**End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland** 

**London, 29 June 2018**

**Introduction**

I would like to express my deep appreciation to the Government of the United Kingdom for its invitation to conduct an official visit. I have met with Government officials, parliamentarians and members of the judiciary, as well as human rights institutions, civil society organizations and academics in London and in the devolved nations of Northern Ireland, Scotland, and Wales. I want to extend my deep gratitude to every person who met with me, for their time and their valuable inputs. I am particularly grateful to have met representatives of the MI5, the MI6 and the GCHQ, despite the difficulty of intelligence agencies to show a public face and openly discuss sensitive aspects of their work.

This statement contains only my preliminary observations. I will submit my final report to the March 2019 session of the United Nations Human Rights Council, and accept submissions from all interested persons and organizations until September 2018.

**1. Surveillance and oversight of surveillance: significant progress since 2015**

Three years ago I had openly criticized the UK’s system of oversight of its intelligent services as “a joke”. In August 2015 I had said “That is precisely one of the problems we have to tackle.” Today, three years down the line, I am pleased to see that people seem to have been listening. Thanks largely to pressure made by civil society, and the conscientious efforts of many officials and concerned members of the UK Parliament, the UK’s oversight regime has been significantly improved.

The problem has been tackled by the development and implementation of the Investigatory Powers Act 2016. This piece of legislation has also been much improved since I called the first draft “worse than scary” back in November 2015. It still remains a subject of controversy, especially with some NGOs and the jury is still out as to whether some of the safeguards that it now offers will completely succeed, but on the whole there can be no doubt that the oversight regime it has established is a significant improvement on what existed before. This includes the establishment of a better resourced Investigatory Powers Commissioner’s Office (IPCO) and the double lock system with the involvement of the equivalent of five full-time Judicial Commissioners who are tasked with reviewing the most sensitive authorization decisions signed off by politicians such as the Home Secretary or the Foreign Secretary.

The Investigatory Powers Act regulates interception and bulk acquisition of communications and other forms of data by intelligence agencies and law enforcement. When it created IPCO as an oversight mechanism it replaced and consolidated the work of previously fragmented oversight authorities and complemented the role of the Intelligence and Security Committee of Parliament and the Investigatory Powers Tribunal. In practice it would seem that the new oversight regime means more inspections by IPCO, more technical expertise available to IPCO, closer attention to renewal procedures for authorization of surveillance and the involvement of retired judges of the greatest integrity in the authorization and review processes.

**a. Necessity, proportionality and bulk powers**

In my meetings with intelligence agencies, police officers and all other public officials, I received a consensus view that the right to privacy needs to be a primary consideration for any decision regarding surveillance measures. All of them understood and appreciated necessity and proportionality as the cardinal principles to be taken into account. The procedures in place both within the intelligence services as within the law enforcement agencies appear to systematically require consideration of the necessity and proportionality of a surveillance measure or operation before it is recommended for authorization as well as its review on the same grounds.

The views I received on the bulk acquisition of data, however, remain more controversial. While many civil society organizations categorically reject any scenario where bulk acquisition may be a proportionate surveillance measure, given the potential impact on the privacy or thousands or millions of persons and the possible availability of less intrusive measures, Government officials remain convinced that certain scenarios warrant the bulk acquisition of data, which might in fact allow intelligence and law enforcement to find the information they need for the prevention of crime with a lesser infringement of privacy: the negative filtering of large-scale information may often greatly reduce the need for one-by-one, human processing of information (more intrusive than algorithm-based processing).

I believe more in-depth evaluation of the surveillance operations authorized under the first few years’ application of the new law is needed to resolve this dilemma, and have recommended that, in due course, the Intelligence and Security Committee (ISC) reviews these cases in order to closely examine the workings in practice of the existing safeguards regarding the use of bulk acquisition with a view to confirming or disproving the necessity and proportionality of such measures.  I would expect such an in-depth evaluation by the ISC to complement the special attention to bulk acquisition which is already being given by IPCO which has inter alia already issued a public consultation about the matter.

**b. Oversight regime: improvements; IPCO; authorization vs approval; resources and review by the same body (“marking their own homework”)**

In the new surveillance oversight regime created by the IPA, there is a “double lock” system, so that all the more sensitive or intrusive requests to conduct surveillance need to be authorized by both a cabinet minister and the Investigatory Powers Commissioner’s Office (IPCO), staffed by technical experts and retired judges. This element of judicial review assisted by a better-resourced team of experienced inspectors and technology experts is one of the most significant new safeguards introduced by the IPA.

