JUSTICE
59 Carter Lane
London
EC4V 5AQ
DX 323 Chancery Lane
(020) 7329 5100
(020) 7329 5055
admin@justice.org.uk
www.justice.org.uk

Rt Hon Sir Malcolm Rifkind QC MP,
Chair,
Privacy and Security Inquiry
Intelligence and Security Committee of Parliament
35 Great Smith Street
London
SW1P 3BQ

10 February 2014

Dear Chair,

Privacy and Security Inquiry – Call for Evidence: Response of JUSTICE

JUSTICE welcomes the determination of the Intelligence and Security Committee that its inquiry into the powers of the security and intelligence agencies to intercept private communications must consider whether the underlying statutory framework which governs such surveillance remains adequate, while balancing the public interest in protecting both individual privacy and public security.

In 2011, JUSTICE published *Freedom from suspicion: Surveillance reform for a digital age*. This report represented the culmination of a major research project for JUSTICE and concluded that the statutory framework in the Regulation of Investigatory Powers Act 2000 ("RIPA") is a wholly inadequate framework for the regulation of surveillance in the digital age. In anticipation of the proposals in the Draft Communications Bill, JUSTICE made a number of practical recommendations for a new surveillance law for the UK.[1] Our recommendations stand. We consider that the need for holistic reform has become more urgent in light of the Snowden revelations about the conduct of the agencies in connection with the Prism/Tempora operations.

Surveillance is a necessary activity in the fight against serious crime. It is a vital part of our national security. It has saved lives. Unnecessary and excessive surveillance, however, destroys our privacy and blights our freedoms. The revelations of 2013 confirm that RIPA has not only failed to check a great deal of plainly excessive surveillance over the last

[1] JUSTICE's response to the Draft Communications Data Bill 2012 can be found here: http://www.justice.org.uk/resources.php/330/draft-communications-data-bill

decade, but, in many cases, inadvertently encouraged it. RIPA was neither forward looking nor human rights compliant. It is badly out of date.

We enclose a copy of *Freedom from suspicion,* by way of JUSTICE's contribution to the Committee's inquiry. A number of our conclusions and recommendations are plainly relevant to the questions which the Committee has committed to consider.

The balance between the individual right to privacy and the collective right to security

JUSTICE is concerned that the Committee should not base its inquiry on a fallacy that surveillance involves a straightforward clash between individual interests – in privacy – and the collective interest served by the operation of surveillance to protect the safety of the public through the prevention and detection of crime and the maintenance of national security. Privacy as a right protects not only the interest of the individual in their own privacy but also its general importance as a public good. A free society is one which respects the individual freedom to live a life without undue interference or scrutiny. In *Freedom from suspicion*, we explore at length the dangers which arise from the false perception of public interest (see Chapter 2).

Is RIPA 'fit for purpose'?

RIPA was neither forward looking nor human rights compliant when it was enacted in 2000.

By 2011, there had been almost 3 million decisions made by public bodies under RIPA yet fewer than 5000 decisions had been subject to judicial approval. The Investigatory Powers Tribunal had dealt with only 1,100 cases in a decade, upholding only 10 complaints. During the short time that the Act has been in force, public confidence in surveillance has been undermined by the disproportionate use of surveillance powers by some public authorities; by the phone hacking scandal and now, the Snowden revelations (See Chapter 1). The time has come for wholesale reform.

We regret that the call for evidence issued by the Committee reflects the out-dated distinction under RIPA between content and communications data. This one example, explored at length in our Report, helps illustrate the inadequacy of RIPA (See Chapter 4). Shifting technology has rendered the distinction between content and what was traditionally understood as "envelope" data arcane. In many cases, the intrusion caused by accessing a person's communication data is as severe as that posed by interception.[2] Nowhere is this more apparent than with regards to the increasingly blurred distinction between traffic data and content in the context of requests for data on internet usage. Details about an individual's search history – for example, time spent exploring services for alcohol and drug abuse support - may reveal highly personal information about a person. Similarly, location data associated with a mobile phone can provide information far beyond a simple fact that two numbers have been involved in a call. That the gathering and interception of this information continues to be treated as peripheral to the right to privacy by RIPA illustrates its continuing failure to adapt to the demands of a digital age.

