement for prior approval by Law Officers.

19. 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 (Article 26(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.

20. Provision is made in the 2005 Law for the form and duration of authorisations and notices (Article 27), and for the reimbursement in whole or in part of costs incurred by service providers in complying with notices (Article 28), and for powers of delegation in relation to the grant of authorisations and notices (Article 53).

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

Directed and intrusive surveillance (2005 Law, Part 3)

22. Surveillance is defined by the 2005 Law, Article 31 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 Part 3 of the 2005 Law, surveillance does not include the use of CHIS or warranted interception.

23. To be classed as ***intrusive surveillance***, it must be covert, and carried out in relation to anything taking place on any residential premises or in any private vehicle (Article 32(2)). Though it may involve the presence of an individual, it classically takes the form of a surveillance device: for example, a "bug" attached to a car, house or flat. 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 (Article 32(3)(a)).

24. Because of its capacity to intrude into the private spaces of vehicle and home, authorisations for intrusive surveillance may be granted only on the application of the same persons entitled to apply for interception, for the same limited purposes and on satisfaction of the same conditions as to necessity and proportionality. Intrusive surveillance requires a warrant from the Attorney General (Article 37).

25. Covert surveillance that is not intrusive but that is undertaken for the purposes of a specific investigation or operation, in such a matter as is likely to result in the obtaining of private information about a person, is known as ***directed surveillance*** (Article 32(1)). 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 previously known to law enforcement. Like other forms of surveillance, it may also help decide the most propitious moment to launch executive action.

26. 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 (Article 34(3)) and the range of public authorities permitted to authorise it (Schedule 2) is similarly wide. Directed surveillance required for police, customs and immigration purposes is authorised by the Chief Officer of Police, Agent of the Impôts and Chief Immigration Officer, or those to whom they have delegated the power pursuant to an Order made under Article 53(2), without any requirement for prior approval by Law Officers. The Attorney General is designated to authorise directed surveillance for other public authorities and, as in the case of communications data, may delegate that power under Article 53(1) to a Crown Advocate. The usual requirements of necessity and proportionality apply.

27. Rules for the grant, renewal, duration and cancellation of authorisations are in Articles 40 and 51 of the 2005 Law.

Covert human intelligence sources ("CHIS") (2005 Law, Part 3)

28. A person is deemed to be a CHIS if they establish or maintain a person or other relationship with a person for the covert purpose of obtaining information, or if they covertly disclose information obtained from such a relationship (2005 Law, Article 32(7)). CHIS may be paid for their work by the public authorities that use them.

29. The public authorities entitled to use CHIS are the same as those authorised to use directed surveillance (Schedule 2). The system for authorisation, and the range of grounds for which CHIS may be authorised, are also the same. Additional requirements are spelled out in Article 35. 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) Another officer (known as the controller) must oversee the use of the CHIS.

    (c) A record must be kept of such use.

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

Interference with property (2003 Law, Part 11)

30. Part 11 of the 2003 Law (under the misleading title "Control of Intrusive Surveillance") renders lawful "entry on or interference with property or with wireless telegraphy", if authorised by the Attorney General in accordance with the Law. The concept of interference with property is not closely defined. It includes, for example, the damage to the fabric of a dwelling that may be required to insert a surveillance device: with this in mind, Article 38 of the 2005 Law provides for the Attorney General to issue combined authorisations under Part 3 of the 2005 Law and Part 11 of the 2003 Law.

31. Property interference may be authorised only where the Attorney General believes that it is necessary for the purpose of preventing or detecting serious crime, or in the interests of the security of the Island, and that the taking of the action is proportionate to what it seeks to achieve (2003 Law, Article 101(2)).

32. In contrast to the powers governed by the 2005 Act, no list of public authorities entitled to seek authorisation for property interference appears in the 2003 Act. In practice, such authorisations are sought only by Jersey Police and by the Jersey Customs and Immigration Service.

Codes of Practice

33. Article 51 of the 2005 Law 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) (Jersey) Order 2006.

CONDUCT OF THE ANNUAL REVIEW

34. As stated at the start of this report, the conduct of the annual review is conferred by law upon a judge of the Jersey 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: 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 this was the Rt. Hon. Sir Adrian Fulford, a serving Judge of the Court of Appeal).

35. 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's Commissioner in person, but by specialised inspectors from IPCO.

36. 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.

