DON'T SPY ON US

RESPONSE TO THE INQUIRIES INTO PRIVACY AND SURVEILLANCE

September 2015

CONTENTS

Introduction 2

Recommendations 3

No surveillance without suspicion 5

Transparent laws, not secret laws 8

Judicial not political authorisation 10

Effective democratic oversight 12

The right to redress 14

A secure internet for all 16

INTRODUCTION

The Don't Spy On Us (DSOU) campaign was launched on 11 February 2014 following Edward Snowden's disclosures regarding the NSA and GCHQ's surveillance programmes. DSOU is a coalition of leading civil liberties groups defending privacy, freedom of expression and digital rights in the UK and Europe. The campaign called for an inquiry to investigate the extent to which the law has failed to protect privacy, recommending new, wholesale legislation that would place targeted surveillance on a stronger legal footing in line with our six principles: no surveillance without suspicion; transparent laws, not secret laws; judicial, not political, authorisation; effective democratic oversight; the right to redress and a secure internet for all.

Since the launch of the campaign, a series of major inquiries was announced in response to the public and civil society's demand for greater transparency. The main inquiries to report have been:

- The Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework* (12 March 2015) – the ISC report
- Independent Reviewer of Terrorism Legislation, *A Question of Trust – Report of the Investigatory Powers Review* (11 June 2015) – the Anderson report
- Royal United Services Institute, *A Democratic Licence to Operate* – *Report of the Independent Surveillance Review* (14 July 2015) – the RUSI review

Between them, these reviews recommended improving oversight and transparency, implementing judicial authorisation and strengthening the legal framework for surveillance. All have concluded that the law needs wholesale reform – a recommendation first made by DSOU in our policy paper *Reforming Surveillance in the UK*.

This paper outlines where there is now consensus to reform the law in the UK and how this could provide a framework for forthcoming primary legislation.

Parliamentarians can use this report to assess how well the draft Investigatory Powers Bill (due to be published this autumn) has met the key recommendations of these inquiries and ensure that the legislation is fit for purpose during parliamentary scrutiny.

The paper assesses the inquiries' recommendations against the six DSOU principles, which are the key demands of civil society for reform.

RECOMMENDATIONS

1. NO SURVEILLANCE WITHOUT SUSPICION

Mass surveillance must end. Surveillance is only legitimate when it is targeted, authorised by a warrant, and is necessary and proportionate.

A new warrantry system that increases the threshold for authorising surveillance is required.

2. TRANSPARENT LAWS, NOT SECRET LAWS

The Government is using secret agreements and abusing archaic laws. We need a clear legal framework governing surveillance to protect our rights.

The public should be informed of the powers that are available to the intelligence agencies to interfere with the right to privacy, as well as the process for the authorisation of such a power.

3. JUDICIAL NOT POLITICAL AUTHORISATION

Ministers should not have the power to authorise surveillance. All surveillance should be sanctioned by an independent judge on a case-by-case basis.

There needs to be a clear international framework for the accessing and sharing of data between companies and governments. This could be delivered through improvements to the Mutual Legal Assistance Treaty (MLAT) as advised in Sir Nigel Sheinwald's recent report to the Prime Minister, which should be made public.

4. EFFECTIVE DEMOCRATIC OVERSIGHT

Parliament has failed to hold the intelligence agencies to account. Parliamentary oversight must be independent of the Executive, properly resourced, and able to command public confidence through regular reporting and public sessions.

DSOU supports calls for a new independent body to be staffed with technical, legal and investigative experts who have relevant expertise, including in privacy and civil liberties.

The Intelligence and Security Committee (ISC) should report to Parliament not the Executive and be chaired by a Member of the Opposition. It should be empowered to make decisions on reporting and publications and be appropriately funded and staffed.

5. THE RIGHT TO REDRESS

Innocent people have had their rights violated. Everyone should have the right to challenge surveillance in an open court.

The right of appeal should be part of any new surveillance law. The Investigatory Powers Tribunal (IPT) should hold open hearings and there should be the right to appeal the IPT's decisions.

Individuals who are subject to surveillance should be legally notified when there is no risk to jeopardising an ongoing investigation. This should ordinarily happen within 12 months of the conclusion of the investigation, although that 12-month period may be extended in six-month intervals by judicial authorisation. Consideration must be given to how citizens are able to seek redress if they have no means to find out if they have been subjected to surveillance.

6. A SECURE INTERNET FOR ALL

Weakening the general security and privacy of communications systems erodes protections for everyone, and undermines trust in digital services.

The Government should cease breaking encryption standards and undermining internet security; such activity should be explicitly prohibited by legislation.