The IPCO started its operation in September 2017 and would appear to be on track to be significantly better resourced than the combined strength of the authorities that it replaces. This does not detract however from the need to ensure that it is quickly and sufficiently resourced to enable it to be pro-active in its audit functions especially with a capacity to carry out technology audits at source-code level.  Given a current complement of approx. 50 staff, I would recommend considering expansion by at least 30 additional staff including a strong contingent of technologically competent individuals able and willing to “get their hands dirty” with the nitty-gritty of checking systems deployed by intelligence services and law enforcement agencies.

I remain concerned however about certain possible deficiencies inherent in the new IPA 2016. Before commenting further I would like to make it abundantly clear that I have no reason to doubt the integrity and competence of the leadership and staff of the new Oversight Authority, IPCO. On the contrary, I am very positively impressed by the strenuous efforts they are making in so many areas and look forward to working closely with them in order to be able to take the many good practices that they are developing and share them with other UN member states. My residing concern about the new Oversight Authority therefore is not about the people who staff it or the efficiency with which they are carrying out their job. It would seem to me that the relatively extensive safeguards now provided by UK law are in very good hands indeed.

The residual concern that I have expressed with various UK authorities lies with those parts of the IPA 2016 which impose on IPCO the dual tasks of both authorizing surveillance and then providing oversight of the way that the very same surveillance is carried out.  To many observers, and especially people sitting outside the British isles, this arrangement still smacks of the new UK law creating a position where somebody is expected to be marking his own homework. This is rather undesirable, since justice should not only be done but also seen to be done and this formulation would probably also detract from the ability to utilize the UK system as a model in other jurisdictions especially those where the culture may be different and not sufficiently robust in some key aspects such as judicial independence and integrity. Moreover, the new UK law may be requiring far too much, more than is humanly possible, from what one single Commissioner may provide, whoever the person holding the post may be. However, the proof of the pudding doubtless will be in the eating and I recommend that this aspect of the IPA 2016 be subjected to special attention when the law is reviewed by or after 2021.

Like any other new piece of major legislation the law and the new mechanisms that it establishes will take some time to bed down, and the UK’s review process, one which the IPA already envisages, should ensure that the workings of the current oversight arrangements should be looked at in great detail when seeking areas for improvement. It should be possible to retain the current structures and mission of IPCO as well as the “oversight dividend” obtainable under the present regime and yet further increase credibility both at home and abroad with an enhanced complementary oversight mechanism independent from IPCO. This review and possible improvement of the oversight mechanisms within the IPA is not a process to be rushed but neither is it one to be neglected.

**c. Non-discrimination between nationals and non-nationals on protection of right to privacy**

One of the most positive aspects I have observed during my visit is that the safeguards against arbitrary or unlawful surveillance, apply equally to all persons put under surveillance by the UK authorities, without any distinction based on nationality or residence. I commend this approach and encourage all Governments to follow it, ending any distinction that reserves the protection of the right to privacy to nationals and residents only.

**d. Intelligence sharing**

While international cooperation is an essential tool in the prevention of crime and especially terrorism, any regime of intelligence-sharing among Governments has to ensure it is done with full respect for human rights principles and obligations , including the right to privacy and the principles of legality, necessity and proportionality. This can only be achieved if an adequate oversight system is in place.

However, the detailed provisions of the agreements that the UK Government has in place to share intelligence with other Governments, including the Five Eyes alliance (which comprises the UK, the United States, Canada, Australia and New Zealand), are not transparent to the public, and the Investigatory Powers Act lacks a robust oversight system for intelligence sharing. The Act regulates requests from foreign Governments to exchange intelligence, but does not mention other forms of intelligence sharing, nor does it clearly establish safeguards comparable to those imposed on UK agencies intended to prevent illegal or arbitrary surveillance which should be applied to surveillance activities carried out on or through UK territory by the personnel of allied powers. I would here like to endorse Privacy International’srecommendation to make intelligence-sharing agreements open to public debate and scrutiny, and establish a strong safeguard and oversight system in the Investigatory Powers Act to ensure that intelligence-sharing is subjected to the same standards of privacy-protection. Intelligence sharing must not result in a backdoor to obtain or facilitate for others the  obtaining of intelligence free from domestic safeguards, nor a loophole for foreign Governments with lower standards on the protection of privacy (or other human rights) to obtain intelligence from UK intelligence that could give rise to human rights violations.

