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 – 31ST DECEMBER 2021

Presented to the States on 5th July 2022

STATES GREFFE

REPORT

Introduction

1. The Regulation of Investigatory Powers (Jersey) Law 2005 ("RIPL") provides a comprehensive structure governing the use of certain law enforcement techniques. It is designed to ensure that the law enforcement techniques in question are regulated by law, operated in a proportionate manner, and, because of their largely clandestine nature, externally supervised. As part of the supervisory regime, Article 43 of RIPL provides that the Bailiff shall appoint one of the ordinary judges of the Court of Appeal as the Investigatory Powers Commissioner. The Commissioner is required to carry out certain supervisory functions and make an annual report to the Bailiff with respect to the carrying out of those functions.

2. In September 2020, I was appointed by the Bailiff as Investigatory Powers Commissioner in succession to Lord Anderson of Ipswich K.B.E. Q.C. who provided his third and final report, covering the calendar year 2019, in July 2020.

3. This is my second annual report. It covers the period January 2021 to December 2021, inclusive.[1]

4. Before turning to the particular activities regulated by RIPL, it is helpful to explain in brief outline my statutory role and responsibilities.

The Investigatory Powers Commissioner

5. Part 4 of RIPL (Articles 43 to 52) bears the heading "Scrutiny Etc of Investigatory Powers". As noted, Article 43 provides for the appointment of the Investigatory Powers Commissioner.[2] In broad terms, the Commissioner's role is to review the exercise and performance of the powers and duties conferred and imposed by RIPL, and to make an annual report to the Bailiff. The Commissioner may also at any time, make any such report to the Bailiff on any matter relating to the carrying out of the Commissioner's functions as the Commissioner thinks fit.[3]

6. As part of his functions, the Commissioner is required[4] to keep under review the exercise and performance of the powers and duties conferred or imposed by RIPL in relation to the following investigatory powers:

[1] My previous report, dated August 2021, was delayed as a consequence of the travel restrictions arising from the Covid-19 pandemic and covered the calendar year 2020. As explained in that report, I did take the opportunity to examine law enforcement activities up to and including June 2021. Thus, while this report is nominally for the calendar year, it covers some of the same ground.

[2] Part 4 also provides for the appointment of Assistant Investigatory Powers Commissioners (Article 45) and establishes a Tribunal which has jurisdiction to hear, consider and determine a variety of proceedings, complains and references arising as a result of the operation of RIPL (Article 46).

[3] Article 44(5).

[4] By reason of Article 43(2).

(i) the interception of communications under Chapter 1 of Part 2, Articles 4 to 23;

(ii) the acquisition and disclosure of communications data under Chapter 2 of Part 2, Articles 24 to 29;

(iii) the use of "directed surveillance", "intrusive surveillance" and "covert human intelligence sources" under Part 3, Articles 30 to 42;

(iv) the investigation of data protected by encryption under Part 3A.[5]

7. The Commissioner is also required to keep under review the adequacy of arrangements[6] for safeguarding warranted interception product by restricting its use to the minimum necessary for the "authorized purposes" (broadly speaking for intelligence gathering purposes or to facilitate the carrying out of the functions of the Commissioner or the Tribunal) which are identified in Article 19(4).

8. It is relevant to note that RIPL does not regulate entry on or interference with property or interference with wireless telegraphy. These activities are governed by the Police Procedures and Criminal Evidence (Jersey) Law 2003 ("PPCEL").[7] Article 103 of the PPCEL imposes a duty on the Attorney General to notify the Commissioner of authorisations in relation to property interference under Part II of that law (Articles 99 – 104).[8]

9. The Commissioner's annual report to the Bailiff with respect to the carrying out of the Commissioner's functions, is to be made as soon as practicable after the end of each calendar year.[9]

10. The Bailiff is required to cause a copy of the Commissioner's annual report to be laid before the States together with a statement as whether any matter has been excluded from that copy if it appears to the Bailiff after consultation with the Commissioner that publication of that matter would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious

