

Title: Investigatory Powers Act 2016 (IPA 2016) PIR No: HO PIR0004 Original IA/RPC No: Click here to enter text. Lead department or agency: The Home Office Other departments or agencies: None. Contact for enquiries: ipareviewteam@homeoffice.gov.uk	Post Implementation Review
	Date: 28/04/2023
	Type of regulation: Domestic
	Type of review: Statutory
	Date measure came into force: 01/03/2017
	Recommendation: Amend
	RPC Opinion: Choose an item.

1. What were the policy objectives of the measure?

1. **Enhanced oversight and safeguards for use of powers:** To provide a clear and transparent framework for the exercise of investigatory powers by the security and intelligence agencies, wider public authorities, and law enforcement, with greater oversight and safeguards across the UK.
2. **Consolidation of existing powers relating to communications data, the interception of communications and equipment interference, and of oversight bodies:** To consolidate existing legislation into a concise and comprehensive Act that will improve public understanding of the need for, and the use of, these important and sensitive capabilities.
3. **Modernisation and future-proofing:** To modernise and update the legal framework surrounding investigatory powers to ensure the security and intelligence agencies, and law enforcement can continue to exercise the capabilities they need to maintain public safety and protect the public from terrorism, and serious crime. This includes cyber-crime, human trafficking and child sexual exploitation and abuse.

2. What evidence has informed the PIR?

Various sources were used to inform the analysis within this PIR. These include results from an Internet Connection Records (ICR) trial, case studies and engagement from operational partners, appeals from the Investigatory Powers Tribunal (IPT), and publicly available data from the Investigatory Powers Commissioner's Office's (ICPO) annual reports, as well as polling results from YouGov.

3. To what extent have the policy objectives been achieved?

The extent to which the new measures under the Investigatory Powers Act 2016 (IPA 2016) disrupted criminal activities and in particular, serious and organised crime and helped to safeguard national security is unknown due to the absence of data available and the sensitivity of these operations. Due to a lack of baseline polling, it has also been difficult to assess the extent to which public understanding and opinions of the IPA 2016 have changed over time. It has not been possible to do a well evidenced benefits assessment around operations and public trust. From the limited evidence available it appears that the oversight and safeguard framework has been successful and that reporting on warrant rejection standards are improving year-on-year. The IPA 2016 allows UK intelligence and law enforcement agencies to conduct their statutory duties in a legally compliant manner.

I have read the PIR and I am satisfied that it represents a fair and proportionate assessment of the impact of the measure.

Signed: Tom Tugendhat
Security Minister

Tim Laken
Chief Economist

Date: 15/06/2023

Further information sheet

4. What were the original assumptions?

1. The UK must always have an uninterrupted data retention regime.
2. It was assumed that the powers previously available to law enforcement, the armed forces and the security and intelligence agencies would remain in place in the long-run had the IPA 2016 not been enacted in 2016.
3. The Home Office maintains a policy of reimbursing 100 per cent of the reasonable costs incurred by business in complying with communications data retention requirements under previous legislation and will continue to do so for existing and new capabilities under the IPA. Given that costs were assumed to be “reasonable”, the net cost of the new provisions to business was estimated to be zero.

5. Were there any unintended consequences or Public Sector Equality Duty impacts?

There is currently a lack of flexibility in the investigatory powers framework to react and remain resilient in a situation where more Judicial Commissioners (JCs) may be needed, or powers need to be delegated to approve warrants. There is currently no provision for temporary JCs or the delegation of powers which could result in major risks in times of emergency.

A further resilience challenge with the authorisation process was identified during the COVID-19 pandemic with the role of the Prime Minister in approving triple locked warrants. During the pandemic the then Prime Minister was hospitalised and unable to consider or approve warrants. Due to the restrictive wording of the IPA 2016, there was no route for delegation of this role to the Deputy Prime Minister or any other Secretary of State. This highlighted a lack of agility and resilience in the warrant process for warrant applications of this kind.

Part 7 of the IPA 2016 requires the agencies to apply the same standard of safeguards to the retention and examination of all bulk personal datasets (BPD) regardless of the potential intrusion arising from doing so, leading to time inefficiencies and an inability to effectively use datasets held by external partners.

6. Has the evidence identified any opportunities for reducing the burden on business?

The impact assessments completed for the IPA 2016 found no net financial impact on business, which remains the case. This legislation does not introduce any new requirements for communications companies or place any unnecessary burden on them. This is because all reasonable costs are to be reimbursed to any telecommunications operators (TOs) involved. Repealing the IPA 2016 would not deliver benefits or cost savings to business.

7. Are there any impacts on small businesses, trade, wider economy / society?

There is no evidence to suggest that the IPA 2016 imposes any significant negative impacts on small businesses, trade, the wider economy, or society. The IPA 2016 has had a positive impact on wider society as the introduction of Investigatory Powers Commissioners Office (IPCO) has streamlined the applicable oversight regime, consolidating it under one body and providing further accountability and transparency for the use of investigatory powers. The IPA 2016 also introduced a new right of appeal from decisions and determinations of the Investigatory Powers Tribunal in circumstances where there is a point of law that raises an important point of principle or practice, or where there is some other compelling reason for allowing an appeal.

Evidence Base

A. Background

1. The Investigatory Powers Act 2016 (IPA 2016) was introduced to replace the emergency legislation passed in July 2014 (the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014)). As emergency legislation passed in response to the European Court of Justice (ECJ) striking down the Data Retention Directive of 2006 (DRD 2006), DRIPA 2014 was subject to a sunset clause providing for the legislation to be repealed on 31 December 2016. During the passage of DRIPA 2014, the Government committed to bring forward new legislation which would provide security and intelligence agencies, law enforcement and other public authorities with the investigatory powers necessary to address evolving threats within a changing communications environment.
2. Pre-existing laws such as the Regulation of Investigatory Powers Act 2000 (RIPA 2000) were not sufficiently equipped to deal with the increasing speed of technological change, which made it increasingly difficult for security and intelligence agencies to carry out their statutory duties including keeping the public safe. The IPA 2016 updated the legal framework governing the state's ability to acquire communications and data about communications, whilst also applying greater safeguards and oversight for when these powers may be used.
3. The introduction of the IPA 2016 also consolidated and updated powers which were previously provided for in a number of different statutes. Some of these Acts were enacted before the internet became a widely used means of communication so were ill-equipped for the challenges of modern technology. Bringing all these powers together under the IPA 2016 helped to make the legal framework that applied to law enforcement and intelligence agencies clearer and more understandable.