37. 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 Jersey. Accordingly, and at my request, the Investigatory Powers Commissioner agreed to make available to me (without charge to the Government of Jersey, save as to travel and subsistence) the services of the IPCO inspectorate for each of my first 2 inspections, as follows –

(a) For my February 2018 inspection (reviewing the 2017 calendar year), I was accompanied by Clare Ringshaw-Dowle, an IPCO Chief Inspector specialising in intrusive and directed surveillance, CHIS and property interference.[4]

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

38. Each brought knowledge and understanding to the task of a specific kind 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 Jersey have profited enormously from their input, as they have made clear to me.

39. I should like to place on record my gratitude to IPCO and Sir Adrian Fulford for their generous assistance in lending me the assistance of these 2 Chief Inspectors in 2019. I am particularly grateful that Sir Adrian and the Chief Executive of IPCO, Amanda Jeffery, offered in June 2019 to continue supporting my inspections in the Channel Islands, through the services of "one or two inspectors with all the right skills and experience, who may include a Chief Inspector". I gladly accepted that offer: the lawful, safe and effective use of investigatory powers in Jersey can only benefit from this continued involvement.

[4] Mrs. Ringshaw-Dowle and Mr. Drummond were invited to Jersey pursuant to the 2005 Law (Article 43(5)), which allows the Commissioner to be provided with "staff".

SCOPE OF THIS REPORT

40. There is an obvious public interest in legislators, and indeed the people of Jersey, 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.

41. 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.[5]

42. 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 powers of which they have oversight have been granted during the review period.[6] I adopted that course in my first report for most of the powers under review, and do so again this year.

43. I am also conscious, however, that there are special factors in a small jurisdiction such as Jersey that make it difficult to disclose information as comprehensive as that which is released in the UK. To take 2 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 Jersey 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.

44. As in my first report, whose pattern this one follows, 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 Jersey, so as to avoid any risk of the use of powers in specific operations being identified. It should, however, be noted that each of the authorisations and warrants of which I was made aware was –

[5] See most recently IPCO, *Annual Report* – 2017, HC 1780, March 2019.
[6] 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.

(a) in support of the activities of Jersey Police or JCIS; and

(b) for the purpose of preventing or detecting crime.

45. Further detail is reserved to the confidential reports prepared by Clare Ringshaw-Dowle and Alex Drummond 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 good practice.

INTERCEPTION

46. A total of 39 warrants for interception were issued during 2018 (down from 57 in 2017), relating to the subjects of 11 investigations (down from 18 in 2017) managed by Jersey Police and/or JCIS. Overwhelmingly, these investigations concerned drug trafficking into Jersey and associated money laundering offences.

47. There were, in addition, 94 applications for communications data under intercept warrants. Such requests are made, in particular, to identify new numbers for warranted subjects or to identify associates involved in the operation through their links to warranted numbers. Forty-two 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.

48. In operations where interception was used, drugs were seized during 2018 to the value of £442,309 (2017 – £4,614,096). The majority of those drugs were cannabis, but substantial quantities of MDMA and heroin were also seized, together with other drugs. Cash was seized to a value of £1,000 (2017 – £156,801 + €579). Fourteen individuals (down from 25 in 2017) were charged as a result of such operations, including 2 for non-drug-related offences. A number of substantial prison sentences have already been imposed as a consequence of those charges, with other cases pending before the Royal Court or Magistrates' Court.

49 Under my supervision, Alex Drummond made a detailed examination of the records pertaining to 14 interception warrants, each 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.

50. That examination identified 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 interception was considered necessary and proportionate. We identified some areas in which further detail could have been beneficial, and others in which quality could be improved by a more succinct and focussed approach.

51. The integrity of the independent authorisation process was demonstrated by the fact that 2 warrant applications were refused by the Attorney General, in one case because the necessary serious crime threshold had not been reached, and in the other because of a specific issue relating to the context of the application. Good awareness was also shown of the risk of inadvertently obtaining legally privileged information.

52. Two errors were identified during the inspection relating to the interception of communications. One related to the loss of a warrant signed by the Attorney General, which appears to have been destroyed in error but which had already been copied, with the result that the detail of the conduct authorised remained available. Nonetheless, the administrative process has been improved to provide additional safeguards. The second error related to the interception of a wrong telephone number. The error was identified as soon as the interception was connected, and the interception immediately terminated. Additional corroboration checks have been introduced when attributing a telephone number for interception purposes, which should reduce the chance that such a human error will recur.