**e. Safeguards to avoid facilitation of non-compliant surveillance by allies**

While several important questions have been satisfactorily answered during my visit, I still have some answers outstanding which I hope to receive later during the forthcoming weeks and months. Amongst these, some hark back to the Snowden revelations of the activities carried out jointly by UK and US intelligence agencies. For example, I have asked the Home Office "In a context where the UK is committed to respecting the right to privacy through the various procedures which UK intelligence services are bound to comply with irrespective of the nationality of the target of surveillance, what safeguards are in place to ensure that allies of the UK based in or using facilities in the UK are respecting the same standards?”

**2. International perspectives: GDPR and Brexit**

**a. GDPR: consensus on positive impact on data protection in the UK**

Few issues during my work as Special Rapporteur have received such consensus as the positive impact in the UK (and elsewhere in Europe) of the European Union’s General Data Protection Regulation (GDPR) and the co-packaged Directive on the use of personal data in the criminal justice sector, which entered into force on 25 May 2018. Despite the uncertainties created by the Brexit process, all officials I talked to remain committed to upholding, and even improving, the European Union’s data-protection standards in the UK.

**b. Brexit: uncertainty on information sharing, EUROPOL, Northern Ireland**

The UK’s imminent exit of the European Union creates an undesirable uncertainty in the regime under which the UK law enforcement agencies exchange information with their partners in the European Union. Nowhere has this a more pernicious effect than in Northern Ireland, where LEAs on both sides of the border have greatly benefitted from close cooperation and information sharing. The sooner that an agreement on such matters is finalized the better for all concerned.

**c. LEA compliance with GDPR/Directive**

While Law Enforcement Agency (LEA) representatives acknowledged the beneficial effect of the GDPR/Directive in increasing awareness and re-examination of current practices amongst police officers, concern was raised that the lack of human resources due to cuts in policing budgets since 2010 and the reluctance to destroy records that may possibly eventually prove useful in some public enquiry, may result in a situation where UK police forces may not have the necessary resource envelope required to sift through numerous legacy computer systems and delete all redundant or inaccurate data in line with the various data protection principles including the time-limitation and data quality principles.

**3. Health data**

**a. Decentralized structure and Deep Mind case**

During my visit, I have discussed the data-sharing agreement between Google’s DeepMind artificial intelligence project and the Royal Free London NHS Foundation Trust. The agreement entered into force on 30 September 2015, and allowed DeepMind to obtain and process partial patient records of approximately 1.6 million patients with the purpose of developing new methods of detection, diagnosis and prevention of acute kidney injury. The sharing of the data started in November 2015.

As the investigation carried out by the UK’s Information Commissioner’s Office found out,the Trust initially believed that the data, which was identifiable, was being processed for the purpose of direct patient care. However, the purpose of processing patient data was the clinical safety testing of Streams, the app developed by Google as part of the DeepMind project. Agreements to conduct a privacy impact assessment were only formalized in January and November 2016, months after patient data had already been shared with DeepMind.

The Information Commissioner’s Office concluded that the sharing of patient information between the NHS and DeepMind violated the 1998 Data Protection Act by breaking, among others, the following principles:

* Patients could not reasonably expect that their records would be shared with a private company for testing of a new mobile app, nor were they informed that this would in fact occur.
* The purpose of the information-sharing was not the direct care of the patient, so no implicit consent could be assumed.
* The Royal Free London NHS Foundation Trust was unable to justify that sharing 1.6 million patient records, a high volume of data, was necessary and proportionate for the clinical safety testing of the application.
* As a result of the lack of information, patients were unable to exercise their right to prevent the processing of their personal data by opting out from the program.

Given the problems exposed in the investigation, and the de-centralized nature of the NHS, with hundreds of health trusts and boards in England, Scotland, Wales and Northern Ireland, I have identified a need for clear, strong guidelines on and oversight of any data-sharing agreement entered by the NHS, either at the UK or local levels. Less experienced local health authorities may need additional support and guidance to negotiate data-sharing agreements with global corporations. I therefore very strongly recommend that the preparation and dissemination of such guidelines be carried out at the earliest possible opportunity. While there are benefits to private-public partnerships, all data-sharing must be done with strict respect to the right to privacy of all patients and data-sharing standards including the Data Protection Act. My discussions with the National Data Guardian (NDG), Dame Fiona Caldicott, suggest that the development of such guidelines could be embarked upon as a matter of priority during the next 12-24 months. I further recommend that the process of placing of the Data Guardian’s role on a statutory footing be completed without undue delay, a development which attracts considerable consensus. At the logistical, as distinct from the regulatory level, it is recommended that the NDG’s Office be suitably resourced with a minimum of thirty staff to achieve and maintain the levels of protection and awareness so clearly required. I am pleased to note that the bill that is currently in Parliament to place the NDG on a statutory footing includes provision for an increase in resources, reflecting the important role that of the office.