1. NO SURVEILLANCE WITHOUT SUSPICION

DON'T SPY ON US RECOMMENDS:

MASS SURVEILLANCE MUST END. SURVEILLANCE IS ONLY LEGITIMATE WHEN IT IS TARGETED, AUTHORISED BY A WARRANT, AND IS NECESSARY AND PROPORTIONATE.

Since DSOU first published this recommendation, a number of different terms have been used to describe indiscriminate surveillance, including 'mass', 'bulk' and 'blanket'. We consider these terms to be interchangeable, as the practices they reference all raise the same concerns.

Our surveillance laws must be reformed to end mass surveillance. The Court of Justice of the European Union (CJEU) took a step in the right direction when it struck down the EU Data Retention Directive in April 2014. The High Court ruled the Data Retention and Investigatory Powers Act (DRIPA) inconsistent with EU law on 17 July 2015. Ending mass surveillance should be a key priority for the Government.

Our policy paper *Reforming Surveillance in the UK* recommended that the interception of communications must always be targeted and specific rather than mass and indiscriminate. Our recommendations included the following:

- Remove the distinction between 'internal' and 'external' communications from the threshold criteria for authorising surveillance. Save in exceptional circumstances that are both clearly and narrowly defined, all interception warrants should be targeted at a specific individual or premises. In any event, interception warrants should never be so broad as to allow for indiscriminate surveillance.
- Raise the threshold applied to the interception of communications. Interception should only occur after it is established, on a case-by-case basis, that:

  i. the surveillance is necessary for a legitimate aim, and is proportionate to that aim;
  ii. other less intrusive investigative techniques have been exhausted;
  iii. information accessed will be confined to that reasonably relevant to the investigation, with excess information promptly destroyed or returned; and
  iv. information is only accessible by the specified authority and used for the authorised purpose.
- The procedural safeguards applied to intercepted material should not differ based on an individual's nationality, residence, location or choice of communications service provider.

- Intercepted material provided to the UK by foreign intelligence agencies should be subject to the same protections and safeguards as material intercepted by the UK. The UK should seek and receive assurances that British standards will be complied with when providing intercepted material to foreign partners.

Communications data (metadata) should be afforded the same protection as the content of communications. The retention of metadata should also be targeted and specific.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

DSOU's recommendations have been noted by the independent reviews. All three reviews recommend a new approach to warrantry for the interception and acquisition of communications and related data.

Both Anderson[1] and RUSI[2] recommend new classification for warrants. The ISC[3] report raises concerns about the extent to which 'thematic warrants' are used and the associated safeguards, recommending that they are used sparingly and that the timescale should be shorter than a standard 8(1) warrant.

We welcome these recommendations while continuing to question and oppose the need for any form of bulk collection.

Anderson does not condemn bulk collection in principle and recommends that the agencies should retain their capability to practise bulk collection of intercepted material and associated data, subject to rulings of the courts. Anderson acknowledges cases being brought to the European Court of Human Rights (ECtHR) by a number of DSOU partners who are challenging the lawfulness of bulk interception. Anderson states that it is not his position to offer a legal assessment in these circumstances. However, he does recommend that bulk collection be subject to strict safeguards including:

- judicial authorisation by the proposed Independent Surveillance and Intelligence Commission (ISIC);
- a tighter definition of the purposes for which it is sought, defined by operations or mission purposes;

---

1 *A Question of Trust, Report of the Investigatory Powers Review*, David Anderson Q.C., Independent Reviewer of Terrorism Legislation – published 11 June 2015

2 *A Democratic Licence to Operate – Report of the Independent Surveillance Review*, Royal United Services Institute (RUSI) – published July 14 2015

3 *Privacy and Security: A modern and transparent legal framework*, The Intelligence and Security Committee of Parliament – published 12 March 2015

- targeting at the communications of persons believed to be outside the UK at the time of those communications; and
- the need for a specific interception warrant to be judicially authorised if the applicant wishes to look at the communication of a person believed to be within the UK.[4]

Anderson also calls for a new bulk communications data warrant, which would be limited to the acquisition of communications data.

The RUSI review acknowledges that data retention can be controversial and that the possibility of data being used for purposes other than for which it was collected, violating data protection principles, is ever present, particularly the longer data is held. RUSI's solution to this is improved oversight, regular reviews and, as with Anderson, much more detail to be provided at the point of warrant request.

DSOU is concerned that the Investigatory Powers Bill may seek to extend the scope of the data being retained by ISPs, for example to include web logs. Anderson recommends that this should only happen under the following circumstances: 'a detailed operational case needs to be made out, and a rigorous assessment conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained'.[6] According to his report, this case has not yet been made.

