Investigatory Powers Bill

Privacy Impact Assessment

November 2015

1. Executive summary

This document is the Privacy Impact Assessment (PIA) for the implementation of new measures included in the Investigatory Powers Bill. The purpose of this PIA is to consider the privacy impact of the proposed legislation; and address any issues raised in the regulatory impact assessments covering each policy area.

This Privacy Impact Assessment (PIA) follows the approach and guidelines recommended by the Information Commissioner's Office (ICO). It considers the impact on privacy of the proposed legislation.

This PIA identifies the risks to privacy arising from the powers that will be available under the new legislation, and sets out the safeguards, existing and new, intended to address these risks (section 4). The PIA concludes with a Privacy Impact Statement (see section 5).

This document should be read in conjunction with the Investigatory Powers Bill Impact Assessment; and the standalone Impact Assessments covering each of the measures in the Bill. These documents can be found on the dedicated Investigatory Powers Bill page on the Gov.uk website.

Document references

Ref No.	Title	Document reference
1.	'A Question of Trust: report of the Investigatory Powers Review' David Anderson QC	Available at: https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review
2.	'Privacy and Security', report by the Intelligence and Security Committee of Parliament	Available at: http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf
3.	'A Democratic License to Operate'	Available at: https://www.rusi.org/downloads/assets/ISR-Report-press.pdf

2. The case for legislation

How public authorities use investigatory powers has been the subject of much polarised debate. The Government has been clear about the need for legislation that will provide public authorities with the investigatory powers they need to address evolving threats within a changing communications environment, as well as providing the public with clarity and reassurance about how those powers and capabilities are used.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) was passed in July 2014. It sought to do two things: to provide for the UK's data retention regime following the European Court of Justice decision to strike down the EU Data Retention Directive, and to clarify the application of the Regulation of Investigatory Powers Act 2000 (RIPA) to overseas communication service providers. DRIPA provided for an independent review of investigatory powers to be undertaken by the Independent Reviewer of Terrorism Legislation, David Anderson QC, to inform new legislation.

His report was published on 11 June. Two further comprehensive reviews were undertaken in parallel. The Intelligence and Security Committee of Parliament undertook an inquiry into the UK Agencies' use of intrusive capabilities – in particular, those relating to GCHQ's interception of communications. They published a report of their conclusions in March 2015. A panel convened by the Royal United Services Institute was commissioned to advise on the legality, effectiveness and privacy implications of UK surveillance programmes, to examine potential reforms to current surveillance practices, including additional protections against the misuse of personal data and alternatives to the collection and retention of data in bulk. Their findings were published in a report on 14 July 2015.

All three reports explicitly considered the impact on privacy of the use of investigatory powers and whether the powers available to the state to investigate and prevent crime and protect the public were necessary and proportionate, given that they provide potentially significant intrusion into privacy.

On privacy specifically, David Anderson made the comment:

'However powerful the need for privacy, it is not (as for example, the prohibition against torture) an absolute right. Just as the interests of public safety and law enforcement will sometimes have to give way to the right to privacy, so the right to privacy may need to yield to competing considerations. That is acknowledged in Article 8(2) of the European Convention on Human Rights, which approves interference by public authorities with the right to respect for private life and correspondence in circumstances where that interference is in accordance with the law, necessary and a proportionate method of achieving specified objectives, including the interests of national security, the prevention of disorder or crime and the protection of health'

David Anderson, A Question of Trust, page 28

He went on to say:

'*Privacy is a prerequisite to individual security, self-fulfilment and the maintenance of a thriving democratic society. So indeed it is: but each of these things depends more directly still upon the population feeling safe, secure and confident that the criminal law in all its aspects will be effectively enforced against wrongdoers'*.

David Anderson, A Question of Trust, page 40

The Intelligence and Security Committee took evidence as part of their inquiry into the allegations regarding the UK. On privacy, they said:

'*While the Agencies must work to protect our national security, they must do so while upholding our basic human rights. Some rights are not absolute: the right to privacy, for example, is a qualified right – as all witnesses to our Inquiry accepted – which means that there may be circumstances where it is appropriate to interfere with that right. In the UK, the legal test is that action can be taken which intrudes into privacy only where it is for a lawful purpose and it can be justified that it is necessary and proportionate to do so. The question that we have considered in relation to each of the Agencies' capabilities is whether the intrusion it entails is justified and whether the safeguards are sufficient'.*

The Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, page 1.