[5] Part 3A of RIPL (Articles 42A- 42H) was inserted by the Cybercrime (Jersey) Law which came into force on 3 May 2019.
[6] Article 19(1) imposes a duty on the Attorney General to ensure that certain general safeguards are in place for intercepted material.
[7] Article 101.
[8] As in previous years, the Attorney General has provided notification in accordance with the statutory requirements imposed by Article 103 of PPCEL and also Article 39 of RIPL (notification of authorizations for intrusive surveillance).
[9] Article 44(4). The Commissioner may also at any time make such other report to the Bailiff or any matter relating to the carrying out of the Commissioner's functions as the Commissioner thinks fit: Article 44(5) of RIPL. The Commissioner is also required to make a report to the Bailiff if at any time there has been a contravention of the provision of RIPL in relation to any matter with which the Commissioner is concerned, or if at any time it appears that any arrangements by reference to which the duty imposed by Article 19 has sought to be discharged have proved inadequate in relation to any matter with which the Commissioner is concerned: Article 44(2) and (3).

crime,[10] 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.[11]

11. As will be apparent from this brief summary, the Commissioner's role is designed to provide oversight of the various public officials and public authorities who are authorised to use intrusive powers of investigation with a view to promoting best practice by those public officials within those public authorities and to enhance public confidence in the operation of the statutory scheme.

The Powers Under Review

12. RIPL is a detailed piece of legislation. It was enacted to provide a lawful basis for a broad range of intrusive investigative techniques including the interception of communications, access to communications data, surveillance (and associated activities) and the investigation of data protected by encryption.[12] For the purposes of this Report it is sufficient to provide a brief summary overview of the various powers under review.

Interception of Communications[13]

13. Chapter 1 of Part 2 of RIPL provides an intricate legislative scheme for the interception of communications in the course of their transmission by a public postal service, (for example, the opening of mail), or by a public or private telecommunication service (in simple terms, telephone tapping). In summary, RIPL makes it unlawful to intercept communications without proper authorization. It also creates a civil action where a communication in intercepted in the course of its transmission by means of a private telecommunication system. Lawful interception may be conducted in one or other of two ways. The first method is where it is authorized by or under Articles 8 or 9 (such as where the interception is consented to by the sender and intended recipient of the communication, or where the interception is by a postal or telecommunications service provider for purposes connected with the operation of that service). The second method is where the interception takes place in accordance with an interception warrant issued by the Attorney General under Article 10.[14]

[10] As defined in Article 1 of RIPL.
[11] Article 43(7).
[12] As noted, the power to investigate encrypted data is a recent innovation: Cybercrime (Jersey) Law 2019.
[13] Part 2, Chapter 1, Articles 4 to 23.
[14] Article 11(2) provides that an interception warrant shall not be issued except under the hand of the Attorney General. The Department of the Judiciary and the Legislature (Jersey) Law 1965 provides that in the event of the Attorney General's absence or incapacity his functions shall be discharged by the Solicitor General (Article 5). It also contains (Article 9(3)) a more general power of delegation: "Notwithstanding anything in any enactment, the Solicitor General, on the authority of the Attorney General, may discharge any function appertaining to the office of Attorney General."

14. Interception wan-ants may be applied for by only a limited number of individuals, as specified in Article 11(1).[15]

15. By reason of Article 10(2) an interception wan-ant may only be issued if the Attorney General believes that the wan-ant is necessary on grounds falling within Article 10(3). The Attorney General must also believe that the conduct authorized by the warrant is proportionate to what is sought to be achieved by that conduct. The grounds falling within Article 10(3) are: (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime;[16] (c) for the purpose of safeguarding the economic well-being of Jersey; or (d) for the purpose of giving effect to the provisions of any international mutual assistance agreement.[17] A factor which must be taken into account when deciding whether a warrant is necessary and proportionate is whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.[18]

16. Detailed provision is made for the contents of warrants,[19] their duration, cancellation and renewal,[20] their modification,[21] and their implementation.[22] General safeguards in relation to the dissemination, retention and disposal of intercepted material are set out in Articles 19 and 20.