4 Anderson p5
5 RUSI p21
6 Anderson p5

2. TRANSPARENT LAWS, NOT SECRET LAWS

DON'T SPY ON US RECOMMENDS:

THE GOVERNMENT IS USING SECRET AGREEMENTS AND ABUSING ARCHAIC LAWS. WE NEED A CLEAR LEGAL FRAMEWORK GOVERNING SURVEILLANCE TO PROTECT OUR RIGHTS.

The Government must ensure that the laws governing surveillance, and the circumstances in which people may come to be surveilled, are comprehensible to the general public. Unless people are sufficiently aware of the scope and nature of surveillance, they cannot hold the Government to account or uphold their liberty.

In addition to our call to overhaul outdated and obscure surveillance laws, our report made two clear recommendations to improve transparency:

- International arrangements governing the collection and sharing of the results of surveillance must be made public, subject to parliamentary and judicial oversight, and should allow individuals to foresee when they are likely to be subject to surveillance. This requirement should be set out in legislation.
- The Government should publish aggregate information on the number of surveillance authorisation requests approved and rejected in order to increase transparency.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

The RUSI review specifically outlines in Recommendation 20 that urgent improvements are required to expedite the mutual legal assistance treaty (MLAT) process.[7] It strongly supports the recommendations made by Sir Nigel Sheinwald and acknowledges that there is currently insufficient clarity regarding the powers and safeguards governing the exchange of data and intelligence with international partners.

Whilst we have only seen a summary of Sir Nigel's report to the Prime Minister, we are encouraged by the detail in the summary and support the call for greater standardisation of procedure, training and guidance.[8]

7 *RUSI p116*
8 *RUSI p116*

Improving the MLAT system should be considered a high priority in the drafting of any new legislation.

The ISC report acknowledges that the legal framework governing the intelligence agencies' use of intrusive powers requires greater transparency, and that the Government must make every effort to ensure that 'as much information as possible is placed in the public domain'.[9]

Anderson, in the general recommendations, calls for a new law to be written, insofar as is possible, in non-technical language.[10]

These are welcome recommendations, providing an opportunity for the public to understand the powers available to the intelligence agencies and law enforcement to interfere with the right to privacy, and the process for the authorisation of such powers.

At the launch of his review, David Anderson QC, stated: 'The current law is fragmented, obscure, under constant challenge and variable in the protections that it affords the innocent. It is time for a clean slate.'

His report condemned the Regulation of Investigatory Powers Act: 'RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.'[11]

He called for a new law that was comprehensive and comprehensible: 'The new law should repeal or prohibit the use of any other powers providing for interference with communications.'[12]

---

9 ISC report p8
10 Anderson p285
11 Anderson p8
12 Anderson p286

3. JUDICIAL NOT POLITICAL AUTHORISATION

DON'T SPY ON US RECOMMENDS:

MINISTERS SHOULD NOT HAVE THE POWER TO AUTHORISE SURVEILLANCE. ALL SURVEILLANCE SHOULD BE SANCTIONED BY AN INDEPENDENT JUDGE ON A CASE-BY-CASE BASIS.

The campaign has argued that all intrusive, directed and targeted surveillance (including interception, access to communications data, hacking and also the use of human intelligence sources) must be must be subject to prior judicial authorisation by an independent, serving judge.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

Both Anderson and RUSI call for judicial approval of warrants which is wholly supported by DSOU.

Anderson's call for judicial authorisation is bolstered by the recent High Court decision in David Davis and Tom Watson's challenge to DRIPA ([2015] EWHC 2092 (Admin)), which in turn relied on the Court of Justice of the European Union's decision in Digital Rights Ireland (CJEU case no. C-293/12). Both courts concluded that authorisation by a court or independent body must be obtained before data can be accessed.

RUSI's recommendations differ from Anderson's: it recommends that serious crime warrants should always be authorised by a judicial commissioner, but that warrants relating to national security issues should be authorised by the Secretary of State subject to review by a judicial commissioner.[13]

Anderson points out that the UK is the only Five Eyes nation that does not implement judicial prior authorisation of interception warrants. He advises: 'Neither the British public nor the global public can be counted on to take the probity of the Secretary of State on trust'.[14] He also argues that communications service providers, particularly those in the US operating under a judicial warrant system, have concerns about political authorisation in the UK. Anderson reports that one company indicated that judicial authorisation may improve cooperation with requests for data made to companies based outside of the UK.[15]

---

13 RUSI pxvii
14 Anderson p271
15 Anderson p207

Anderson calls for authorisation by judicial commissioners, comprising serving or retired senior judges. However, DSOU believes it would be preferable for warrants to go through the courts and be signed by serving judges to help ensure that surveillance is necessary and proportionate.