B. Rationale

4. The introduction of the IPA 2016 was a landmark piece of legislation to help enable law enforcement, intelligence and security agencies and public authorities to exercise their powers in a way that is compliant with a need to have adequate protections for privacy in an ever-changing technological landscape. The objective of this PIR is to review whether these policy objectives have been achieved. This is done by reviewing the evidence presented in the original impact assessments (IA) made in 2016 and, where possible, present any new analysis which has been carried out since then to inform the rationale.

C. Policy objectives

Strategic objective

5. The objective of the IPA 2016 was to update and modernise the legal framework for the use of investigatory powers, including the acquisition of communications data (targeted, and in bulk), the retention of communications data, the interception of communications (targeted, and in bulk), equipment interference (targeted, and in bulk) and the intelligence agencies' use of bulk personal datasets, as well as improvements to the oversight and safeguards that apply to these powers.
6. The IPA 2016 framework exists and is used by the relevant public authorities to obtain communications and communications data to carry out operations and to continue to protect the public.

Policy objectives

- c.1 **Enhanced oversight and safeguards for use of powers:** To provide a clear and transparent framework for the exercise of investigatory powers by the security and intelligence agencies, wider public authorities and law enforcement, with greater oversight and safeguards.
- c.2 **Consolidation of existing powers relating to communications data, the interception of communications and equipment interference, and of oversight bodies:** To consolidate existing legislation into a concise and comprehensive Act that will improve public understanding of the need for, and the use of, these important and sensitive capabilities.
- c.3 **Modernisation and future-proofing:** To modernise and update the legal framework to ensure the security and intelligence agencies, wider public authorities and law enforcement can continue to exercise the capabilities they need to maintain public safety and protect us from terrorism, and serious crime including cyber-crime, human trafficking and child sexual exploitation.

D. Policy option implemented

7. The policy decision taken in 2016 was to deliver the IPA 2016 which clarified the existing legal framework for investigatory powers, including:
 - Interception,
 - Communications data and equipment interference,
 - The safeguards for security and intelligence agencies' use of bulk personal datasets, and the retention of communications data, including additional retention of internet connection records,
 - Increasing oversight and providing for judicial approval of warrants.
8. Had the Government failed to introduce legislation, it would have severely hindered the capabilities of law enforcement, the security and intelligence agencies and wider public authorities to fulfil their obligations effectively. It would still have left a patchwork of legislation governed over different legal statutes.

E. Summary of the analytical assessment at the time

Assumptions

9. The assumptions presented below were those considered in the Overarching IA published in 2016 that combined the assumptions, costs, and benefits within the six other IAs for the IPA 2016.¹
 - That the UK requirement for a data retention regime is such that it would not be permitted to lapse.
 - It was assumed that the powers currently available to law enforcement, the armed forces and the security and intelligence agencies would remain in the long run were the IPA 2016 not implemented.
 - While efforts have been made to understand the costs and benefits to all affected groups, it is necessary to make some assumptions. The Home Office has consulted government departments, Telecommunications Operators (TOs) and operational partners including law enforcement and the security and intelligence agencies.

¹ Investigatory Powers Act: Overarching Impact Assessment - Link
https://www.legislation.gov.uk/ukia/2017/130/pdfs/ukia_20170130_en.pdf

- The Home Office maintains a policy of reimbursing 100 per cent of the reasonable² costs incurred by business in complying with communications data retention requirements under current legislation and will continue to do so for existing and new capabilities under the IPA 2016. The net cost of the new provisions to business will be zero.

Analysis

10. Table 1 outlines the analysis done across the six IAs produced for the IPA 2016. Of the six IAs, only two contained monetised costs and none of the IAs contained monetised benefits.
11. As there would be minimal increases above existing baseline costs for interception, equipment interference and bulk personal data the costs of the IPA 2016 are primarily in relation to increased cost of establishing a new oversight body (led by the Investigatory Powers Commissioner (IPC)), including accommodation, overheads, running costs and the administration of a new warrant process. The provisions in the IPA 2016 in relation to internet connection records and the request filter for communications data also have associated costs to business, which are reimbursed by government.

Costs and benefits

12. This section describes the costs and benefits set out in the original overarching IA from 2016³, see Table 1.

² The Communications Data Code of Practice, page 119 - Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

³ Investigatory Powers Act 2016: Overarching Impact Assessment – Link: https://www.legislation.gov.uk/ukia/2017/130/pdfs/ukia_20170130_en.pdf

Table 1, Net Present Cost (NPC) £ million (PV), over 10 years.

Policy provision	NPC (£m PV)	Non-monetised cost	Non-monetised benefit
Oversight⁴	61.51	There are additional non-monetised costs as staff in the new bodies take time to familiarise themselves with new structures and reporting arrangements.	Increased understanding of public oversight of accountability and investigatory powers. Public and parliamentary trust and confidence in the rigour of Commissioner oversight and the way that investigatory powers use is authorised. There are likely to be efficiency savings from the merger of the existing oversight bodies, (shared resources and knowledge, reduce duplication of effort).
Domestic right of appeal from the IPT⁴	The Home Office and MoJ have agreed that the impact to the justice system is likely to be minimal.	There will likely be a necessary cost of time to train the IPT and its secretariat in the new rules and procedures.	Allowing a domestic right of appeal from the IPT has a positive impact on those who are able to appeal. It is easier to understand and less stressful to those involved. Fewer cases referred to the European Court of Human Rights (ECtHR), having been dealt with in the domestic courts, saving appellants' time and cost.
Interception⁴	n/k	n/k	Greater public confidence and transparency in the interception regime. Legislation will allow UK intercepting agencies to continue to investigate threats to ensure they can keep the public safe.
Communications Data⁴	187.1	Minimal business costs associated with change of each capability, for example, training for operational personnel	Greater public confidence and transparency in the communications data regime. Law enforcement and public authorities able to access the data needed as part of the investigations.
Bulk Personal Data⁴	n/k	Additional training and familiarisation costs for reporting arrangements, applicable to the Commissioners, Security and Intelligence Agencies (SIA), Home Office, and the Foreign and Commonwealth and Development Office (FCDO), policy, legal officials and advisers as they spend time understanding the new authorisation / reporting arrangements.	Will improve public confidence in the safeguards that apply to the SIA use of bulk personal datasets, providing the public with greater understanding and transparency.
Equipment Interference⁴	n/k	n/k	Greater confidence in the public exercise equipment by interference of law agencies, the armed enforcement forces and the security and intelligence agencies. To acquire communications, equipment, data and other information of the clearer, well-evidenced resulting safeguards and oversight applied to the use of equipment interference, with accountability to Parliament.