17. Disclosure of the issue or existence of a warrant, the interception of a communication or the content of an intercepted communication (identifiable as such) is generally prohibited and may in certain circumstances amount to the commission of a criminal offence.[23] As in the United Kingdom and Guernsey, intercept product is inadmissible in criminal trials[24] and the purpose of the warranted intercept regime is to gather intelligence to prevent or detect serious crime and not directly to gather evidence for use in any legal proceedings.[25] The scheme is intended, among other things, to preserve the secrecy of the practical operation of the

[15] Most relevantly, the Chief Officer of the States of Jersey Police Force, the Agent of the Imp6ts (viz. the person appointed as such under Article 4 of the Custom and Excise (Jersey) Law 1991), the Chief Immigration Officer, and any person who, for the purposes of any international mutual assistance agreement (within the meaning of Article 5(4)) is the competent authority of a country or territory outside Jersey.
[16] For these purposes "serious crime" means conduct which constitutes one or more offences (a) which involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; and (b) for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for 3 years or more: see the interpretation provisions in Article 1.
[17] This concept is explained by Articles 4 and 5(4). The essential point is that there is a lawful basis upon which to assist the competent authorities of countries or territories outside Jersey who require assistance in the form of interception of communications.
[18] Article 10(4).
[19] Article 12.
[20] Article 13.
[21] Article 14.
[22] Article 15.
[23] Article 23.
[24] Article 21.
[25] This is apparent from the structure of Chapter 1 of Part 2 of RIPL and in particular by Article 1(2) (which defines "detecting crime") and 21 (which contains the general exclusion of matters from legal proceedings).

interception regime and to protect to the maximum extent possible the privacy of those whose conversation are overheard without their consent.

Acquisition and disclosure of communications data[26]

18. Chapter 2 of Part 2 of RIPL contains the legislative scheme for access to and handling of communications data, that is data about the use made of a telecommunication or postal service, excluding the contents of communications themselves, or contact with websites.[27] In relation to postal items, "data" means anything written on the outside of them. Communications data are sometimes described as the "who, how and where" of a communication. This includes subscriber information and call data held by communications service providers. A person who acquires or discloses communications data must be properly authorized and must act in accordance with that authority.

19. A test of necessity must be met before any communications data is obtained. The assessment of necessity is one made by a designated person. Designated persons are certain persons within specified public authorities which include the States of Jersey Police Force, the Immigration and Nationality Department and Customs and Excise.[28] Except where the Attorney General is the designated person, applications for communications data may only be made by persons in the same public authority as a designated person. A designated person must not only consider it necessary to obtain the communications data must also consider the conduct involved in obtaining the communications data to be proportionate to what it is sought to be achieved.[29]

20. The purposes for which communications data may be sought are considerably wider than in the case of interception. For example, communications data may be requested if it is necessary for the purpose of preventing or detecting crime or of preventing disorder (not merely for the purpose of preventing or detecting serious crime).[30] Data may additionally be requested in the interests of the economic well-being of Jersey[31] the interests of public safety or public health,[32] or for the purpose of accessing or collecting taxes,[33] or for the purpose, in an emergency, of preventing death or serious injury or any damage to a person's physical or mental

[26] Part 2 Chapter 2, Articles 24 to 29.
[27] The meaning of "communications data" is contained in Article 24. That is a person designated for the purposes of Chapter 2 of Part 2
[28] Articles 26 and 29 and Schedule 1. It follows that the range of public authorities and designated persons is wider than in the case of the warranted interception of communications.
[29] Article 26.
[30] Article 26(2)(b).
[31] The economic well-being of Jersey will only arise as a basis for an authorization if it is related to "national security": see the Regulation of Investigatory Powers (Code of Practice) (Jersey) Order 2006, Schedule 3, paragraph 4.2.
[32] Article 26(2)(d), (e).
[33] Article 26(2)(t).

health, or mitigating any injury or damage to a person's physical or mental health.[34]

21. Communications data may be obtained by using one or other of two routes. The first route is by the giving of notices to a postal or telecommunications operator requiring the operator to obtain and disclose the relevant data to the public authority which served the notice.[35] The second route by which data may be obtained is by an authorization which allows the public authority to collect or retrieve the data itself (where this is possible).[36] Provision is made for the form and duration of authorisations and notices.[37]

22. Communications data, unlike intercept product, are admissible in evidence in legal proceedings in Jersey and are frequently used in prosecutions of serious criminal offences.[38] Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and in accordance with data protection principles.

Surveillance and the Conduct and Use of Covert Human Intelligence Sources.[39]

23. Part 3 of RIPL applies to three kinds of covert activity, directed surveillance, intrusive surveillance and the conduct and use of covert human intelligence sources.