Sir Nigel Sheinwald's recent report to the Prime Minister identified ways to take forward the British Government's relationship with service providers and explore how new formal arrangements could improve data access and sharing with companies and governments in foreign jurisdictions. This report has not been published, despite the Prime Minister stating that: 'The Government will be taking forward Sir Nigel's advice, including pursuing a strengthened UK-US Mutual Legal Assistance Treaty (MLAT) process and a new international framework.' [16]

This report should be published without delay so that it can be fully scrutinised should it influence future government policy.

Some UK service providers share data with intelligence agencies in what Anderson refers to as 'a cosy, voluntary relationship', and the review rightly says, 'governments in the UK and elsewhere can no longer expect to conduct surveillance of communications' on this basis.[17] Indeed, many service providers are increasingly uncomfortable with these voluntary arrangements.

Don't Spy On Us shares the view that there needs to be a clear international framework, for example through improvements to the MLAT.

16 *House of Commons: Written Statement (HCWS27) made by the Prime Minister on 11 Jun 2015*
17 *Anderson p204*

4. EFFECTIVE DEMOCRATIC OVERSIGHT

DON'T SPY ON US RECOMMENDS:

PARLIAMENT HAS FAILED TO HOLD THE INTELLIGENCE AGENCIES TO ACCOUNT. PARLIAMENTARY OVERSIGHT MUST BE INDEPENDENT OF THE EXECUTIVE, PROPERLY RESOURCED, AND ABLE TO COMMAND PUBLIC CONFIDENCE THROUGH REGULAR REPORTING AND PUBLIC SESSIONS.

The oversight of the intelligence agencies has been inadequate to date. DSOU recommends the reform of the Intelligence and Security Committee (ISC) in Parliament as well as reform of the offices of the Intelligence Services Commissioner and the Interception of Communications Commissioner.

- The ISC should be reformed so that it is: answerable directly to Parliament; empowered to take decisions on reporting and publication; and appropriately funded and staffed.
- It should have strengthened powers to compel the production of information and witnesses. The chair should be a member of the largest opposition party and the Commons members should be elected not appointed by the Whips.
- The Intelligence Services Commissioner and the Interception of Communications Commissioner should report to Parliament, be insulated from executive influence, be properly resourced and, in the absence of prior judicial authorisation, review ex post facto all surveillance decisions.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

Both RUSI and Anderson go beyond our recommendations and call for a new commissioner body, which it is anticipated would establish better oversight, independence and greater transparency. They differ on their approach as to how this new independent body should be formed and the scope of its responsibilities.

RUSI recommends the creation of a National Intelligence and Surveillance Office (NISO), which would be placed on a statutory footing to guarantee its independence. It should be based outside Whitehall, have a public profile and be led by a senior public official. This body would be responsible for inspection and audit, intelligence oversight, legal advice and public engagement.[18] It would support and assist the Investigatory Powers Tribunal (IPT) and the

18 *RUSI p113*

judicial commissioners, who, under RUSI's recommendation, would be a separate body.[19]

Anderson recommends that the Interception of Communications Commissioner's Office, the Office of Surveillance Commissioners and the Intelligence Services Commissioner be replaced with a new Independent Surveillance and Intelligence Commission (ISIC). This new body would be responsible for the authorisation of warrants by judicial commissioners as well as for certain types of request for communications data.

We support calls for any new, independent body to be staffed with technical, legal and investigative experts who have relevant expertise including in privacy and civil liberties, as suggested by RUSI and Anderson.

With regard to the ISC, RUSI acknowledges the criticisms made of the committee, particularly its 'cosy' relationship with the agencies.[20] RUSI recommends that engagement between the commissioner and the ISC is 'substantially improved' to 'ensure as thorough oversight process as possible'.[21]

The ISC notes that neither the Intelligence Services Commissioner nor the Interception of Communications Commissioner's roles are independent of the Government, as they are appointed by, and report to, the Prime Minister.

DSOU believes it is vital that the commissioners are independent, report to Parliament and that the new oversight body is chaired by a member of the opposition.

The ISC recommends greater resourcing for the commissioners to enable them to look at a much larger sample of authorisations. This is consistent with our own recommendations.[22]

19 *RUSI., p114*
20 *Ibid., p95*
21 *Ibid., p95*
22 *ISC report p116*

5. THE RIGHT TO REDRESS

DON'T SPY ON US RECOMMENDS:

INNOCENT PEOPLE HAVE HAD THEIR RIGHTS VIOLATED. EVERYONE SHOULD HAVE THE RIGHT TO CHALLENGE SURVEILLANCE IN AN OPEN COURT.