Source: Home Office own estimates, See the IPA Investigatory Powers Act 2016: Overarching IAT⁴

Note: n/k = not known. No net present benefit is given as this is unknown. ECtHR, FCDO, SIA

⁴ [Investigatory Powers Act 2016 - Impact Assessment Link: https://www.legislation.gov.uk/ukpga/2016/25/impacts/2017/131](https://www.legislation.gov.uk/ukpga/2016/25/impacts/2017/131)

Note: The reader can select the relevant enactment part to read the relevant policy provision in the Legislation.gov website. For example, the reader would select "Enactment part 2", to read the Impact Assessment relating to Communications Data.

Any other (small business, trade, wider etc)

13. The IPA 2016 did not introduce any new requirements for TOs or place any unnecessary burden on them. The Government has worked with TOs to ensure that any requests for assistance can be carried out with the least amount of impact on their business.

F. Evaluation / review of impacts

14. **Objective 1: Enhanced oversight and safeguards for use of powers:** *To provide a clear and transparent framework for the exercise of investigatory powers by the security and intelligence agencies, law enforcement, and wider public authorities with greater oversight and safeguards.*

Oversight

15. The Investigatory Powers Commissioners Office (IPCO) was created to increase public understanding of the oversight and accountability of investigatory powers. It was also intended to boost public and parliamentary trust and confidence in the rigour of Commissioner oversight and the way in which the use of investigatory powers is authorised.
16. In previous analysis, it was estimated that the average annual cost of creating IPCO would be **£7.4 million** (2016 prices), with a 10-year Net Present Social Value of **-£61.5 million**. These costs considered the extra resources required for the increased workload of the agencies and other government departments in terms of new oversight arrangements.
17. Due to an absence of data, it has not been possible to estimate the costs to agencies and other government departments brought about by the oversight measures. However, the annual IPCO spend is published publicly every year.
18. The initial year was a transition year so the 2017/18 spend is for six months rather than 12. In the 2019/20 and 2020/21 annual reports the annual IPCO budgets were also published and IPCO spent below budget in both years.

Table 2, IPCO Annual Spend, £ million (PV)

Year	Spend (2022/23 Prices)
2017/18 (01/10/17 - 31/03/2018)	3.1
2018/19	6
2019/20	6.6
2020/21	6.1

Source: IPCO Annual Reports, 2017/18-2020/21⁵

19. If the average cost over the remaining six years was the average annual cost of years 2018/19 to 2020/21 (**£6.2 million**, 2022/23 prices), then the cost over the next six years would be **£31.8 million (PV)**. This would bring the total cost to **£54.8 million (PV)** over 10 years. Whilst actual figures appear to be lower than initially estimated, also after adjusting for inflation, the two NSPV estimates are not directly comparable as the latest does not take into account the extra resources required for the increased workload of agencies and other government departments in regard to the new oversight reporting arrangements and is expected to be an under-estimate.
20. IPCO have released four annual reports since it began and collect a wide range of statistics on the use of investigatory powers, including those required to be published in their annual reports under section 234 of the IPA 2016. These reports provide transparency around oversight, and below are some examples of what is included. These focus on 2019 data as COVID-19 resulted in changes in the way inspections took place over the following years.

⁵ Annual Reports – IPCO - Link: <https://www.ipco.org.uk/publications/annual-reports/>

Safeguarding and oversight - Warrant applications

21. In 2019, a Judicial Commissioner (JC) rejected one application for the renewal of a combined Targeted Interception (TI) and Targeted Equipment Interference (TEI) warrant from MI5. The circumstances of the case were that data could not be obtained at the time of the renewal and had not been obtained in the previous period, but MI5 assessed that their officers might be required urgently to conduct actions under the warrant if the subject of the warrant was released from custody. The JC considered that the renewal was driven by considerations of administrative convenience and was neither necessary nor proportionate. The JC considered that, if the subject was released, MI5's operational team and the Home Office warrantry team might need to apply to put monitoring techniques quickly in place, but that this should not be prioritised over the subject's rights to privacy.⁶
22. This example demonstrates, qualitatively, the effective and impactful safeguarding of an individual's rights to privacy. This provides some evidence to suggest that the objective of enhanced oversight and safeguards for use of powers has been achieved to an extent.
23. Within the IPA 2016, a new offence was introduced under section 11 for knowingly or recklessly obtaining, examining or disclosing communications data without lawful authority. This was created to prohibit the misuse of capabilities by public authorities and to provide additional reassurance to the public. It was assumed in the overarching IA¹ there would be minimal costs incurred to the criminal justice system (CJS) associated with the creation of new offences. This has been the case as the IPCO has not yet recommended that a police force carry out an investigation and nor has the Crown Prosecution Service prosecuted a suspected section 11 offence since the inception of the IPA 2016 and therefore no offences have been recorded for any of the three new offences introduced. Had there been any investigations, prosecutions or convictions of these three new offences, a marginal cost would have been conferred on the justice system. As there were no prosecutions for this crime in the years since section 11 was commenced, no marginal costs have been conferred on the justice system.

Safeguarding and oversight - Serious errors

24. IPCO carries out serious error investigations and publishes the outcomes of these in annual reports. In 2019, IPCO undertook 18 serious-error investigations and determined that 14 cases were serious errors, where an instance of non-compliance has resulted in significant prejudice or harm to an individual or individuals. The IPCO has a duty to inform affected parties of a serious error under section 231 of the IPA 2016, if they judge that this is in the public interest. These cases are summarised within annexes in the IPCO annual reports, increasing the transparency around the use of IPA 2016.
25. This data from 2019 demonstrates, qualitatively, a diligent oversight function. This provides some evidence to suggest that the objective of enhanced oversight and safeguards for use of powers has been achieved to an extent.
26. In 2020, IPCO undertook 29 serious error investigations. Of these investigations, 16 were caused by the relevant public authorities and 13 were caused by the Telecommunications Operator (TO). IPCO identified significant harm in four of the 29 cases investigated. Compared to the 2019 data, the proportion of cases which were judged to impose serious harm was reduced from 78 per cent to 14 per cent. Although it is not possible to draw strong conclusions from a small sample size of errors over 2 years, the 2019 and 2020 data show an overall increase in the safeguarding and oversight in the use of the IPA 2016.
27. No monetary benefits were quantified for the introduction of IPCO. The non-monetary benefit of this would be increased public confidence and understanding in the oversight system and greater public and parliamentary trust in the authorisation and oversight regime.