---

[2] JUSTICE, *'Freedom from Suspicion: Surveillance Reform for a Digital Age',* § 190

JUSTICE is concerned that this outdated distinction should not be used to downplay the impact on individual privacy of the mass collection and retention of data by or on behalf of Government. The retention of data poses an interference with the right to privacy, both in its creation and in the risk that it may be accessed unlawfully or in error. As the Newton Committee reported in 2003, 'there are obvious risks to privacy in keeping information about individuals. The existence of data creates its own demand for access to it from a wide range of bodies for a variety of reasons, mostly unrelated to national security. It also creates the potential for abuse'. Simply because it may be possible for the State to gain access to a significantly greater pool of information about our private lives as a result of this shifting technological and social base does not mean that it necessarily should. We consider that prior to the consideration of the adequacy of the safeguards contained within RIPA, the Committee must first consider whether the gateways to the collection and retention of information are adequate to safeguard against the disproportionate invasion of individual privacy.[3]

Specific recommendations for the reform of parts of the legislative framework

Root-and-branch reform of our existing law on surveillance is needed to provide freedom from unreasonable suspicion and to put in place truly effective safeguards against abuse. We consider that piecemeal reform – and in particular that which seeks to expand the existing powers of the agencies to gather, retain and use information about us all – will be inadequate to provide a modern, effective framework for the regulation of surveillance in a digital age. Not least, public confidence in the effective operation of RIPA is unlikely to be increased by adding yet another layer of complexity or tinkering with an already failing model for oversight and redress. In our view, a number of basic safeguards would lie at the heart of any new statutory framework (See Conclusions):

- The definitions within RIPA are, in the digital age, outdated and artificial. For example, the definition of intrusive surveillance is overly narrow and must be expanded to cover all surveillance likely to constitute a serious interference with privacy (para 244);

- Prior judicial authorisation should be introduced for a significantly higher proportion of surveillance activities. For example, for interception warrants (paras 141 – 143), surveillance warrants (paras 245-246) and for access to communications data made by any public body other than requests for subscriber data made by the agencies, law enforcement agencies and the emergency services or other requests made by those bodies in cases of emergency (paras 190-193);

---

[3] We deal with these concerns at greater length in our response to the Draft Communications Data Bill (See above; paras 21-22). However, we have had the benefit of reading the opinion of Jemima Stratford QC on the proportionality of data collection retention and use under RIPA by the agencies and we share her concern that the statutory framework does not prevent and may encourage disproportionate and unjustified activities incompatible with the right to respect for private life guaranteed by Article 8 ECHR and the HRA 1998.

- Reduce the number of Commissioners with responsibility for oversight of surveillance and revisit the oversight powers of those Commissioners which retain a role. Specifically, we consider that the responsibility for oversight of most surveillance activities should lie with the Chief Surveillance Commissioner working with the Office of the Information Commissioner. Responsibility for oversight of intrusive surveillance should shift from the Intelligence Services Commissioner to the Chief Surveillance Commissioner (para 247);

- The powers and function of the Investigatory Powers Tribunal must be revised. The relevant oversight Commissioner should be required to refer cases for investigation to the Tribunal where the Commissioner reasonably suspects that a public authority has acted unlawfully (para 397);

- The investigative capabilities of the Tribunal should be increased and extended to enable it to undertake proactive investigations which arise from any systemic failings identified or in cases where there are reasonable grounds to suspect the unlawful use of surveillance (para 398);

- The Tribunal should adopt internal procedures designed to increase the opportunity for adversarial testing of relevant evidence, including through the appointment of a standing panel of special advocates to act in any case where an investigation by the Tribunal has identified a case to be answered (para 399);

- The policy of neither confirming nor denying the existence of surveillance should be relaxed sufficiently to enable the Tribunal to adopt fair procedures in any case where the Tribunal is satisfied that there is a serious issue to be determined and that the public interest in the fair administration of justice outweighs that in the continuing secrecy of a surveillance operation (para 400).

JUSTICE is available to answer any further questions about the recommendations in *Freedom from suspicion.* We would be pleased to assist the Committee further with its inquiry in due course.

Yours sincerely,

Angela Patrick
Director of Human Rights Policy

T: 020 7762 6415
E: apatrick@justice.org.uk