**b. NHS and “hostile environment”, memorandum between NHS digital and Home Office for immigration enforcement**

During my visit, I have heard the concern of civil society organizations about the effects of a memorandum of understanding between the NHS and the Home Office to share confidential patient information for immigration enforcement purposes (including deportation of persons in irregular status), as part of the policy known as  the “hostile environment” policy. I echo the recommendation made by Dr. Sarah Wollaston, Chair of the Health and Social Care Select Committee of the House of Commons, who called the NHS to immediately stop sharing confidential information of patients under this agreement. The pernicious effect of the agreement on persons needing medical care, including pregnant women requiring prenatal care, has been well documented, not only violating the right to health care of the individuals concerned but also having a negative impact on public health.

In general, personal information obtained by institutions providing basic services (health, education, psychosocial care) should be inaccessible to immigration enforcement authorities in order to avoid a chilling effect that would prevent migrants from accessing services that are essential for the enjoyment of their human rights.

The Minister of State for the Department for Digital, Culture, Media and Sport, Margot James, announced in the Commons on Wednesday 9 May that the Government would be amending the data sharing arrangements between the Home Office (HO) and NHS Digital (NHSD) that facilitated the tracing of individuals for the purpose of immigration control. This restriction took place with immediate effect and the MoU is being revised to set out the new arrangements.

**c. Possibility of GPs selling patients’ data**

In some jurisdictions within the devolved nations the possibility of primary care providers and especially some GP practices selling their patients’ data was raised with me. I have not seen concrete evidence of this happening, nor have such allegations been corroborated, and therefore I am not yet in a position to comment further about this suspicion being founded in fact. I would however recommend erring on the side of caution and advise that deeper investigation into such matters should be carried out in order to properly determine the facts and possibly detect and regulate more adequately the existence of any data handling practices which may be putting patients unduly at risk.

**4. Open data, big data**

**a. Approaches among UK, Wales, Scotland, Northern Ireland Governments: innovation and right to privacy, anonymization**

Many government officials have expressed their belief that open data can be an important driver for innovation and economic growth, and also for the optimization of public services. I have observed varying degrees of awareness on the risks that open data can pose to the right to privacy, and I encourage all Government bodies with a role on open data to carefully assess the privacy risks in any open data policy. That assessment should be an integral part of any strategy, guideline or policy document on open data. Caution should be the guiding principle in order to avoid the disastrous effects that sharing personal information, even after an anonymization processes, can have among the data subjects. I recommend to all UK authorities engaged in big data and open data practices to further engage with my mandate’s work in this area with a view to developing and adopting new guidelines in this sector.

**5. Biometrics, facial recognition**

**a. Facial recognition in law enforcement; “experimental” deployment in South Wales**

Civil society organizations have shared with me their concerns around the deployment of facial recognition technology by the South Wales police. It was reported to me that the use of such technologies not only was felt to be violating privacy but also may have had an important chilling effect on the fundamental right to association.  Some citizens present to events where this technology was deployed reportedly felt intimidated by a police vehicle prominently marked with the legend “Face Recognition”.

In addition to the admitted lack of precision of the technology, I find it difficult to see how the deployment of a technology that would potentially allow the identification of each single participant in a peaceful demonstration could possibly pass the test of necessity and proportionality. Therefore, I strongly recommend to the Government and especially to the police forces concerned to conduct strict privacy impact assessments before the deployment, even under the label of “pilot” or “experimental” use, of technologies potentially affecting the enjoyment of the right to privacy.

**b. DNA database in Northern Ireland**

According to reports I have received, the Police Service of Northern Ireland has a database containing the DNA of up to 150,000 individuals. Given that the population of Northern Ireland is approximately 1.8 million persons, this means around 8% of the population would have their DNA information in the hands of the police, an unusually high number. I would like to support the recommendations made by the Northern Ireland Human Rights Commission with a view that the retention of that data is strictly done based on the principles of necessity and proportionality. Selecting and destroying the samples that are no longer necessary will require the deployment of significant resources, which I recommend the Government to make available so that the database is rationalized as soon as possible. On the other hand, the needs of the new Historical Investigations Unit (HIU), that will investigate crimes and human rights violations committed during the Troubles, should be taken into account in this process, so that the destruction and disposal of DNA material does not jeopardize an effort that could be essential for victims’ right to the truth and accountability in Northern Ireland.