The Royal United Services Institute also set out their consideration on privacy:

'*The concepts of liberty, security and privacy are central to a number of universal rights outlined by important pieces of twentieth-century treaties and legislation, including the Universal Declaration of Human Rights 1948, the European Convention on Human Rights (ECHR) 1950, and the UK Human Rights Act 1998. Article 5 of the ECHR sets out a combined right to liberty and security of each person; Article 8 sets out a right to privacy for each person. These rights are not seen as absolute or unconditional, but rather as qualified rights. This qualification - that these rights are in turn subject to other rights – is important if these rights are to be consistent, balanced and mutually reinforcing. Each right must be protected and respected, to the greatest extent possible, but it cannot exist in isolation. There is no privacy without respect for security; there is no liberty without respect for privacy, security requires both certain liberties and privacy. It is therefore unfruitful (and therefore misleading) to cast debates about privacy, liberty and security as a matter of choice or 'balancing' between these rights, still less to think of trade-offs between these rights'*

The Royal United Services Institute Panel of the Independent Surveillance Review: A Democratic License to Operate: Report of the Independent Surveillance Review, page 29

They went on to say:

'*Rights can only be curtailed under certain conditions: firstly, to secure other rights or protect other public interests; secondly, where the consequent restrictions on each right are proportionate; and thirdly, if the specific ways of adjusting rights one to another are lawful. It follows that measures taken by the government to protect rights to personal security will sometimes limit either liberty or privacy (or both) for some. However, the security of the state is not, in itself, a legitimate constraint on the rights of individuals. The security measures taken by states – from surveillance to policing investigation, from data collection to data mining – are legitimate only insofar as they contribute to respecting the rights of persons, such as the right to life.*'

The Royal United Services Institute Panel of the Independent Surveillance Review, A Democratic License to Operate: Report of the Independent Surveillance Review page 30.

The Government believes in the right to privacy. It is committed to providing strong legal protections to uphold this right. It is also committed to providing a safe and secure environment in which privacy can thrive.

The public and Parliament deserve legislation that provides adequate protection for both their privacy and their security. They should be able easily to understand and access the laws governing how public authorities collect, store, access and use their information.

All three reviews agreed that the powers currently available to law enforcement and the security and intelligence agencies remain essential. Collectively they recommended reforming the oversight regime and increasing safeguards and openness.

The use of investigatory powers in the UK is already governed by one of the strongest legal and regulatory frameworks in the world. But communications technology continues to evolve rapidly, as does the nature of the threats and challenges we face. Investigative tools and techniques have adapted to meet these challenges, but the law has been updated ad hoc to accommodate new practices.

Investigatory powers cover a wide range of activity. Law enforcement make use of investigatory powers to collect evidence and pursue criminal investigations, support arrest, seizures and prosecutions. This may involve the use of communications data or the power to seize a mobile phone. Investigatory powers are used to acquire covert intelligence using sensitive capabilities to stop terrorists and serious criminals. They are used to identify threats to the UK from overseas and to establish links between suspects in the UK. This includes powers to collect data in bulk to discover threats; to join the dots between individuals and groups in national security investigations; to understand a suspect's behaviour and connections; and for cyber defence to protect the UK from foreign attack. Investigatory powers are used to acquire information to

trace where a missing or vulnerable person might be, to intervene or to rescue someone at risk of suicide or harm.

The powers are essential to tackle child sexual exploitation, to dismantle serious crime cartels, to get drugs and guns off our streets and to prevent human trafficking. Legislation is needed to ensure these powers remain available to law enforcement, the armed forces and the security and intelligence agencies so that they can continue to carry out their most essential function; to protect the public.

These powers are some of the most sensitive and closely scrutinised. The current system of oversight provides multiple checks and balances: rigorous internal procedures; a requirement for warrants to be signed by Secretaries of State; inspections by judicial Commissioners; Parliamentary oversight; redress for individuals via an individual Tribunal.

The three judicial Commissioners with oversight responsibilities under the current model are the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner. They have access to the information and internal processes of public authorities and departments, to undertake rigorous inspection of their compliance. They provide annual, published reports on the powers they oversee.

David Anderson said in relation to the Interception of Communications Commissioner in particular:

'*IOCCO employs nine experienced and technically skilled inspectors… who were given access without reservation not only to all the material they requested but to the Agencies' own systems and to the processes of the warrant granting department [WGD] that assists each relevant Secretary of State…. The Commissioner's latest report sets out the manner in which IOCCO inspected every aspect of the interception process, from compliance with the Interception Code and the previous Communications Data Code to the actual application of individual selection criteria, the retention, storage and destruction of intercepted material, security and administrative safeguards and audit checks carried out by the Agencies. These inspections are by no means whitewashing exercises*.'

