
STATES OF JERSEY



THE REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 2005 AND POLICE PROCEDURES AND CRIMINAL EVIDENCE (JERSEY) LAW 2003: REPORT OF THE INVESTIGATORY POWERS COMMISSIONER FOR THE PERIOD 1 JANUARY TO 31 DECEMBER 2024

Presented to the States on 17th March 2026

STATES GREFFE

**THE REGULATION OF INVESTIGATORY POWERS (JERSEY) LAW 2005 AND POLICE
PROCEDURES AND CRIMINAL EVIDENCE (JERSEY) LAW 2003**

**REPORT OF THE INVESTIGATORY POWERS COMMISSIONER FOR THE PERIOD 1
JANUARY TO 31 DECEMBER 2024**

RT HON JAMES WOLFFE KC FRSE

NOVEMBER 2025

Introduction

1. The Regulation of Investigatory Powers (Jersey) Law 2005 (“RIPL”) and Part 11 of the Police Procedures and Criminal Evidence (Jersey) Law 2003 (“PPCEL”) set out a legal framework governing the use of certain law enforcement techniques, such as the interception of communications and surveillance. The statutory framework is designed to ensure that the use of particular surveillance techniques is regulated by law and is externally supervised.
2. As part of the supervisory regime, Article 43 of RIPL provides that the Bailiff shall appoint as Investigatory Powers Commissioner a judge of the Court of Appeal to carry out certain supervisory functions and to make an annual report with respect to the carrying out of those functions. Article 104 makes corresponding provision for the appointment of a Commissioner under that Law.
3. The Bailiff appointed me as Investigatory Powers Commissioner in 2023. This is my second annual report. It covers the calendar year 2024. The overall conclusion of this report is that the investigatory powers which I describe below were used lawfully and proportionately and continue to make an important contribution to the detection and prevention of crime in Jersey.

The Investigatory Powers Commissioner

4. Part 4 of RIPL (sections 43 to 52) is headed “Scrutiny Etc of Investigatory Powers”. This provides for the appointment by the Bailiff of the Investigatory Powers Commissioner. The Commissioner’s functions are, broadly, to keep under review the exercise and performance of the powers and duties conferred by RIPL and to make an annual report to the Bailiff.
5. As part of the functions of the office, the Commissioner is required to keep under review the powers and duties conferred or imposed in relation to the following investigatory powers:
 - (i) the interception of communications under Chapter 1 of Part 2 of RIPL (Articles 4 to 23);
 - (ii) the acquisition and disclosure of communications data under Chapter 2 of Part 2 of RIPL (Articles 24 to 29);
 - (iii) the use of ‘directed surveillance’, ‘intrusive surveillance’, ‘covert human intelligence sources’ and ‘interference with property under Part 3 of RIPL (Articles 30 to 42); and
 - (iv) the investigation of data protected by encryption under Part 3A of RIPL (Articles 42A to 42H).
6. The Commissioner is also required to keep under review the adequacy of arrangements for safeguarding warranted interception product by restricting its use to the minimum necessary for the “authorised purposes” identified in Article 19(4) of RIPL.
7. RIPL does not regulate entry on or interference with property or interference with wireless telegraphy. These activities are governed by Part 11 of PPCEL (Articles 99 to 104). Article 104 provides for the appointment of a Commissioner to keep under review the carrying out by the Attorney General of the Attorney General’s functions under Part 11 PPCEL and to make an annual report to the Bailiff.
8. 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 to whether any matter has been excluded from it.

9. As will be apparent from this brief summary, the Commissioner's role is designed to provide external oversight of the various public office-holders and public authorities who are authorised to use intrusive (and for the most part clandestine) investigatory powers. This oversight enables the Commissioner both to scrutinise the compliance of those officials and authorities with the requirements of the legislation and to seek to promote best practice in relation to the use of those powers. The reporting requirements are designed to enhance public confidence in the operation of the statutory scheme.

The powers under review

10. It will assist the reader if I provide a brief summary of the investigatory techniques which I am charged with keeping under review.