53. Some administrative issues were also identified, which may have been linked with the transition to a new joint interception suite and a merger of procedures. With a single operating model now in place, and additional checks and safeguards being introduced, the team had confidence that such issues will not occur in future.

54. Paragraph 6 of the Code of Practice sets out requirements for the disclosure, copying and retention of intercept material. Alex Drummond examined the arrangements in place and was satisfied that they complied with the applicable rules.

COMMUNICATIONS DATA

55. As in the UK, communications data requests were the most widely used of the investigatory powers in Jersey. During 2018 there were 162 applications for communications data other than under intercept warrants.[7] Four of those applications were rejected.

56. 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 not only for piecing together criminal networks and activities, but for supporting the alibis of innocent suspects and tracing, e.g. 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.

57. Accordingly, communications data was used during the period under review not only to target drug trafficking networks, but in support of investigations into a range of other crimes, as well as in a missing persons investigation.

[7] The 2017 figure given last year of 162 is not comparable, since it did not include 10 JCIS applications.

58. 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.

59. Under my supervision, Alex Drummond examined 24 records relating to applications and authorisations to obtain communications data, most of them relating to the prevention and detection of crime, and a smaller number relating to enquiries into the circumstances surrounding a person's death.

60. A good standard of application and authorisation was found, with sound reasoning in relation to necessity and proportionality resulting in communications data being obtained lawfully, for proper purposes and for appropriate periods of time tailored to the specific circumstances of the application. An opportunity to streamline the procedures applied by Jersey Police was also identified and communicated to them.

61. A total of 6 administrative errors were reported by Jersey Police and one by JCIS. Of these, 5 related to excess data being provided by the relevant CSP beyond the parameters of the authorisation. The other 2 errors related to data that was acquired on the wrong telephone number. All were attributable to human error, and none resulted in any serious impact or significant additional breach of privacy. To reduce the likelihood of further errors relating to the wrong telephone number, additional safeguards have been introduced, and advice as to process given.

INTRUSIVE SURVEILLANCE / PROPERTY INTERFERENCE

62. Six authorisations for intrusive surveillance and 16 for interference with property were granted in the period under review. Both figures were the same as in 2017. Two additional authorisations for property interference were applied for and refused.

63. Clare Ringshaw-Dowle, under my supervision, inspected the records for 2 intrusive surveillance authorisations and 5 property interference authorisations (including one urgent oral authorisation). Much good practice was observed, for example in the applications for both authorisation and cancellation completed by JCIS, the clarity of the forms to be completed by Law Officers and in relation to the prompt deletion of video footage that was no longer required. No significant criticisms were noted or recommendations made.

DIRECTED SURVEILLANCE

64. A total of 27 directed surveillance authorisations were granted in the period under review (down from 37 in 2017). One further application was refused. Seven of the authorisations were inspected by Clare Ringshaw-Dowle under my supervision, 2 from JCIS and 5 from Jersey Police. Some very good practice was observed, and no serious criticisms were noted. Advice was however given on completing applications and improving record-keeping.

COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

65. JCIS and Jersey Police now share a joint Source Management Unit for managing CHIS, which is in principle a positive development.

66. Clare Ringshaw-Dowle reviewed a number of CHIS records, and was appreciative both of the efforts being made by the relevant officers at a time of restructuring, and of the candour with which they discussed their responsibilities.

67. Resourcing constraints were, however, observed to be making it difficult to manage this area of business in accordance with the applicable rules and guidance, and the level of risk identified last year had not been mitigated. In view of these concerns, Clare Ringshaw-Dowle made a formal recommendation that the current resourcing and operational practices of the joint SMU be reviewed, to ensure that the integrity of its processes and the duty of care owed to any CHIS can in future be met in full.

CONCLUSION

68. The investigatory powers under review were, as a rule, exercised during the year under review in a compliant, proportionate and conscientious manner. To the extent that specific and continuing difficulties were observed, the detailed reports provided confidentially to the Bailiff contain the material necessary to achieve improvement. There are hardworking officers in Jersey Police and JCIS, keen to achieve good levels of compliance, and their approach to the inspection and to the feedback were encouraging.

69. Despite the difficulties inherent in policing relatively small communities, considerable successes in preventing and detecting crime have been achieved through the use of a variety of covert tactics.

70. I express my gratitude to Jersey Police and JCIS for the thorough and well-presented materials that were prepared, and for their candour and welcoming engagement with the inspection process.

Lord Anderson of Ipswich, K.B.E., Q.C.
14 August 2019