Bulk Communications Data

28. The only new costs associated with the bulk communications data provisions relate to increased reporting in line with the new safeguards and form part of the oversight costs. From 2018/19 to

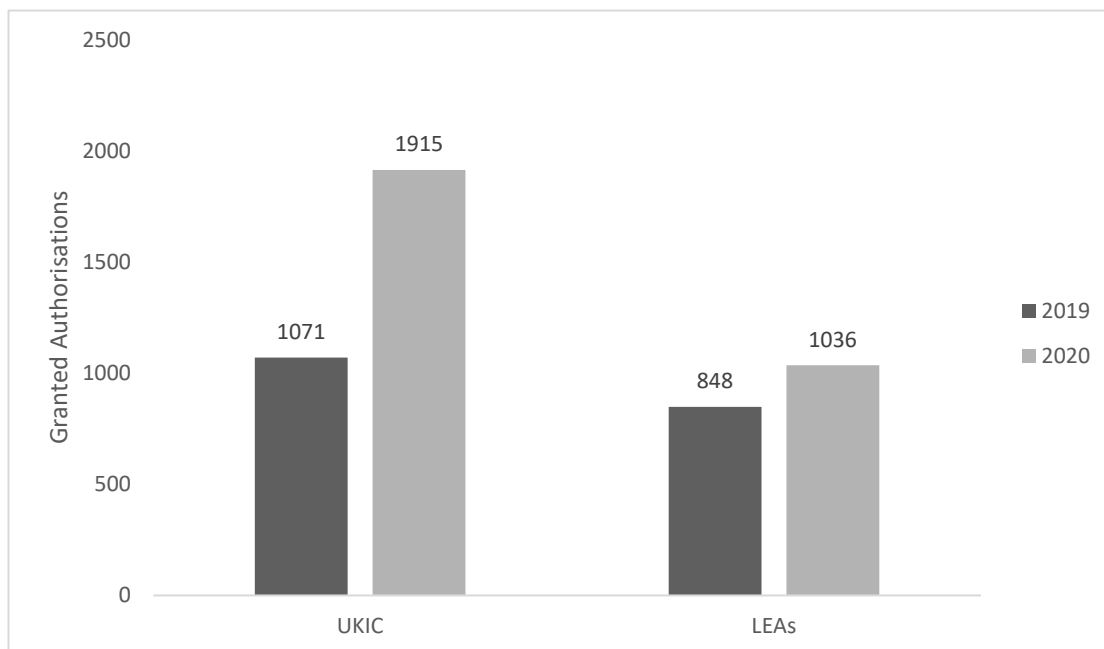
⁶ Annual Report of the Investigatory Powers Commissioner 2019 - Link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf

2020/21 there have been no bulk communications data acquisition warrants refused by a JC, showing that only necessary and proportionate applications are being made. This does, however, assume that the warrant authorisation requirements are sufficiently high.

Equipment interference

29. When brought in, the IPA 2016 replaced existing statutory bases for equipment interference for the acquisition of electronic communications and other data with a single legislative provision that would provide for equipment interference by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis. It made it clear that assistance can be requested under a technical capability notice; and it applied additional protections for the communications of MPs and other legislatures.
30. The number of targeted equipment interference (TEI) authorisations cannot be presented as comparable statistics from 2017 because the introduction of TEI warrants under the IPA 2016 established a new category of authorisation for activity which was previously conducted under disparate legislation. Figure 1 shows 2020 authorisations only and for UK intelligence community (UKIC) includes applications made under combined warrants compared to the number of authorisations granted to use TEI powers in 2019.

Figure 1, Targeted equipment interference authorisation for the UKIC and LEA, 2019-20.



Source: IPCO Annual Report 2020⁷

Note: UKIC = UK Intelligence Community, LEA = Law Enforcement Agencies.

31. In 2020, 2,951 authorisations were granted to use TEI powers, an increase of 54 per cent compared to 2019, when 1,919 authorisations were granted. Of the 2,951 authorisations issued, 363 were made under urgent provisions. For UKIC, many TI warrants were combined with TEI. Six warrants were refused by a JC, down from 17 in 2019. This provides evidence to suggest that safeguards are being used to ensure that equipment interference is being used appropriately.

Interception

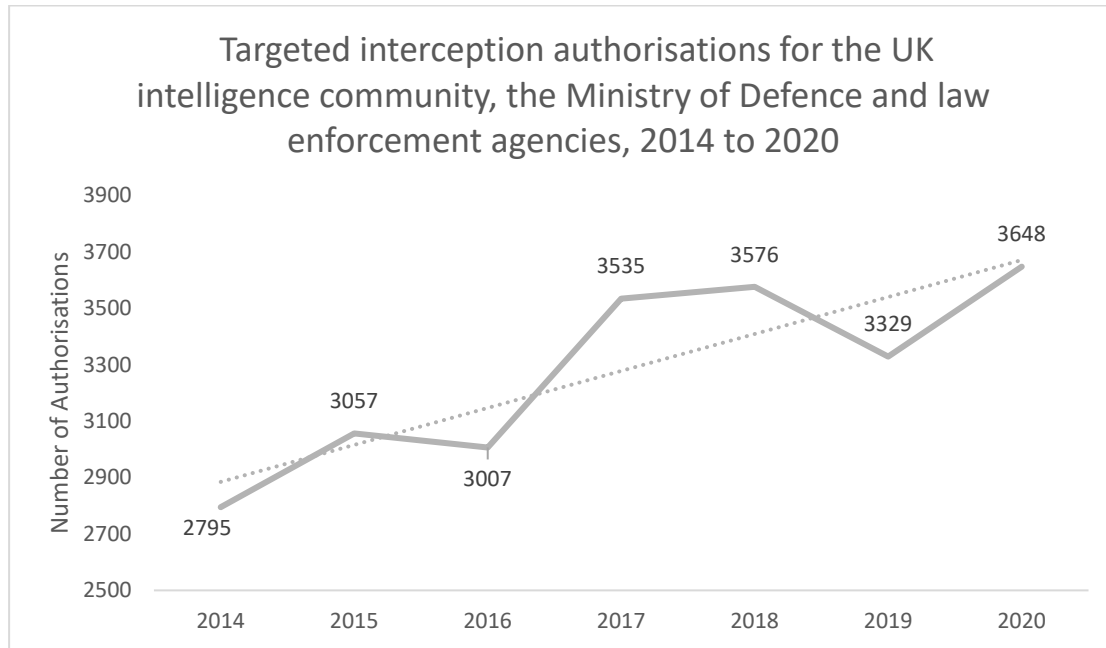
32. As a result of the IPA 2016, the UK intercepting agencies have been able to *continue* to investigate threats to ensure they can keep the public safe. The additional costs as a result of this policy are those in respect of additional reporting requirements as a result of new oversight measures that fall on the intercepting agencies. As a result of the reporting requirements, the main benefits of the IPA 2016 are captured in non-monetised benefits through improved oversight and safeguards that apply to the interception of communications. Interception should not be undertaken if the information could

⁷ HC 897 – Annual Report of the Investigatory Powers Commissioner 2020 Link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

be obtained by another less intrusive method. Interception warrants are only sought and granted where information about subjects of interest and their networks cannot be acquired via other means.