Interception of communications

11. Chapter I of Part 2 of RIPL regulates the interception of communications in the course of their transmission by a public postal service (opening of mail) or by a public or private telecommunications provider (telephone tapping).
12. In broad terms, RIPL makes it unlawful to intercept such communications without proper authorisation. Lawful interception may be conducted in one of two ways: where it is authorised under Article 8 or 9 of RIPL (for example where the sender and intended recipient both consent) or where it takes place in accordance with an interception warrant issued by the Attorney General under Article 10 of RIPL.
13. The Attorney General may not issue an interception warrant unless he believes: (a) that the warrant is necessary on grounds falling within Article 10(3) of RIPL; and (b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. The grounds specified in Article 10(3) are: (a) the interests of national security; (b) the purpose of preventing or detecting serious crime; (c) the purpose of safeguarding the economic well-being of Jersey; and (d) the purpose of giving effect to an international mutual assistance agreement (in circumstances equivalent to those covered by the provision relating to the prevention or detection of serious crime). A factor which must be taken into account when considering whether these requirements are satisfied is

whether the information which it is thought necessary to obtain under the warrant could be obtained by other means.

14. RIPL makes detailed provision for the content of warrants, their duration, cancellation and renewal, their modification and their implementation. Articles 19 and 20 contain general safeguards in relation to the dissemination, retention and disposal of intercepted material. In particular Article 19 imposes a duty on the Attorney General to ensure that such arrangements are in force as he considers necessary for securing that the dissemination of intercepted material is limited to the minimum necessary for the authorised purposes and that any copy of intercepted material is destroyed as soon as there are no longer grounds for retaining it as necessary for any of the authorised purposes.
15. Disclosure of the existence of a warrant, the interception of a communication or the content of an intercepted communication (identifiable as such) is generally prohibited. As in the UK and Guernsey, intercepted material is inadmissible in criminal trials. The purpose of the warranted intercept regime is, accordingly, broadly to gather intelligence for the statutory purposes, and not to gather evidence for use in legal proceedings. The scheme is intended, among other things, to preserve the secrecy of the practical operation of the interception regime and to protect so far as possible the privacy of those whose communications are intercepted without their consent.

Acquisition and disclosure of communications data

16. Chapter 2 of Part 2 of RIPL contains the legal provisions governing access to and handling of communications data – that is data about the use made of a telecommunications or postal service, excluding the contents of the communications themselves. They are sometimes described as the “who, how, when and where” of a communication. They include subscriber information and call data held by a communication service provider.
17. The acquisition or disclosure of communications data is lawful if it is properly authorised under RIPL and is in accordance with that authorisation. RIPL gives powers to certain designated persons to grant an authorisation. The designated persons are (depending on the authority which seeks to exercise the powers under Chapter 2) the Chief Officer of the States of Jersey Police Force, the Agent of the Impôts, the Chief Immigration Officer and the Attorney General.

18. The powers under Chapter 2 of Part 2 apply only where a designated person believes that their exercise is necessary on one of the grounds specified in Article 26(2) of RIPL. These are wider than the grounds which apply to interception warrants, and including the purpose of preventing or detecting crime (not only serious crime) or of preventing disorder, protecting public health, assessing or collecting taxes, preventing (in an emergency) death or injury or any damage to a person's physical or mental health or mitigating any injury to a person's physical or mental health, as well as the interests of national security and the economic well-being of Jersey.
19. Chapter 2 of Part 2 of RIPL permits communications to be obtained by one of two routes. The first is by giving notice to the postal or telecommunications operator requiring the latter to obtain and disclose information to the public authority. The second is by an authorisation permitting the public authority to collect or retrieve the data itself. The legislation provides for the form of authorisations and notices. Although not specifically provided for in the legislation, communications data must be handled and stored securely and in accordance with data protection principles.
20. Communications data, unlike intercept product, are admissible in legal proceedings and are often used in the prosecution of serious criminal offences.

Surveillance and Covert Human Intelligence Sources

21. Part 3 of RIPL contains provisions regulating three kinds of covert activity: directed surveillance; intrusive surveillance; and the conduct and use of covert human intelligence sources ("CHIS").
22. For these purposes, surveillance is defined in Article 31 of RIPL to include: "(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". It does not include certain excluded activities.