However, the independent reports on investigatory powers made recommendations about how safeguards could be strengthened and greater transparency provided in order to give the public greater reassurances that their privacy was being respected.

David Anderson noted:

'*Trust between strangers and within communities itself depends on assurance that the state will afford proper protection both to security and privacy'*. [A Question of Trust, page 246]

The ISC recommended:

'*We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do.*

However, that legal framework has developed piecemeal, and is unnecessarily complicated. We have serious concerns about the resulting lack of transparency, which is not in the public interest.

Our key recommendation therefore is that the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so.

Our Report also contains substantial recommendations about each of the Agencies' intrusive capabilities, which we consider are essential to improve transparency, strengthen privacy protections and increase oversight.' Intelligence and Security Committee of Parliament, Privacy and Security

RUSI recommended:

Ten Tests for the Intrusion of Privacy

1. **Rule of law**: All intrusion into privacy must be in accordance with law through processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.

2. **Necessity**: All intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.

3. **Proportionality**: Intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented.

4. **Restraint**: It should never become routine for the state to intrude into the lives of its citizens. It must be reluctant to do so, restrained in the powers it chooses to use, and properly authorised when it deems it necessary to intrude.

5. **Effective oversight**: An effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials and ministers to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.

6. **Recognition of necessary secrecy**: The 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.

7. **Minimal secrecy:** The 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of its employees) and all other aspects of its work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters

8. **Transparency**: How the law applies to the citizen must be evident if the rule of law is to be upheld. Anything that does not need to be secret should be transparent to the public; not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands.

9. **Legislative clarity:** Relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike.

10. **Multilateral collaboration**: Government policy on intrusion should be capable of being harmonised with that of like-minded open and democratic governments.

Legislation governing investigatory powers will update the statutory framework to ensure it is modern, fit for purpose and achieves the right balance of privacy and security.

3. Overview of the proposed legislation

Legislation will replace the existing statutory scheme with one that is comprehensive and comprehensible. It will bring together all of the powers available to the state to access communications: the use of interception, the acquisition and retention of communications data, the use of equipment interference for the purposes of acquiring electronic communications and other private data, and it will provide the statutory

safeguards and protections for the acquisition and use of bulk personal datasets. It will do so in a transparent way that leaves no doubt about when and how public authorities acquire, store and access information.

Legislation will ensure consistent and effective statutory safeguards and strengthen our already robust oversight regime. It will seek to remove doubt or ambiguity about the sufficiency and efficacy of checks and balances. And it will provide world leading oversight arrangements

An overview of each of the powers included in the Investigatory Powers Bill is set out below:

Interception

The key elements of this power are:

- The Bill will replace the existing statutory regime for the interception of communications, both targeted and in bulk.
- The nine intercepting agencies will retain their ability to intercept the content of communications on a targeted basis for a limited number of purposes.
- The three security and intelligence agencies will retain their ability to intercept communications in bulk to allow the Agencies to discover new targets.
- Bulk interception warrants used to identify threats from outside of the UK will be made subject to enhanced safeguards.
- Safeguards currently provided for in relation to interception under the Wireless Telegraphy Act 2006 will be repealed and provided for within the Bill.

Communications Data

The key elements of this power are:

- The Bill will replace the existing statutory regime for acquisition and retention of communications data, both targeted and in bulk.
- The Bill will set out which public authorities will have access to communications data in the future, permitting bodies to retain powers to access communications data only where a clear case has been made.
- Listed public authorities will retain their ability to request authorisation to acquire communications data on a targeted basis.
- Local authorities will be prohibited from acquiring internet connection records.
- The three security and intelligence agencies will retain their ability to acquire communications data in bulk to allow the Agencies to discover new targets.
- The Bill will revise the definitions of communications data to update them and make them less dependent on the current technological landscape.
- The Bill will provide for the Secretary of State to require communications service providers to retain communications data where it is necessary and proportionate to do so for one or more of the statutory purposes in the BillThe Bill also provides for the retention of internet connection records (the records captured by a network access provider of the internet services with which an

individual device interacts). The retention period must not exceed twelve months.
- The Bill makes it a criminal offence to recklessly or knowingly obtain communications data without lawful authority.
- The Bill repeals the acquisition of communications data under other statutes, including the Telecommunications Act 1984.