24. Surveillance is defined as including: "(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the assistance of a surveillance device".[40] It does not include certain activities specified in Article 31(2) or (3).[41]

Directed Surveillance

25. In order to amount to "directed surveillance", the surveillance must be covert, and not intrusive. Further, it must be undertaken for the purposes of a specific operation or investigation, in such manner as is likely to result in

[34] Article 26(2)(g).
[35] Article 26(4).
[36] Article 26(3).
[37] Article 27.
[38] See Articles 1(2) and 21 of RlPL which makes clear the distinction between intercept product and communications data.
[39] Part 3 Articles 30 - 42.
[40] Article 31.
[41] These activities include any conduct of a covert human intelligence source for obtaining or recording any information which is disclosed in the presence of the source, any entry or interference with property or wireless telegraphy as would be unlawful unless authorised under section 5 of the Intelligence Services Act 1994 or Article 101 of PCCEL. Nor does it include warranted interception.

the obtaining of private information about a person, and otherwise than by way of an immediate response to events.[42]

26. The criteria for the authorisation of directed surveillance by a person designated for this purpose is set out in Article 34. This incorporates the requirement of necessity and the principle of proportionality. In order for a designated person to grant authorization for directed surveillance the designated person must believe that the surveillance is necessary on the grounds set out in Article 34(3) which are virtually the same as those set out in Article 26(2) in relation to the obtaining at disclosure of communications data.[43]

27. The range of public authorities permitted to authorize directed surveillance though individual officers or positions specified by regulations is relatively broad and includes, for example, the Jersey Financial Services Commission.[44]

Intrusive Surveillance

28. In order to amount to "intrusive surveillance", the surveillance must be covert and must be carried out in relation to anything taking place on any residential premises[45] or on any private vehicle,[46] and involve the presence of an individual or the premises or in the vehicle, or be carried out by means of a surveillance device.[47]

29. Thus, while intrusive surveillance may involve the presence of an individual, in its classic form it involves the use of a listening device placed in a private vehicle or dwelling.[48]

30. Because of its potentially intrusive character authorizations for intrusive surveillance may only be granted by the Attorney General where he believes it is necessary on certain limited grounds and that the authorized surveillance is proportionate to what is sought to be achieved by carrying it out.[49] The grounds are similar to those governing the interception of

[42] Article 32(1) of RIPL. A classic form of directed surveillance is static, foot or mobile surveillance in the street whereby surveillance teams follow targets covertly to obtain information about what they are doing.
[43] Article 26(2)(g) (for the purpose, in an emergency, of preventing death or injury, or any damage to a person's physical or mental health) has no equivalent in Article 34(3).
[44] Article 36 and Schedule 2, although the Attorney General is the designated person for the public authorities other than the Islands Police Force, Customs and Excise, and the Immigration and Nationality Department.
[45] This includes hotel rooms, bedrooms in barracks, and police and prison cells: Article 30(1).
[46] A private vehicle is any vehicle which is used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it: Article 30(1).
[47] If the surveillance involves entry on or interference with property, or with wireless telegraphy, it will be governed by the authorizations procedures under the 1994 Act or the Police Procedures and Criminal Evidence (Jersey) Law 2003. Applications can only be made to and granted by the Attorney General on an application by an official listed in Article 101(1A) PPCE.
[48] Although surveillance carried out by a device designated or adapted principally for the purpose of providing information about the location of a vehicle is not intrusive: Article 32(3).
[49] Article 37(2).

communication: (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; or (c) in the interests of the economic well-being of Jersey.[50] A factor which must be taken into account in deciding whether an authorization is necessary and proportionate is whether the information which it is thought necessary to obtain by means of the intrusive surveillance could reasonably be obtained by other less intrusive means.[51]

31. Authorizations for intrusive surveillance may be sought by only a limited number of individuals (the officers listed in Article 37(1) or by a member or official to whom Article 37(7) applies), and most relevantly for present purposes, these include the Chief Officer of the States of Jersey Police Force, the Agent of the Impots and the Chief Immigration Officer.[52]

32. General rules in relation to the grant, renewal and duration of directed and intrusive surveillance authorizations are to be found in Article 40 of RIPL.[53] As a general rule a written authorization will cease to have effect (unless renewed) at the end of a period of 3 months beginning with the day in which it took effect.