Directed surveillance

23. In order to amount to directed surveillance, the surveillance must be covert but not intrusive. Further, it must be undertaken for the purposes of a specific operation or investigation and in such manner as is likely to result in the obtaining of private information about a person, and otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for authorisation to be sought. This would cover, for example, static, foot or mobile surveillance in the street, whereby a surveillance team follows a target covertly to obtain information about what they are doing.
24. Article 34 identifies designated persons who have the power to grant authorisation for directed surveillance. These include (depending on the public authority which is to undertake the surveillance) the Chief Officer of the States of Jersey Police Force, the Agent of the Impôts, the Chief Immigration Officer and the Attorney General. A designated person may not authorise directed surveillance unless that person believes that the surveillance is necessary on one of a number of specified grounds and that it is proportionate to what is sought to be achieved. The grounds are effectively the same as those which may justify the disclosure of communications data, with the exception of the purpose of preventing death or injury or danger to a person's physical or mental health.
25. The legislation sets out general rules for the grant, renewal and duration of directed surveillance authorisations. As a general rule, a written authorisation ceases to have effect, unless renewed, at the end of a period of three months beginning on the day on which it took effect.

Intrusive Surveillance

26. In order to be intrusive surveillance, the surveillance must be covert and must, subject to certain qualifications, be carried out in relation to anything taking place on residential premises or in a private vehicle, and involve the presence of an individual on the premises or in the vehicle, or be carried out by means of a surveillance device. Intrusive surveillance might, for example, involve the use of a listening device placed in residential premises or a vehicle.
27. Because of its potentially intrusive character, authorisation for intrusive surveillance may be granted only by the Attorney General. Only certain public

authorities may seek authorisation. These include the Chief Officer of the Island Police Force, the Agent of the Impôts and the Chief Immigration Officer. The Attorney General may not grant an authorisation unless he believes that the intrusive surveillance is necessary on one of certain limited grounds and that it is proportionate to what is sought to be achieved. The grounds are: (a) the interests of national security; (b) the purpose of preventing or detecting serious crime; or (c) the interests of the economic well-being of Jersey. A factor that must be taken into account in deciding whether an authorisation is necessary and proportionate is whether the information could reasonably be obtained by other less intrusive means. Authorisation for intrusive surveillance may be sought by police and customs officers.

28. RIPL contains rules in relation to the grant, renewal and duration of authorisations. As a general rule, a written authorisation ceases to have effect, unless renewed, at the end of a period of three months beginning on the day on which it took effect.

Covert Human Intelligence Sources ("CHIS")

29. A CHIS is a person who: (a) establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the obtaining of information or the provision of access to information; (b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or (c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. An essential feature of the definition is that the person acts covertly. The legislation does not apply where a member of the public comes forward with information about a crime, but does include an informant or police officer who cultivates a relationship with another person for the purposes of supplying or obtaining information about that person to the police or other law enforcement authorities.
30. The public authorities which may use a CHIS, in terms of RIPL, are the same as those which may use directed surveillance. The system for authorisation, and the range of grounds for which a CHIS may be authorised, are also the same. There are, though, additional requirements. In particular:
- (i) an officer, known as a handler, must have day to day responsibility for contact with the CHIS and for his or her welfare;

- (ii) a different officer (known as a controller) must oversee the use of the CHIS;
- (iii) records must be kept of the use made of the CHIS and other specified matters;
- (iv) the CHIS' identity must be protected.

31. RIPL contains provisions regulating the duration and renewal of authorisations and identifies the persons who are entitled to grant authorisations for the use of CHIS. As a general rule, a written authorisation ceases to have effect, unless renewed, at the end of a period of twelve months beginning on the day on which it took effect.

Interference with Property

32. Entry on or interference with property or wireless telegraphy is governed by Part 11 of PPCEL. PPCEL provides that no interference with property or with wireless telegraphy shall be unlawful if it is unauthorised by an authorisation having effect under Part 11. Article 101 provides that the Attorney General may authorise interference with property or with wireless telegraphy where he believes that this 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 the action seeks to achieve.

33. The legislation contains provisions dealing with the form and duration of authorisations. Written authorisations generally cease to have effect at the end of a period of three months beginning with the day on which they took effect.

Obtaining data protected by encryption

34. Part 3A of RIPL provides for the giving of notices requiring the disclosure of the key to encrypted information that is lawfully within the possession of the authorities. This power may be used to obtain passwords so as to allow access to electronic devices such as computers or mobile phones. The provisions contain power to issue a disclosure notice, where the person issuing the notice believes on reasonable grounds that doing so is in the interests of national security, for the purpose of preventing or detecting crime, in the interests of the

economic well-being of Jersey or for the purpose of securing the effective exercise or performance by any public authority or any statutory power or duty. Failure to comply with such a notice is a criminal offence.