33. The number of TI warrants granted increased by 9.8 per cent in 2020 in comparison to 2019. Of the warrants approved, 1,470 were renewals and 59 were obtained under urgency provisions.

Figure 2, Targeted interception authorisation for the UKIC, MoD and LEA, 2014-20.



Source: IPCO Annual Report 2020

Note: UKIC = UK Intelligence Community, MoD = Ministry of Defence, LEA = Law Enforcement Agencies.

34. Based on these data available (IPCO Annual Report 2020)⁷, it is not possible to infer whether the upward trend in TI warrants was caused, either partially or wholly, by the IPA 2016. The IPA 2016 did not intend on decreasing TI warrants, nor did it directly intend on increasing TI warrants. Rather, the IPA 2016 sought to enhance oversight and safeguards for use of powers. Of 3,649 warrants applied for in 2020, one was refused by a JC.
35. **Objective 2: Consolidation of existing powers relating to communications data, the interception of communications and equipment interference, and of oversight bodies-** *To consolidate existing legislation into a concise and comprehensive Act that will improve public understanding of the need for, and the use of, these important and sensitive capabilities*

Confidence

36. The non-monetised benefits in equipment interference, interception, IPT appeals, communications data and bulk personal dataset legislation all focussed on increased public confidence and transparency as a result of the IPA 2016. This is difficult to measure due to lack of baseline polling done before IPA 2016 came into force. Proxy polls available on YouGov have been used to attempt to investigate confidence levels over the past seven years. As stated throughout the previous analysis, there is a risk that the IPA 2016 does not fully realise the objective of policy to improve public confidence in the regime. Due to an absence of data, the analysis is not well-evidenced enough to suggest this occurred or that there is a direct association with the IPA 2016 but does provide context for the overall government policy targeting this objective.
37. In August 2013, 1,886 individuals were asked about the way the Government balances fighting terrorism and protecting the privacy and human rights of ordinary people. Of these, 31 per cent answered that security forces should be given more investigative powers to reduce terrorism, even if this means the privacy or human rights of ordinary people suffers.

Table 3 Thinking about the way the government balances fighting terrorism, and protecting the privacy and human rights of ordinary people...(do you agree that?)⁸

Description	(%)
More should be done to protect the privacy and human rights of ordinary people, even if this puts some limits on what the security forces can do when combatting terrorism	22
The security forces should be given more investigative powers to combat terrorism, even if this means the privacy or human rights of ordinary people suffers	31
The current balance between combatting terrorism and protecting the privacy and human rights of ordinary people is about right	30
Don't know	17

Source: YouGov, August 2013

38. In December 2019, 1,699 individuals were asked a similar question surrounding the balance of government powers to protect against terrorism vs peoples' freedom to go about their daily lives. Although phrased slightly differently, the second poll allows the Home Office to assess how general attitudes towards government powers around security have changed over time.

Table 4, Thinking about the balance between protecting against terrorism, and protecting people's freedom to go about their daily lives, do you think... (do you agree that?)⁹

Description	(%)
The government should introduce stricter measures to protect against terrorism, even if it means people's personal freedoms are restricted	45
The government have restricted people's personal freedoms too much and measures should be relaxed, even if it limits the ability of the authorities to combat terrorism	7
The current balance is about right	32
Don't know	16

Source: YouGov, December 2019

39. In 2019, 45 per cent of those questioned believed that the Government should introduce stricter measures to protect against terrorism, even if it means people's personal freedoms are restricted. Just 7 per cent stated that measures should be relaxed to increase people's personal freedoms.
40. Although tempting to make direct comparisons between the 2013 and 2019 polling answers, this cannot be done due to the different phrasing of the questions. In general, there appears to be a more positive attitude to the Government having more strict measures to protect against terrorism in 2019 than in 2013. Both surveys were conducted by YouGov, a polling firm.¹⁰
41. The answers to these questions must be considered in the context of the time. The 2013 YouGov poll was conducted shortly after Edward Snowden (former US computer intelligence consultant) leaked information from the US National Security Agency (NSA) on the surveillance operations of various agencies. This was publicised throughout the media and may have led to heightened fears of government surveillance.
42. Before the 2013 murder of Lee Rigby, the last UK terrorist attack had been the 7/7 bombings in 2005. Between 2013 to 2019 there were nine terrorist attacks, including the high-profile Manchester Arena

⁸ Survey Report (yougov.com) - Link: <https://docs.cdn.yougov.com/gsuxbb3zi3/GB%20attitudes%20to%20Snowden%20%26%20surveillance%2C%20Aug%202013.pdf>

⁹ Survey Report (yougov.com) - Link: https://docs.cdn.yougov.com/42o6h7hrr0/TheTimes_TerrorismResults_191203.pdf

¹⁰ YouGov | Panel Methodology - Link: <https://yougov.co.uk/about/panel-methodology/>

bombing which was the deadliest terror attack¹¹, 23 people killed (including the attacker) and over 1,017 injured, on British soil since the 7/7 bombings 12 years before.¹²

43. In the context of this and the polling questions not referring to the IPA 2016 or specific legislation, it is difficult to know if the shift in opinion is due to the IPA 2016 and therefore, cannot be attributed to the IPA 2016 directly. Nevertheless, the evidence suggests that there has been a shift in opinion towards government surveillance powers since the IPA 2016 came into force, and from these polls it appears the public has a better understanding of the need for, and the use of, capabilities to protect the public against terrorism.

Investigatory Powers Tribunal (IPT) appeals

44. Although the route available to challenge a decision of the IPT was not clearly defined prior to the introduction of the right of appeal in the IPA¹³, claimants who wished to challenge a decision of the IPT generally did so via the ECtHR. Proceedings in the ECtHR are generally dealt with on paper, with public hearings being exceptional. As recommended by David Anderson QC in 'A Question of trust'¹⁴, the IPA 2016 saw the introduction of a domestic right of appeal on a point of law and on the basis of either a decision or a determination made by the IPT. It was originally anticipated that there would be fewer than 10 claims / complaints which would be eligible for an appeal per year. The test for the grant of leave to appeal is strict and usually requires there to be not only a real prospect of success but also an important point of principle or practice.
45. On average, 10 applications for leave to appeal have been received per year from 2019-2021. [The](#) number of requests is increasing year on year, reaching 18 in 2021. Due to the limited period covered by the data available and because some cases from these years are still ongoing and the figures may change in future reporting, it is not possible to infer whether this rising trend can be associated with the introduction of IPT appeals or is a short-term trend.
46. Relating to the period between 2019 to 2021, there have been 32 applications for leave to appeal received by the IPT. The decision granting or refusing leave to appeal are dealt with in a matter of weeks by the IPT. It is not possible to quantify the time that might have been saved by the introduction of a UK-based right of appeal to IPT judgments when compared to when the ECtHR/judicial review were the only options available. Given the relatively recent introduction of the right of appeal, together with the complex nature of IPT cases and the delays caused by COVID-19, it is not possible to calculate an average time for appeals from the IPT to make their way through the Court of Appeal and the Supreme Court. An example of how long the process can take is seen in the "Third Direction" case (*Privacy International & others -v- Secretary of State for Foreign and Commonwealth Affairs & others* [2019] UKIPTrib IPT_17_186_CH)¹⁵, judgment dated 18 December 2019) where the IPT handed down its judgment in December 2019 and granted leave to appeal. The Court of Appeal dismissed the appeal in 2021 and the Supreme Court refused permission to appeal the Court of Appeal's decision in 2022. From the date of the appeal against the IPT's decision being received by the Tribunal to the decision of the Supreme Court it took 831 days. Previously if someone wanted to appeal an IPT judgment they would have had to go to the ECtHR which endeavours to deal with cases within three years, 1095 days, Although this is not a direct comparator, it does suggest that the introduction of the domestic right of appeal provides some time efficiencies. It also reduces the likelihood of a successful application to the ECtHR, since the domestic courts are likely to correct any errors of law that there may have been.