Equipment Interference
The key elements of this power are:

- The Bill will replace the existing statutory regime for equipment interference for the purposes of obtaining communications and other private data, both targeted and in bulk.
- Law enforcement agencies will retain an ability to request an authorisation for targeted equipment interference from Chief Constables (or equivalent) – subject to approval by a judicial commissioner.
- The security and intelligence agencies (SIA) will retain an ability to obtain communications and private data through equipment interference, both targeted and in bulk.
- The Bill will prohibit the use of existing powers under the Police Act 1997 and the Intelligence Services Act 1994 to undertake equipment interference for the purposes of obtaining communications and other private data.

The Bill will also provide new statutory safeguards and protections for the acquisition and use of bulk personal datasets, as set out below, in section 4. The Bill will not create a new power, as the power to obtain bulk personal datasets will remain under the Intelligence Services Act.

Further measures are included within the Investigatory Powers Bill that provide additional safeguards and protections, including robust consideration of the necessity and proportionality of intrusion into privacy. This includes changes to the oversight and authorisation of these powers, elaborated in section 4.

Further background information on the measures can be found in the overarching and standalone impact assessments on Gov.uk.

4. Overview of planned safeguards

The UK already has in place a stringent framework of safeguards to protect against privacy and ensure the proportionate use of investigatory powers. Public authorities who make use of investigatory powers are accountable to the judiciary (via the Commissioners), to the courts (via the Investigatory Powers Tribunal), to the Executive (via Secretaries of State) and to Parliament (via the Intelligence and Security Committee and others). This structure, providing multiple points of accountability and oversight, will remain. But it will be strengthened, and improved.

Planned Safeguards

In addition to the current safeguards already outlined, the new legislation will go further in protecting privacy. The new safeguards include:

- The establishment of a new judicial oversight body, the Investigatory Powers Commission, consolidating the existing three judicial Commissioners into a single body reducing opportunity for gaps/overlaps in oversight.
- A double lock authorisation of warranted powers, whereby warrants issued by a Secretary of State are subject to approval by a judicial commissioner before they come into force.
- Ensuring that all powers that result in similar levels of intrusion have consistently robust safeguards.
- Providing a new domestic right of appeal to the Investigatory Powers Tribunal on a point of law.
- Ensuring statutory Codes of Practice cover all powers to acquire communications and private data in the Bill.
- Providing protections against unlawful access to communications or related data that are consistent, backed by a criminal offence.

The Investigatory Powers Commission (IPC) will replace the tripartite structure of judicial oversight and audit of investigatory powers. Currently, the Interception of Communications Commissioner oversees public authorities' compliance with legislation governing interception and the acquisition and retention of communications data. The Surveillance Commissioner oversees the use of other powers, including covert human surveillance, undercover policing and powers under the Police Act, and the Intelligence Services Commissioner oversees the other powers available to the Security and Intelligence Agencies. All of the Commissioners produce annual reports that are publicly available, on the statutory oversight functions that they have. The IPC will consolidate the roles of these Commissioners into a single body, headed by a senior member of the judiciary, the Investigatory Powers Commissioner.

Currently Secretaries of State are responsible for authorising the use of a range of investigatory powers by issuing a warrant: this includes interception of communications by the police and other agencies and interference with property by the security and intelligence agencies. In that decision, the Secretary of State must consider whether the proposed conduct is for a lawful purpose and is both necessary and proportionate before issuing a warrant. This includes assessing the degree of intrusion into the privacy of the subject of the warrant and of any third parties, and whether this is justified. In future, powers requiring warrants will have them issued by a Secretary of State and approved by a judicial commissioner before the warrant comes into force.

The IPC will have technical and legal expertise and a team of inspectors and judicial commissioners. The judicial commissioners will retrospectively scrutinise public authorities' use of investigatory powers, as they do currently, but they will also review Secretary of State authorisations of warranted powers before they come into force.

The IPC will have the power to refer cases where it thinks public authorities have acted in serious error, to the Investigatory Powers Tribunal.

We consider that these new safeguards provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy. These safeguards, along with the protections already in place, are examined in greater detail in section 4 below.

4. Privacy Risks and Mitigation

This section outlines the potential risks to privacy that arise in relation to the policies in the Bill. It sets out the principle safeguards (both new and existing) that will mitigate those risks.

4.1 The risk of infringing on an individual's privacy through interception

Interception – the making available of the content of a communication, such as the text of an email – is an intrusive power and it is rightly subject to strict safeguards, authorisation and oversight. The legislation does not seek to provide public authorities with further powers to intercept communications, so it is not considered to provide further risk to people's privacy.