Covert Human Intelligence Sources

33. A covert human intelligence source ("CRIS") is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of obtaining information, or if they covertly disclose information obtained from such a relationship.[54] An essential feature of the definition is that the person (who may be a law enforcement officer or a civilian) acts covertly. This does not include the situation where a member of the public comes forward with information about a crime as part of their normal civic duties, but it does include an informant (or police officer) who cultivates a relationship with another for the purpose of supplying (or obtaining) information about that person to the police or other law enforcement authorities.

34. The public authorities entitled to use CRIS are the same as those authorized to use directed surveillance.[55] The system for authorization, and the range of grounds for which CRIS may be authorizes are also the same.[56] Additional requirements are also identified,[57] in particular:

[50] Article 37(3) (there is no equivalent of Article 10(2)(d)(giving effect to the provisions of any international mutual assistance agreement).
[51] Article 37(5).
[52] Article 37(1).
[53] Article 40 who deals with other authorizations under Part 3.
[54] Article 32(7).
[55] Article 36.
[56] Article 35(3).
[57] Article 35(5).

(i) an officer (known as the handler) must have day-to-day responsibility for contact with the CHIS and for his or her welfare;[58]

(ii) a different officer (known as the controller) must oversee the use of the CRIS;[59]

(iii) records must be kept of the use made of the CRIS (and other specified matters);

(iv) the CHIS's identity must be protected.[60]

35. The public authorities entitled to authorize the use and conduct of a source are those listed in Schedule 1 to RIPL. Responsibility for authorizing the use or conduct of a source rests with the authorising officer. An authorising officer is a person designated under Article 36. Durations and renewals of authorizations are governed by Article 40. As a general rule a written authorization will, unless renewed, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect.

Interference with Property

36. The control of entry on or interference with property or with wireless telegraphy is governed by provisions contained in Part 11 of the PPCEL.[61] In many cases a covert surveillance operation may involve both intrusive surveillance and entry on or interference with property or with wireless telegraphy. This can be achieved by way of combined authorization, although the criteria for the authorization of each activity must be considered separately.

37. PPCEL Article 100 provides that no entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorized by an authorization having effect under Part 11. The grant of authorizations is governed by Article 101 which provides that the Attorney General may authorize interference with property or the taking of action in respect of wireless telegraphy where he believes it is necessary for the purpose of preventing or detecting serious crime[62] or in the interests of the security of the Island and that the taking of the action is proportionate to what the action seeks to achieve.[63]

[58] Article 35(5)(a).
[59] Article 35(5)(b).
[60] Article 35(5)(c).
[61] Articles 99- 104.
[62] As defined in Article 101(4) of PPCEL.
[63] The Attorney General is required to consider whether what it is thought necessary to be achieved by the authorized conduct could reasonably be achieved by other means: Article 101(3) of PPCEL.

38. Article 102 contains provisions which govern the form and duration of authorizations.[64] Written authorization will cease to have effect at the end of a period of 3 months beginning with the day on which they took effect.

39. Article 103 places a duty on the Attorney General to notify the Commissioner of authorizations given, renewed or cancelled, at least every 12 months, in accordance with arrangements made by the Commissioner.[65]

Investigation of data protected by encryption

40. The Cybercrime (Jersey) Law 2019 which came into force on 3 May 2019 amends RIPL by inserting a new Part 3A (Articles 42A - 42H). These provisions allow for the issue of notices requiring the disclosure of the key to encrypted information that is lawfully within the possession of the authorities.[66] The power is most often used to obtain passwords allowing access to electronic devices such as mobile telephones and computers. A disclosure notice may be given by a person permitted under Schedule 2A who believes on reasonable grounds that it is necessary in the interests of national security or for the purpose of preventing or detecting crime, or in the interests of the economic well-being of Jersey, or where it is necessary for the purpose of securing the effective exercise or proper performance by any public authority or any statutory power or statutory duty.[67]

41. Failure to comply with a notice issued under Article 42B 1s a criminal offence, punishable by up to five years' imprisonment and/or a fine.[68]

Codes of Practice and Guidance

42. Article 51 of RIPL makes provision for the making of codes of practice relating to the exercise and performance of powers and duties that are conferred or imposed by RIPL and those conferred or imposed under the PPCEL. While a failure on the part of any person to comply with any provision of a code of practice shall note itself render that person liable to any criminal or civil proceedings. The codes of practice are admissible as evidence in criminal and civil proceedings, and, where relevant, the provisions of the codes must be taken into account by a court of tribunal.