Codes of Practice and Guidance

35. Article 51 of RIPL makes provision for the making and revising of Codes of Practice relating to the exercise and performance of powers and duties conferred or imposed by the statutory scheme. Persons exercising or performing powers under the legislation are obliged to have regard to the provisions of any relevant Code of Practice. The Codes of Practice are admissible in evidence and where relevant must be taken into account by a court or tribunal.

36. Five Codes of Practice have been made under this provision. These address:

- (a) the interception of communications;
- (b) the interception of communications (postal);
- (c) accessing communications data;
- (d) covert surveillance (including interference with property or with wireless telegraphy); and
- (e) covert human intelligence sources.

37. The Codes of Practice provide general guidance in plain language about the procedures that must be followed before the various intrusive investigation techniques can take place. They are primarily intended for use by the various public officials who authorise or use the measures in question, although they will also be useful to anyone who is interested in the operation of the legislative scheme.

General observations on the statutory scheme

38. The provisions of RIPL and PPCEL, supplemented by the Codes of Practice, provide a comprehensive framework for the regulation of intrusive investigative techniques such as the interception of communications and surveillance. The framework is intended to provide a lawful basis for executive action and

appropriate protection for citizens by seeking to ensure that these techniques are used only where that is justified and after careful and proper consideration. Whilst the need for the use of these techniques in the public interest is undeniable, so too is the need for them to be regulated so as to ensure that they are carried out in accordance with law and that the privacy of those who are the targets of surveillance is infringed only where that is necessary and proportionate.

39. Proportionality is a central concept in the legislation and in the Codes of Practice. Even if a particular course of surveillance is directed at a legitimate aim, this will not in itself be sufficient to justify the interference with the privacy of the target of the surveillance if the means used are excessive in all the circumstances. The legislative scheme is accordingly directed to ensuring respect for the Convention rights guaranteed under the Human Rights (Jersey) Law 2000.
40. The statutory provisions and the associated Codes of Practice have drawn heavily on the UK Regulation of Investigatory Powers Act 2000 and the Codes of Practice made under the Act. Whilst the 2000 Act remains the governing statutory in the UK for directed and intrusive surveillance and the use of CHIS, in the case of interception of communications and the acquisition and disclosure of communications data, that Act has been replaced by the Investigatory Powers Act 2016 and associated Codes of Practice. There have also been other amendments to the UK statutory regime. The present Jersey legislation predates the introduction of the first iPhone. The relevant authorities will wish to consider whether the legislation should be updated in light of technological developments and legal changes elsewhere.

Conduct of the Review

41. I undertook an inspection visit to Jersey in May 2025. As in previous years, the UK Investigatory Powers Commissioner, the Rt Hon Sir Brian Leveson, agreed to make available (without charge to the Government of Guernsey, save as to travel and subsistence) the services of two experienced IPCO inspectors to assist me in the exercise of my functions. In previous years, the inspection has been supported by Mr Paul Gration and Mr Steven Matthews. This year, I was supported by Mr Nicholas Fletcher and Mr Daniel Caldwell. As well as being experienced IPCO inspectors, Mr Fletcher and Mr Caldwell had previously undertaken inspections as Assistant Investigatory Powers Commissioners in Guernsey. It is right that I express publicly my gratitude to Mr Fletcher and Mr

Caldwell for their contribution to the 2025 inspection, and also to Sir Brian Leveson for continuing to make available the services of his professional inspectors. I would also like to acknowledge and express gratitude, on my own behalf and that of my predecessors, for the considerable contribution which has been made over a number of years by Mr Paul Gration and Mr Steven Matthews.

42. Like their predecessors, Mr Fletcher and Mr Caldwell brought to the inspection an expertise in and understanding of the various surveillance techniques which no Commissioner could be expected to possess. Their detailed observations, together with recommendations, drawn from their expert knowledge of best practice in the UK, were made in oral briefings to relevant personnel during the course of our inspection visit and are also contained in confidential written reports which I have submitted to the Bailiff along with this report. These confidential reports have also been provided to the relevant agencies, so as to assist them with the ongoing development of best practice.
43. As in previous years, the inspection visit focused principally on the use of surveillance powers by the Jersey law enforcement authorities (the States of Jersey Police and the Jersey Customs and Immigration Service) and on the authorisation of the use of such powers by the Law Officers. Although HMP La Moye is not within the statutory regime, the Acting Governor met with me and with the IPCO Inspectors this year. This built on a visit, last year, to HMP La Moye, at the invitation of the then Governor; and will provide a foundation for future visits.
44. During the inspection visit, the IPCO Inspectors and I received classified written briefing on the use of the various powers by Jersey law enforcement authorities. This was supplemented by oral briefings with a number of personnel involved in the authorisation, management and oversight of covert operations. The inspection team was given full access to the records relating to the use of those powers during 2024. We were given access to all of the information and provided with every facility which we required in order to undertake a full and proper inspection. I am grateful to all those in Jersey who assisted in the inspection process.