Continuing Safeguards

As before, interception will remain a power only available to a limited number of public authorities, and for a limited set of statutory purposes: in the interests of national security; for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the United Kingdom; or for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he or she would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

Warrants for interception may only be issued for a period of six months and assessed for the necessity and proportionality of the interception within the organisation, by a senior official in a warrant-granting department, as well as by the Secretary of State and a judicial commissioner.

Bulk interception warrants will be issued by the Secretary of State and approved by a Judicial Commissioner. Additional safeguards will apply to the examination of any material intercepted under those warrants. In future, bulk warrants will include a schedule that specifies the Operational Purposes for which any data acquired under the warrant may be examined. In order to examine the communications of a person in the UK that have been intercepted under a bulk warrant, the Bill will require that a targeted examination warrant is sought from the Secretary of State and approved by a Judicial Commissioner.

The current interception regime includes multiple checks and balances: the current system of inspection by judicial Commissioners, annual reports on the interception of communications by intercepting agencies, Parliamentary oversight by the Intelligence and Security Committee of Parliament and the right of redress for individuals to the

Investigatory Powers Tribunal and, of course, accountability to the courts will all remain.

A statutory Code of Practice for Interception will set out the retention, destruction and dissemination safeguards that apply to intercepted material.

New Safeguards

Warrants for interception must be issued by the Secretary of State including consideration on grounds of necessity and proportionality, and subject to approval by a judicial commissioner before they come into force.

In addition to approval by a Judicial Commissioner, the Bill will state that the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant to intercept an MP's communications. This will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.

Legislation will incorporate the provisions of the Wireless Telegraphy Act 2006 that permit the interception of communications into the new Bill, to make clear that the same levels of authorisation and statutory oversight apply.

Legislation will make clear that when the UK Government solicits the interception of communications by a foreign Government, an appropriate authorisation in the UK must be in force.

The Investigatory Powers Commissioner will have a statutory role in overseeing the use of these powers by law enforcement and security and intelligence agencies, including auditing compliance and providing reports on an annual basis that will be publicly available.

4.2 The risk of infringing on an individual's privacy through acquisition, retention and handling of communications data

The acquisition and retention of communications data – the 'who', 'when', 'where' and 'how' of a communication, but not its content – carries risk to an individual's privacy. The legislation provides for the acquisition of communications data on a targeted basis and in bulk by the security and intelligence agencies. Provision already exists in legislation for this activity, and it is considered there is no further risk to privacy as a result of legislation governing access.

The Bill provides for the retention of internet connection records by communication service providers, to allow law enforcement and the security and intelligence agencies to determine which device connected with which application or internet-based service, at a point in time.

The Bill will provide improved safeguards for the acquisition and retention of communications data.

Continuing Safeguards

Access requests for communications data will need to be communicated through Single Points of Contact (SPoCs) and approved by independent Designated Persons before the requests can be made.

Public authorities will continue to be restricted to the least intrusive category of communications data that is required for their statutory function. When public authorities cannot justify the need for communications data, their powers to acquire it will be removed.

As now, only communication service providers (CSPs) served with a data retention notice will be required to retain specific types of communications data. The maximum period for data to be retained by CSPs will remain twelve months.

Public authorities' compliance with acquisition powers will continue to be audited and annual reports published. The Interception of Communications Commissioner currently fulfils this function.

A Code of Practice will be published, making clear the handling, retention and destruction arrangements that must apply. The Information Commissioner has an ongoing role in overseeing the handling, retention and destruction of data held by public authorities and the protections in the Data Protection Act 1998 apply.

New Safeguards

The legislation will streamline access to communications data so that it can only be obtained under the Investigatory Powers Bill. It will also introduce a criminal offence, carrying a maximum sentence of two years imprisonment, for knowingly or recklessly obtaining communications data from a telecommunications operator or postal operator without lawful authority, to penalize those breaking privacy unlawfully.

The policy will allow for automated systems to process and analyse communications data needed to answer more complex requests where data from different communications services might be required. It will ensure that, after analysis, only the data which identifies the key facts about a communication is passed to a public authority for examination and data irrelevant to the investigation is destroyed.

Local authorities will be prohibited from acquiring internet connection records.

Legislation will require infrequent users of communications data to set up collaborative agreements with more frequent and experienced users to enable shared services and to take advantage of expert advice, in order to authorise requests for communications data.