¹¹ Sky News | Terror in the UK: Timeline of attacks - Link: <https://news.sky.com/story/terror-in-the-uk-timeline-of-attacks-11833061>

¹² Manchester Arena Inquiry Day 44 Official Court Reports - Link: <https://files.manchesterarenainquiry.org.uk/live/uploads/2020/12/07182655/MAI-Day-44.pdf>

¹³ It was also possible to challenge a decision of the IPT by way of judicial review proceedings in the courts of the UK, although this was not clear until the decision of the Supreme Court in *R (Privacy International v Investigatory Powers Tribunal)* in 2019. For link please see footnote 15.

¹⁴ A question of trust: report of the investigatory powers review – Link: <https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review>

¹⁵ *Privacy International & others v Secretary of State for Foreign and Commonwealth Affairs & others* - The Investigatory Powers Tribunal – Link: <https://investigatorypowerstribunal.org.uk/judgement/privacy-international-others-v-secretary-of-state-for-foreign-and-commonwealth-affairs-others/>

47. No cases have gone through the ECtHR since the introduction of the right of appeal at IPT, although this may happen in the future if cases exhaust domestic options. The available evidence suggests the IPA 2016 may have contributed to creating a clear and transparent way in which to appeal IPT decisions. For those cases that may go to the ECtHR, the benefit will be that arguments have been heard in more than one court and expressed at a very senior judicial level which will aid the legal process, ensuring stronger judgments overall.

Equipment interference

44. The IPA 2016 makes clearer and more transparent the use of TEI for the acquisition of electronic communications and other data by security and intelligence agencies, armed forces and law enforcement agencies, and the use of bulk EI which is reserved for use by security and intelligence agencies.
45. As the past regime was simply being replicated through new legislation, there were no additional costs to industry as a result of this policy from the baseline. The ongoing baseline costs of the technical systems and resource used to carry out equipment interference remain, with no cost incurred above those already established.
46. The non-monetary benefits were greater public confidence in the transparency and clarity of the legislation that applies to interference with equipment to acquire electronic communications and other data as a result of the strengthened safeguards and additional oversight, through the introduction of a double-lock authorisation process, whereby a JC approves warrants issued for equipment interference following authorisation from the Home Secretary. This has been considered in the polling discussion in paragraph 34-41.

Interception

47. The IPA 2016 makes clearer and more transparent the legislative basis for the interception of communications by law enforcement, the armed forces and the security and intelligence agencies on a targeted basis, and the interception of communications in bulk by the security and intelligence agencies.
48. Costs of interception are not made public so that inferences cannot be made about the nature of these capabilities. As mentioned above, the benefits are captured in non-monetised benefits as the legislation improved the oversight and safeguards that apply to the interception of communications, giving the general public greater confidence in the transparency and accountability of the state's ability to intercept communications.
49. **Objective 3: Modernisation and future-proofing:** *To modernise and update the legal framework to ensure the security and intelligence agencies and law enforcement can continue to exercise the capabilities they need to maintain public safety and protect us from terrorism, and serious crime including cyber-crime, human trafficking and child sexual exploitation.*

Internet connection records (ICRs)

50. Internet Connection Records (ICR) have been trialled since the IPA 2016 was enacted. Where it is deemed necessary and proportionate, an authorised public authority, as defined in schedule 4 of the IPA 2016, can acquire ICRs to identify individuals who have been accessing a site or service on the internet, or for a given device the sites or services accessed.
51. Two ICR trials have been led by the National Crime Agency (NCA), supported by the Home Office, and overseen by the IPCO. The total number of applications for ICR data within the trials equate to less than 1 per cent¹⁶ of applications made nationally for other types of Communications Data. All applications for disclosure of data were considered by the independent Office for Communications Data Authorisation (OCDA). ICRs within the trial could only be used *for intelligence purposes* and in corroboration with other evidence as opposed to being solely relied upon to prosecute. Despite this

¹⁶ Annual Report of the Investigatory Powers Commissioners Office 2020 - Link: <https://www.ipco.org.uk/publications/annual-reports/>

limitation, ICRs remain a crucial tool for investigative purposes and underpin other substantive evidence which can be presented in court as evidence.