43. There are five Codes of Practice which were brought into force by the Regulation of Investigatory Powers (Codes of Practice) (Jersey) Order 2006.These Codes of Practice address:

    (i) the interception of communications;

[64] The Attorney General is required to cancel an authorization if the action authorized if the action authorized by it is no longer necessary.
[65] The Attorney General has again complied with his duty under section 103.
[66] Article 42B.
[67] Article 42B(2), (3).
[68] Article 42F.

(ii) the interception of communications (postal);

(iii) accessing communications data;

(iv) covert surveillance (including interference with property or with wireless telegraphy);

(v) covert human intelligence sources.

44. The Codes of Practice provide general guidance (in plain language) on the procedures that must be followed before any of the intrusive investigation techniques can take place. They are primarily intended for use by the various public officials who authorize or use the measures in question although they will also prove useful to anyone interested in the operation of the legislative scheme and the procedures followed by public officials. The Codes are intended to be a readily available to any members of those public authorities involved in operations under RIPL or PPCEL.

General Observations on the Statutory Scheme

45. The detailed provisions of RIPL and the PCCEL, as supplemented by the Codes of Practice, are intended to provide a comprehensive framework for the regulation of surveillance and other forms of intrusive law enforcement activities. This is in the interests not only of the public officials, who are required to follow the procedures set out in the statute, it also serves the public interest by respecting the principle of legality. While, the need for surveillance is undeniable, so too is the need for it to be regulated in such a way to ensure that the privacy of those who are the target or surveillance is infringed only where it is lawful to do so and where the tests of necessity and proportionality are satisfied.

46. Proportionality is a crucial concept in both the legislation and the Codes of Practice. This means that even where an interference with an individual's Convention rights[69] is directed at pursuing a legitimate aim, this will not in itself justify the interference if the means used to achieve it are excessive in the circumstances. Any interference with a Convention right must be carefully designed to meet the objective in question and must not be arbitrary or unfair.

47. The statutory provisions and codes of practice have drawn heavily on the United Kingdom's Regulation of Investigatory Powers Act 2000 and associated Codes of Practice.[70] The 2000 Act remains the governing statute in the United Kingdom for directed and intrusive surveillance and the use and conduct of CHIS. In the case of the interception of communications and

[69] That is the rights within the meaning of the Human Rights (Jersey) Law 2000. Such as the right to privacy as guaranteed by Article 8 of the European Convention on Human Rights.
[70] Made under section 71 of the 2000 Act.

the acquisition and disclosure of communications data, the 2000 Act has been replaced by the Investigatory Powers Act 2016 and new codes of practice have been produced on the exercise of these specific powers. Those codes have much in common with the earlier codes of practice, but they also reflect a number of significant statutory changes. The most notable of which relates to the acquisition of communications data where a new independent Office for Communications Data Authorizations ("OCDA") was established from March 2019.[71]

Conduct of the Review

48. As with the case of my first inspection, and a result of a practice initiated by my predecessor, Lord Anderson of Ipswich K.B.E. Q.C., I have been greatly assisted in the conduct of my review by specialised inspectors from the Investigatory Powers Commissioner's Office ("IPCO"). As in previous years, the United Kingdom's Investigatory Powers Commissioner, the Rt Hon Sir Brian Leveson, 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, and, in particular, the services of Mr Stephen Matthews and Mr Paul Gration, both IPCO Inspectors.[72] Mr Matthews has expertise in, among other matters, the interception of communications and the acquisition and disclosure of communications data. Mr Gration has expertise in, among other matters, all areas of surveillance and the conduct and use of covert human intelligence sources.