The role of the Investigatory Powers Tribunal will be extended to cover the retention of communications data, in addition to its current role in respect of the acquisition of communications data.

The Bill will require judicial commissioner approval of communications data requests for the identification of journalistic sources. The Code of Practice will also make clear the considerations that must apply when acquiring the communications data of a sensitive profession.

Under new legislation, there will not be an absolute prohibition on communication service providers from disclosing to their users that they are subject to a communications data request unless it will affect the operation.

4.3 The risk of infringing on an individual's privacy through the use of equipment interference

Law enforcement and the security and intelligence agencies require the ability to interfere with equipment in order to acquire communications and other private data. Equipment interference may include, for example, remote access to a device or terminal to acquire information, or downloading the contents of a mobile device covertly. This is by its nature intrusive, and does carry a small risk of infringing on an individual's privacy. This will be mitigated by ensuring that intrusion is only undertaken where necessary and proportionate.

The Bill consolidates existing powers to interfere with equipment and puts them on a clearer statutory footing. This will provide greater transparency as well as apply greater protections against unnecessary intrusion into privacy.

<u>Continuing Safeguards</u>

Equipment interference will only be available to law enforcement and the security and intelligence agencies, as is the case under existing legislation (the Police Act 1997 and the Intelligence Services Act 1994).

It will remain an offence under the Computer Misuse Act to unlawfully interfere with equipment. This offence applies to everyone, including public authorities who have the power to apply for a warrant.

Bulk equipment interference warrants can only be applied for by the security and intelligence agencies and only for a limited set of statutory purposes: the interest of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom so far as those interests are also relevant to the interests of national security.

Any individual who thinks that equipment interference powers have been used against them unlawfully can apply to the Investigatory Powers Tribunal to review their case.

<u>New Safeguards</u>

Authorisation for equipment interference will require an application for a warrant. Applications will require setting out clearly how the necessity and proportionality requirements have been met.

Warrants requested by the security and intelligence agencies will be authorised by the Secretary of State and subject to approval by a judicial commissioner in the Investigatory Powers Commission before coming into force. Warrants requested by law enforcement agencies will need to be signed off by an authorising officer, and subject to approval by a judicial commissioner in the Investigatory Powers Commission before coming into force.

For equipment interference in respect of MP's communications, there will be a requirement in addition to approval by a Judicial Commissioner, the Bill will state that the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant. This will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.
The Bill also makes explicit the duty those issued a warrant for equipment interference are under, to safeguard the data acquired through equipment interference.

The Investigatory Powers Commissioner will have a statutory role in overseeing the use of this power by law enforcement and security and intelligence agencies, including auditing compliance and providing reports on an annual basis that will be publicly available.

A revised statutory code of practice for equipment interference will set out further guidance on the rules and safeguards that govern the use and handling, retention and destruction arrangements for information obtained by equipment interference.

The safeguards that apply to bulk interception under the Bill will also apply to bulk equipment interference. In particular, before examining the content of a UK person's communications acquired under a bulk equipment interference warrant, the Bill will require that a targeted examination warrant must be sought.

4.4 The risk of infringing on an individual's privacy through the use of bulk personal datasets

The measures within the Investigatory Powers Bill that relate to bulk personal datasets are intended to provide greater safeguards and protections of privacy. The power to acquire bulk personal datasets will remain under the Intelligence Services Act 1994 and the Security Service Act 1989. As the Bill does not provide for new powers, it is considered that there is no greater risk to privacy as a result of policy.

<u>Continuing Safeguards</u>

A statutory Code of Practice, that make explicit the safeguards relating to the usage, handling, retention and destruction arrangements, will be provided for.

The Investigatory Powers Commission will retain the statutory function of the Intelligence Services Commissioner in auditing the compliance of the security and intelligence agencies. This will be included in the annual reports of the Investigatory Powers Commissioner, made publicly available.

Datasets will, as now, be deleted when no longer required.

New Safeguards

The Bill will create a requirement for the security and intelligence agencies to acquire class-based authorisation for the acquisition and use of bulk personal datasets from the Secretary of State. These will only last for six months.

All authorisations issued by the Secretary of State will be approved by a judicial commissioner before they come into force.

The Bill will also introduce a requirement that further authorisation would be necessary in order for the agencies to analyse the most sensitive datasets.

5. Privacy Impact Statement

This Privacy Impact Assessment has been carried out to assess the risks to privacy posed by the work carried out on the basis of the proposed legislation. It is assessed that implementation of the proposed legislation is capable of being fully compliant with relevant domestic and international law.