52. There are sensitivities associated with the ongoing investigations resultant from ICRs. This is because the ICRs acquired in the trial often relate to serious crimes in line with the conditions for the use of ICRs as set out in s62 IPA. In addition, ICRs within the trial were used for intelligence only. As such, any harm-reduction outcomes, resultant from ICRs alone, cannot be quantified from the limited available data. Instead, a qualitative description of the potential benefits which the trial may have conferred to society is described in the case studies below.
53. The ICR trial data has contributed to several investigations. The data provided by the trial has provided information which would not have been available in the absence of the ICR trial, providing several qualitative benefits.
54. **Case Study One – Subject Discovery - Child Sexual Abuse and Exploitation** - ICRs were acquired on the 50 highest priority subjects seeking connection to websites whose sole purpose was to provide access to indecent images of children. Analysis suggested that only four were previously known to Law Enforcement. Individual enquiries are ongoing, but information derived from the trial informed strategic assessments concerning the scale, methodology and behaviours behind this type of offending.
55. This case study reports that police are being provided with additional valuable investigative information to identify subjects of interest who might otherwise have evaded detection. This would not have been possible in the absence of the ICRs, enabling reduced risk and potential safeguarding of children.
56. **Case Study Two – Homicide Investigation** - ICR data acquired in connection with a Homicide Investigation provided officers with focused leads as to the whereabouts of a wanted subject. Without ICRs bringing this direction to the enquiry, investigating officers would have had to conduct more extensive, broad and intrusive enquiries to narrow down potential locations of interest.
57. This case study reports economic benefits through police FTE time savings associated with being able to make more concentrated enquiries around specific geographic locations.
58. **Case Study Three: Firearm offences** - In an investigation into the discharge of a firearm, a suspect was located directly as a result of ICRs acquired. Their temporary location was some significant distance from their usual area of operation and would not have been identified, certainly as swiftly, without the ICR data. This allowed police search resources to be stood down far more quickly than might otherwise have been the case (making them available for other investigations) and mitigate anticipated further threat.
59. This case study suggests there have been two economic benefits. Firstly, police FTE time and resource were saved due to the ICRs directing them to the subject's location. Secondly, the risk of potential further firearm offences was averted as a direct result. Further, public confidence in the police services' ability to deal with firearms offences have been enhanced.
60. **Case Study Four: Subject Development – Child Sexual Exploitation and Abuse** - In an Investigation into activities of a registered sex offender, ICRs were instrumental in securing a search warrant for a subject's home address where officers recovered 1000s of indecent images. The ICR intelligence formed the primary information in support of the warrant from a Magistrate which would not otherwise have been possible to secure under the circumstances.
61. This example reports a potential economic benefit of reducing the risk of contact child sexual abuse (CSA) from taking place. Further information regarding CSA is reported below.
62. CSA is often split into contact and non-contact offending:
 - Contact offending is defined as any sexual abuse that *“involve[s] physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as*

masturbation, kissing, rubbing, and touching outside of clothing” (Department for Education, 2018a¹⁷).

- Non-contact offending is defined as where “*a child is abused without being touched by the abuser. This can be in person or online and includes flashing, showing pornography and forcing a child to make, view or share child abuse images or videos*” (NSPCC, 2022¹⁸).
63. There is overlap between contact and non-contact abuse, and abuse that takes place online. For example, offenders may elicit indecent images from children they interact with online without ever meeting them in the ‘offline’ world. Alternatively, contact offenders may create child sexual abuse material in the ‘offline’ world, that is then subsequently shared and used by offenders in online spaces, who never have contact with that child.
64. Whilst the impact of child sexual abuse on victims and survivors can vary significantly, there is strong evidence that child sexual abuse is associated with an increased risk of adverse outcomes in many areas of a person’s life. This can include physical, emotional, and mental wellbeing, relationships, socioeconomic outcomes, and vulnerability to re-victimisation. The impact of child sexual abuse can be significant, regardless of the type of abuse suffered (including where the abuse takes place in an online environment) and can be influenced by a range of factors including the duration of the abuse, an individual’s coping mechanism, and the support they receive. The Home Office estimates the financial and non-financial (monetised) cost relating to all victims who continued to experience contact sexual abuse, or who began to experience contact sexual abuse, in England and Wales in the year ending 31 March 2019 is at least £10 billion¹⁹ and includes the costs of this cohort being victimised in previous and future years, in addition to lifetime consequences as a result of experiencing child sexual abuse.
65. Some subjects of interest (SOI’s) identified through the ICR trial have been found to already be known to the authorities. It is not possible to state whether this is for similar crimes at this stage. Data from two meta-analyses conducted by Seto and others (2011)²⁰ reports the proportion of men to be dual offenders of both illicit images of children (IIOC) and contact CSA to range between 12 and 55 per cent. This provides some evidence to suggest that some proportion of the SOIs identified in the ICR trial may be dual offenders and may have been prevented from imposing harm on children because of the trial. **Due to a lack of conclusive evidence from the trial, it is not appropriate to determine how much harm has been avoided. Hence, this benefit has not been quantified.**

Interception and equipment Interference

66. Currently, it has not been possible to obtain case studies that showcase the use of interception and equipment interference due to the sensitivity of operations.

Value for money (VfM) and economy, efficiency, and effectiveness test (the 3Es test)

67. The first stage in meeting the VfM test²¹ is assessing whether the IPA 2016 has met the policy objectives. As a full assessment of the IPA 2016 could not be made due to the limited evidence available, it is not possible to make a conclusive assessment on VfM. There is however some limited evidence which suggests that some aspects of the policy objectives may have been achieved.

¹⁷ The economic and social cost of contact child sexual abuse - Link: <https://www.gov.uk/government/publications/the-economic-and-social-cost-of-contact-child-sexual-abuse/the-economic-and-social-cost-of-contact-child-sexual-abuse> (under heading 1.2)

¹⁸ NSPCC Learning – Protecting Children from sexual abuse - Link: <https://learning.nspcc.org.uk/child-abuse-and-neglect/child-sexual-abuse>

¹⁹ The economic and social cost of contact child sexual abuse - Link: <https://www.gov.uk/government/publications/the-economic-and-social-cost-of-contact-child-sexual-abuse/the-economic-and-social-cost-of-contact-child-sexual-abuse>

²⁰ Contact sexual offending by men with online sexual offences - Link: <https://pubmed.ncbi.nlm.nih.gov/21173158/>

²¹ HM Treasury (2022) Green Book Supplementary Guidance, value for money - Link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064518/Green_Book_supplementary_guidance_-_Value_for_Money.pdf

68. The 3Es test, the criteria used to assess the value for money of government spending, is explained clearly on the NAO webpage²².
69. **Economy** (minimising the resources used with regard to quality – spending less): The evidence available suggests the number of appeals to IPT have been increasing over the period 2019 to 2021, and internal IPU evidence suggests no cases have been submitted to the ECtHR since the introduction of the right of appeal at IPT. As appeals through the ECtHR are free to make, additional costs may have been imposed on the UK justice system in dealing with these new appeals.
70. There may have been a moderate underspend in the cost of oversight measures established by the IPA 2016, compared to initial estimates. The two figures currently available (see paragraph 20 for more information) are not directly comparable therefore it has not been possible to conclude that the IPA 2016 has met the Economy test overall. Given that it has not imposed additional significant burdens beyond those estimated in the original IA, it is reasonable to judge that the **Economy test is neutral**.
71. **Efficiency** (relationship between the intended and actual results of public spending, the outcomes – spending well): Efficiency savings are expected from the merger of the existing oversight bodies, as shared resources and knowledge reduce duplication of effort. Efficiency savings are also expected in investigations as law enforcement and public authorities are able to access the data needed as part of their investigations. More efficient outcomes may include increased intelligence packs, arrests, prosecutions, convictions, and criminal assets recovered.
72. The extent of these efficiency benefits cannot be quantified due to a lack of data. Case studies (see paragraphs 60 – 71) reported by the NCA demonstrate, qualitatively, that a range of economic benefits were conferred on society due to the use of ICRs. These benefits take the form of FTE savings, reduced risk of serious and organised crime and enhanced public confidence. This provides limited evidence that some of the intended outcomes of the IPA 2016 may have been realised. While it has not been possible to use monetised evidence that the IPA 2016 has fully met the efficiency test, it is reasonable to judge (given expected economies of scale, efficiency savings and more efficient outcomes) that the actual **efficiency effect is somewhere between neutral and positive**.
73. **Effectiveness** (relationship between the resources used to produce outputs – spending wisely): The IPA 2016 may allow agencies to keep up with constantly evolving technology, allowing them to continue to investigate criminals through, for example, the ICR trial and protect the citizens of the UK effectively. There is some limited qualitative data relating to effective safeguarding of an individual's rights to privacy due to an intervention by a JC. With the caveat that this represents one individual example of safeguarding, this may suggest that the IPA 2016 is, to an extent, **meeting its operational objectives with effective oversight measures** in place.