49. As with my previous report, I wish to place on record my gratitude to Sir Brian Leveson and all those at the IPCO who provided support and assistance to the inspection process. Mr Matthews and Mr Gration brought to the inspection process a knowledge and understanding that no Commissioner, no matter how senior or experienced, could be expected to possess. I have again benefitted enormously from their expertise and practical knowledge. Their recommendations and guidance drawn from years of experience and a thorough appreciation of current best practice in the United Kingdom, were made in both oral briefings to relevant personnel and in confidential reports which are submitted to the Bailiff together with this report. I am again confident that the supervision and management of investigatory powers in Jersey have benefitted significantly from their involvement in the inspection process. I wish to record also my gratitude to

[71] OCDA was established by The Data Retention and Acquisition Regulations 2018 (No. 1123) following the decision of the Court of Justice of the European Union in the joined cases of Tele2 Sverige AB v Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Watson (C-698/15). Following the Court's judgment the UK Government accepted that amendments were needed to the Investigatory Powers Act to make it consistent with EU law, in particular to provide for independent authorisation for most communications data applications. As a result, OCDA was established to consider nearly all communications data applications made by public authorities in the UK, other than the intelligence agencies, on behalf of the Investigatory Powers Commissioner. In Jersey, applications are channelled through single points of contact within each public authority and these single points of contact are in a position to advise a designated person on whether an authorization is appropriate.

[72] Both of whom assisted with the previous inspection carried out in July 2021.

the Bailiff who has welcomed this arrangement and repeat my sincere hope that the arrangement will continue in the future.

50. The inspection visit took place between 21 March and 23 March 2022 when I visited Jersey with the assistance of Mr Matthews and Mr Gration.[73]

Briefings

51. In the course of the inspection, and in keeping with the practice established by my predecessors, the inspectors and I received detailed, classified written accounts of the use of each of the relevant powers by Jersey Law Enforcement authorities. The inspection team was also provided with the opportunity to inspect files showing the procedures that were followed by the authorities when using the powers granted by RIPL (and PPCEL). I was also able to discuss the operation of the legislative scheme with the Deputy Chief Officer of the States of Jersey Police and the Jersey Customs and Immigration Service Head of Service, as well as the Law Officers.

52. I am grateful to all those who assisted in the work of the inspection process and the great efforts that were taken to ensure that I was provided with all the necessary information and support to conduct a thorough review and produce this Report.

Scope of this Report

53. In keeping with observations made by my predecessors, I recognise the tension between the public interest that lies in transparency and the need to avoid any risk of undermining the effective use of the various surveillance powers in ongoing or future operations. In balancing these competing interests I have been guided by the approach adopted in previous Reports.

54. Without disclosing the details of specific operations, it is to be noted that the overwhelming majority of authorisations requested and granted were in support of the law enforcement activities conducted for the purpose of preventing or detecting serious crime, largely, but not solely, arising from large scale, commercial drug trafficking.[74]

55. Further detail is contained in the confidential reports prepared by the IPCO Inspectors under my supervision. Those reports have been provided to the Bailiff as confidential appendices to this report, and may, at the Bailiffs discretion, be provided to those who apply for and authorize investigatory powers, so as to assist with training and the continuing pursuit of best practice.

[73] Their familiarity with the legislation, codes of practice and the process of inspection greatly assisted the efficiency of the inspection process. They remained in Jersey until 25 March 2022.
[74] The powers were also used in investigations into other offences such as money laundering, financial crime and for purposes connected with the protection of vulnerable minors.

56. The use of RIPL powers by other Jersey public authorities was also the subject of scrutiny and in particular directed surveillance operations carried out by the department now known as Infrastructure, Housing and Environment.

The Period Under Review

57. It is to be noted that while Article 44 of RIPL envisages annual reports by the Commissioner to the Bailiff. This report covers the calendar year 2921 although my previous inspection considered authorizations up to and including June 2021. This reflects the difficulties caused to the inspection process by the COVID-19 virus. It is to be hoped that next year's inspection will see a return to normal reporting practice.

58. In 2020 and 2021, Jersey, like the rest of the world, was severely affected by the COVID-19 virus. Despite the difficulties caused by the pandemic, law enforcement activities have continued and the powers available under RIPL and PPCEL have been used lawfully and to good effect in detecting and deterring crime. A number of intelligence led law enforcement operations resulted in the seizure of in excess of £300,000 worth of drugs and a number of arrests (largely in connection with drug trafficking).

Interception

59. The previous inspection took place between 13 and 14 July 2021 with no areas of non-compliance identified. In the course of the most recent inspection a random sample of warrants of interception (some 6 in total) and applications for communications data (some 54 in total) were examined and assessed for their compliance with the provisions in RIPL and the relevant Codes of Practice.