The Scope of this Report

45. Like my predecessors, I recognise the tension between the public interest in transparency and the need to maintain the confidentiality which necessarily

attends the use of covert surveillance powers. In particular, I recognise the need to avoid any risk of undermining the effectiveness of those powers in ongoing and future operations. In balancing these competing interests, I have generally followed the approach adopted by my predecessors in their reports.

46. The focus of my report is on compliance with the statutory requirements and the Codes of Practice. As in previous years, the inspection identified opportunities for improvements in practice, and these were communicated during the inspection visit. Further detail is contained in confidential reports prepared by the IPCO Inspectors which I have provided to the Bailiff along with this public report, and which have also been provided to the relevant agencies to assist them with training and the ongoing pursuit of best practice.

47. This report relates specifically to calendar year 2024.

Overview of 2024

48. I give an overview below of the use made of the various covert powers by Jersey law enforcement in the course of 2024. I can confirm that the use of these statutory powers continues to contribute significantly to the prevention and detection of serious crime in Jersey. The powers are generally being lawfully used for proper purposes and, in general, applications and authorisations were completed to a good standard, and the requirements of necessity and proportionality considered with care.

Interception Warrants

49. During 2024 twelve written interception warrants were granted. All of the warrants were properly authorised for statutory purposes. During the inspection, documentation relating to the grant, modification, cancellation and refusal of applications was inspected. This disclosed a good standard of compliance with the legislation and Codes of Practice.

Communications Data

50. During 2024 127 authorisations were granted in relation to the acquisition of communications data. They were mainly concerned with the prevention and detection of crime (the lion's share being drugs offences) but there were also

authorisations in relation to missing persons. The inspection team was satisfied that all of the authorisations were granted in respect of a correct statutory purpose and that they were appropriately tailored to the circumstances.

Intrusive Surveillance/Interference with Property

51. Four intrusive surveillance authorisations and eight property interference authorisations were granted in 2024. These were principally concerned with the detection and prevention of serious crime, mainly drug trafficking offences. These operations, as well as operations which took place in 2023, have resulted in a number of arrests, charges and convictions, and the seizure of quantities of drugs.

Directed Surveillance

52. A number of directed surveillance authorisations were granted in 2024, mainly for the purpose of preventing or detecting crime, principally (though not exclusively) drug trafficking. All of the authorisations were lawful and for proper statutory purposes.

Covert Human Intelligence Sources (CHIS)

53. In my last report, I noted that Mr Gration had made a number of recommendations in relation to the management of CHIS. Progress has been made, but I will continue to keep this aspect of the agencies' work under review.

Obtaining data protected by encryption

54. During the inspection visit, three cases were reviewed. No vulnerabilities were identified.

Notification of Errors

55. In the course of 2024, I was proactively notified of one error. Two further reportable errors were proactively disclosed in the course of the inspection visit, and advice and guidance provided in relation to these matters. The reported errors do not undermine the overall conclusion which I set out below.

Overall Conclusion

56. During the inspection visit, the IPCO Inspectors and I were provided with all necessary support and assistance. Those who facilitated the process were well-informed and generous with their time. They responded to requests for information and were receptive to feedback. In my report for 2023, I stated that I was impressed with the commitment of all of the personnel involved to realising and maintaining high standards. My appreciation of that commitment has been reinforced by my second inspection visit.
57. The inspection visit disclosed that the public officials involved in the operation of RIPL strive to meet good standards of practice, and that they generally achieve that aim even if there are also opportunities for improvement. The confidential reports which the IPCO Inspectors have prepared and which I have provided to the Bailiff include recommendations which will assist in that regard.
58. The powers are generally being lawfully used for proper purposes and, in general, applications and authorisations were completed to a good standard, and the requirements of necessity and proportionality considered with care. The inspection confirmed that the use of these powers continues to make a significant contribution to the prevention and detection of crime in Jersey. Their use has resulted in a number of convictions for serious crime and the seizure of quantities of drugs. The people of Jersey have good reason to be confident that the use of these powers serves the public interest.

Rt Hon James Wolffe KC
November 2025