G. Risks, unintended consequences, PSED impacts and mitigating actions

Unintended consequences

74. Currently, Part 7 of the IPA 2016 requires the agencies to apply the same standard of safeguards to the retention and examination of all BPD regardless of the potential intrusion arising from doing so.
75. Whilst the standard of safeguards set out in Part 7 is appropriate where the retention and examination of a dataset is highly intrusive, Part 7 applies the same safeguards to datasets where retention and examination is substantially less intrusive (for example, datasets containing data that can be freely accessed via the internet or bought commercially). For these datasets the Part 7 safeguards go beyond what is necessary and in doing so prevent UKIC from making best use of the data. For example, the *RMS Titanic* manifest is a commonly used training dataset in the global data science community for Machine Learning development, however, data scientists and engineers within UKIC would be required to obtain a warrant under the double-lock authorisation process

²² The National Audit Office, 'Assessing value for money' - Link: <https://www.nao.org.uk/successful-commissioning/general-principles/value-for-money/assessing-value-for-money/>

before they could retain and/or examine it. Consequently, the Part 7 regime currently hinders UKIC's ability to better develop new capabilities, such as machine learning and artificial intelligence and prevents UKIC from making best use of techniques to allow us to keep pace with wider industry and adversaries.

76. In 2020, in the context of the pandemic, the IPCO annual report identified that Judicial Commissioners might need longer to consider urgent warrants and that there might be a need to temporarily replace the JCs should they be unable to carry out their duties as a result of ill health or other reasons. If there is not a JC available to consider the necessary applications, there is a risk that there will be potential impacts on national security and law enforcement operations.²³ This should be considered in future legislation. The IPCO report also identified a lack of flexibility in the system in various areas:
- The IPC cannot delegate powers in case of emergency and does not have a Deputy.
 - Senior officials are unable to sign off warrant renewals that they did not initially authorise.
 - There is not an alternative procedure for warrants requiring a triple lock (PM sign off) for situations in which the PM is incapacitated or in some cases unavailable.
77. The three points stated above reduce the resilience of the system and results in lower operational agility which could result in inefficiencies and could jeopardise national security in cases of emergency.

Risks

78. There are analytical risks with the assessment presented due to the high degree of uncertainty and limited evidence and data to support a full assessment. Many of the benefits are based on public confidence and there are few monetised benefits in the analysis.
79. There are likely to be very few economic risks as much of the legislation involved a past regime being replicated through the IPA 2016, resulting in no additional costs to industry as a result of this policy from the baseline.
80. Previous risks presented in the initial IAs remain relevant and include:
- There is a risk that technology will continue to evolve and develop rapidly, outpacing legislation.
 - There continues to be a risk that in consolidating existing legislation, criminals and terrorists will be more aware of the security and intelligence agencies, armed forces, and law enforcement capabilities to detect and prevent terrorism and serious organised crime and will take new or additional measures to evade discovery.
 - There continues to be a risk that the IPA 2016 does not fully realise the objective of the policy to improve public confidence in the legislative regime. With the present external influences and no baseline polling, it is difficult to assess whether this risk is reducing.
 - There continues to be the risk that technical solutions will be outpaced by technical change and/or changes in consumer behaviour. This risk is difficult to mitigate and will be present as long as the IPA 2016 relies on technology.
81. There are likely to continue to be analytical risks due to the high degree of uncertainty and limited evidence and data to support a full assessment.

²³ HC 897 – Annual Report of the Investigatory Powers Commissioner 2020 - Link: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf

H. Recommendation (keep, amend, repeal)

82. Although limited evidence is available to assess the impact of IPA 2016, this PIR has identified some areas where the IPA 2016 appears to be meeting its objectives. Where quantitative evidence may be lacking, there are areas where qualitative evidence and feedback from operational partners and stakeholders suggests that the PIR is meeting its objectives. The PIR has also identified some areas where further improvements can be made, drawing on a range of data sources. These include improving the warrant regime under Part 7 of the IPA to remove unnecessary burden on UKIC and clarifying the powers available to judicial commissioners. Future policy intervention may wish to amend these provisions to make the current system more agile and flexible in emergency situations.
83. In conjunction with this document, the Home Secretary has prepared a Statutory Report as per the legal obligations under Section 260 of the IPA 2016. This report has examined the operational effectiveness of the IPA 2016 since its inception and considering challenges posed by technological change and changes in the operational use of data and these powers. It has identified areas where legislative intervention may be necessary to ensure that the Home Office continues to deliver its objectives under the IPA 2016.
84. **The recommendation of this PIR is to consider amendments to the Investigatory Powers Act 2016 legislation, allowing for improved flexibility in the system where needed and ensuring that the powers remain fit for purpose, whilst providing strong oversight and safeguards to ensure powers are used appropriately.**

Specific Impact Test Checklist

Mandatory specific impact test - Statutory Equalities Duties	Complete
<p>Statutory Equalities Duties</p> <p>The IPA 2016 makes clear the circumstances in which various investigatory powers may be used and the strict safeguards that apply, ensuring that any interference with privacy is strictly necessary, proportionate, authorised, and accountable. The regime is overseen by the Investigatory Powers Commissioner and a cadre of Judicial Commissioners This independent oversight ensures that the powers are used in a way that is necessary and proportionate. There is an intentionally high bar for their use. As a result of these strict safeguards, and the nature of the application of the powers, there is not a disproportionate impact on any specific protected groups. Protections have also been afforded by the Investigatory Powers Tribunal which provides a right of redress for anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques.</p> <p>The SRO has agreed these summary findings from the Equality Impact Assessment.</p>	<p>Yes</p>

Any test not applied can be deleted except **the Equality Statement**, where the policy lead must provide a paragraph of summary information on this.

The Home Office requires the **Specific Impact Test on the Equality Statement** to have a summary paragraph, stating the main points. **You cannot delete this and it MUST be completed.**