The right to redress should be improved through reform of the Investigatory Powers Tribunal (IPT), new legal remedies for the use of unlawful surveillance techniques and, to facilitate this, an end to the bar on the admissibility of intercept evidence in court.

- Adequate remedies should be available for the unlawful access to communications data and the use of other surveillance techniques.
- The IPT should adopt a more open and fairer procedure. This should include: hearings; public hearings, unless the Government demonstrates that secrecy is required in the particular case; evidence should be disclosed and judgments and reasons published unless the Government demonstrates that secrecy is necessary; special advocates should be appointed; and decisions should be subject to appeal.
- To facilitate redress, all evidence, whether gathered through surveillance or intercept, should be admissible in criminal court proceedings in order to allow for full, adversarial vetting of the lawfulness of the surveillance techniques used and type of evidence collected.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

Six of RUSI's recommendations focus on the IPT, including supporting our recommendation that it should hold open public hearings, except where the tribunal is satisfied that private or closed proceedings are necessary in the interests of justice or other identifiable public interest.[23]

RUSI's report also stresses the importance of domestic right of appeal and calls for judicial commissioners to have a statutory right to refer cases to the IPT.[24] The ISC report notes that the President of the IPT has himself recognised that a domestic right of appeal could be accommodated, for example by a senior body such as the Privy Council. The ISC also acknowledges the importance of a domestic right of appeal and recommends that this should be built into any new legislation.[25]

---

23 RUSI p113
24 Ibid., p113
25 ISC p116

Anderson recommends that the new oversight body ISIC be given the power to: 'inform a subject of an error on the part of a public authority or CSP; and inform the subject of his right to lodge an application to the IPT'.[26]

Anderson also recommends that there should be a right of appeal to rulings of the IPT and that the tribunal should be given the same power as the High Court to make a declaration of incompatibility under HRA 1998 s4.[27]

DSOU supports the inquiries' findings that there should be the right of appeal. We believe that individuals who are subject to surveillance should be legally notified when there is no risk to jeopardising an ongoing investigation. This should ordinarily happen within 12 months of the conclusion of the investigation, although that 12-month period may be extended in six-month intervals by judicial authorisation. Consideration must be given to how citizens are able to seek redress if they have no means to find out if they have been subjected to surveillance.

We support RUSI's recommendation that the IPT should hold open hearings and believe that this would increase public trust in the work of the security services.

26 Anderson p303
27 Anderson p305

6. A SECURE INTERNET FOR ALL

DON'T SPY ON US RECOMMENDS:

WEAKENING THE GENERAL SECURITY AND PRIVACY OF COMMUNICATIONS SYSTEMS ERODES PROTECTIONS FOR EVERYONE, AND UNDERMINES TRUST IN DIGITAL SERVICES.

The intelligence agencies have undermined encryption standards and weakened commercial security online which risks undermining the trust essential for key commercial transactions such as online banking. Undermining encryption and online security makes it easier for authoritarian regimes to breach our collective security.

- The Government should cease breaking encryption standards and undermining internet security. Such activity should be explicitly prohibited by legislation.

SUMMARY OF THE INQUIRIES' RECOMMENDATIONS

RUSI acknowledges that encryption is an integral part of internet communication and is necessary to ensure that online transactions remain secure, whilst noting that encryption can impact on policing and national security. While not coming to one clear conclusion RUSI determines that 'in principle' encrypted data should not be 'beyond the reach of law enforcement',[28] yet offers no solution or recommendation as to how that process would or should be legislated or enforced.

DSOU welcomes RUSI's acknowledgement that encryption is an integral part of internet communications.

Anderson states that the power to encrypt communications should exist. However, when it comes to accessing encrypted communications, he recommends that a system where encryption keys are handed over by either individuals or service providers would be far preferable to a system where the state holds master keys to all communications or back doors are inserted.[29]

28 *RUSI p59*
29 *Anderson report p248*

DON'T SPY ON US

Don't Spy On Us is a coalition of the most influential organisations who defend privacy, free expression and digital rights.

We've come together to fight back against the system of unfettered mass state surveillance that Edward Snowden exposed. Right now, the UK's intelligence services are conducting mass surveillance that violates the right to privacy of internet users and chills freedom of expression.

OPEN RIGHTS GROUP

ARTICLE 19

ENGLISH PEN

PRIVACY INTERNATIONAL

BIG BROTHER WATCH