Warranted Interception

60. In the calendar year 2021, there were a total of 14 interception warrants. The documentation was of a good standard and the requirements of the legislation and the Code of Practice had been properly observed. Each of the warrants had been granted for the statutory purpose of preventing or detecting serious crime (principally drug trafficking) and the applications contained a good explanation of the justification for the interception and an explanation of why the proposed activity was considered necessary and proportionate. Cancellations were timely and the law enforcement officers involved in gathering intelligence demonstrated an appropriate awareness of their responsibilities.

General safeguards for Intercepted Material

61. Article 19(2) of RIPL imposes a duty on the Attorney General to ensure that arrangements are in place for securing that the disclosure and distribution of intercepted material is kept to the minimum necessary for the "authorized purposes."[75] The inspection revealed that appropriate safeguards are in place and that the requirements of Article 19 are satisfied.

Communications Data

62. There were 108 applications to acquire communications data for evidential purposes in a wide-range of suspected offending. Fifty-four of these written applications were examined. In the course of the inspection the applications were found to be well-crafted with proper consideration being given to the requirements of necessity and proportionality. It is apparent that applicants and authorizing officers take their responsibilities seriously. It is also the case that the powers are being exercised lawfully and for the correct statutory purposes.

63. Overall the inspection found that the requirements of RIPL and the Code of Practice in relation to warranted interception and communications data are being observed and a good level of compliance is being achieved.

Property Interference and Intrusive Surveillance

64. In 2021, there were a total of 14 authorizations for property interference and 7 authorizations for intrusive surveillance in 10 operations concerned with the investigation of drug trafficking. These powers were exercised lawfully and for the correct statutory purposes.

65. Schedule 2 of RIPL lists those public authorities with power to conduct directed surveillance. The list includes the Environment and Public Services Department, now known as Infrastructure, Housing and Environment. In 2021, Infrastructure, Housing and Environment carried out two directed surveillance operations in connection with pollution control. These operations were reviewed during the inspection process and found to be in compliance with the requirements of RIPL.

Directed surveillance

66. In 2021, there were a total of 8 directed surveillance operations (in the period from July to December inclusive). The majority of them related to drug trafficking offences. These powers were also exercised lawfully and for correct statutory purposes.

[75] The authorized purposes are set out in Article 19(4).

Covert Human Intelligence Sources (CHIS)

67. During the period under review Jersey Law Enforcement used the services of registered CHIS.

68. In previous years a number of recommendations have been made in relation to the application for and authorizations and management of CHIS. Mr Oration has made a number of important recommendations as a result of our most recent inspection. These recommendations and the reasons for them are explained in the confidential report prepared by Mr Oration and provided to the Bailiff. It should be emphasised that the recommendations are principally directed at standards of record keeping and the need to ensure that the structure and management of CHIS are properly resourced and supported by an appropriately secure covert structure. I fully support Mr Oration's recommendations and intend to keep these issues under review during the inspection in 2023.

Investigation of Data Protected by Encryption

69. This is a relatively recent power. There have been eight notices issued in 2021, each of which was served in relation to suspected related offences of drug trafficking. The ability to serve notices is an important addition to the powers available to Jersey law enforcement and it has been used with appropriate consideration for the requirements of the statutory scheme. The scheme appears to be working well.

Notification of errors

70. There were no recordable errors in relation to the acquisition of communications data in the period under review.

Conclusion

71. In the course of my inspection I was provided with all necessary assistance and the public officials who facilitated the process were without exception courteous, well- informed and generous with their time. They were responsive to requests for information and receptive to suggestions for how their practices might be improved in the future.

72. As with my previous visit, the inspection process revealed that the powers in RIPL and PPCEL are being exercised lawfully in pursuit of legitimate and proportionate objectives. Applications for authorizations are well drafted and give proper consideration to the purposes of the legislation and the principle of legality. It is a reflection of the hard work of the States of Jersey Police and the Jersey Customs & Immigration Service that no areas

of non-compliance were identified. There are however improvements to be made in relation to the management of CHIS. The operations carried out by Infrastructure, Housing and Environment showed an impressive level of compliance with the legislative scheme.

73. The overall conclusion of this, my second report as Commissioner, is that the statutory investigatory powers are being used lawfully for legitimate purposes in the public interest.

David Perry Q.C.
April 2022