**6. Children**

**a. Privacy of children: corporate collection and use of their data, privacy in the school and family environments**

Children’s right to privacy is an area that is receiving increasing attention by Governments, academics and civil society organizations. I have discussed this issue extensively during my visit, and share the concern that children require increased protection against the collection and use of their personal data by private corporations, as well as strong guidelines for parents’ sharing videos and photos of their children on social media. The use of CCTV in children’s private rooms, as well as in educational facilities, referring here primarily to those systems intended to enable parents to monitor their children, should also be carefully studied. Above all, children need to be heard on their needs and views on their right to privacy. In this sense, I commend the upcoming research by Dr. Sonia Livingstone funded by the Information Commissioner’s Office, which will focus on children’s understanding of digital privacy.

**7. Anti-radicalization measures and privacy: Prevent program**

**a. Impact on Muslims: concerns by SR on freedom of assembly and SR on racism**

During my visit, I have studied the concerns of civil society and other Special Rapporteurs in their recent visits to the UK (Special Rapporteur on the rights to freedom of peaceful assembly and of association in 2017 and the Special rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance in 2018) regarding the Prevent strategy.

My colleagues observed that excessively ambiguous definitions of terms like “extremism”, and loose guidelines to the entities implementing the strategy resulted in arbitrariness and in “crude racial, ideological, cultural and religious profiling”. Furthermore, the encouragement to report any suspicious speech, including in the classroom, created “unease and uncertainty regarding what can legitimately be discussed in public”, possibly pushing individuals to discuss difficult matters in the margins instead of in the public arena, where the healthy exchange of ideas can prevent radicalization.

According to the information gathered in previous visit by my colleagues, some families would even avoid discussing the negative effects of terrorism in their own homes, for fear that their children would talk about it at school leading to possible misconstructions and eventual reporting to Prevent.

Representatives of British Muslims reported to me that Prevent is dividing, stigmatizing and alienating communities. I was to date unable to gather sufficient evidence to substantiate such claims but hereby recommend that sufficient resources be allocated by the UK Government to reinforce the evidence-base as to the precise impact of Prevent and similar measures on privacy and other fundamental rights.

**b. Proposals to criminalization of access to extremist material**

The mediaand civil society organizations have reported the Government’s intent to study the possibility of criminalizing the access to extremist materials online. However, the freedom to access information that is available online should be protected against such proposals becoming too draconian. While international human rights law rightly allows, and obliges, States to prohibit speech that constitutes incitement to hatred and violence, criminal law should be limited to the active producers and divulgers of the information, and not extend it to the receiving end of that information. One should be able to freely browse the internet in private without fear of criminal repercussion as part of the basic enjoyment of the right to privacy and freedom of information, as long as this activity does not actively contribute to further disseminating materials that incite violent and intolerant behavior.

**OVERALL CONCLUSIONS**

While the new set-up may still contain a number of imperfections, the UK has now equipped itself with a legal framework and significant resources designed to protect privacy without compromising security. Given its history in the protection of civil liberties and the significant recent improvement in its privacy laws and mechanisms, the UK can now justifiably reclaim its leadership role in Europe as well as globally. For example, the UK is now co-leading with that tiny minority of EU states which have made a successful effort to up-date their legislative and oversight frameworks dealing with surveillance. This will remain work-in-progress for years to come, during which I look forward to the UK joining the SRP mandate in efforts to raise the level of privacy protection globally through good practices and innovative legislation.

\_\_\_\_\_\_\_\_\_\_\_\_\_

1/ Privacy International, Policy Briefing – UK Intelligence Sharing Arrangements, April 2018 available at <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf>

2/ <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf>

3/ A/HRC/35/28/Add.1, para. 8

4/ A/HRC/35/28/Add.1, para. 13

5/ In this I would like to echo the call made by the Special Rapporteur on the rights to freedom of peaceful assembly and of association, the Special rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance, the Independent Reviewer of Terrorism Legislation, the parliamentary Joint Committee on Human Rights and the United Nations Committee on the Rights of the Child for an independent review of the strategy to assess the human rights impact of the Prevent programme, including the impact on the right to privacy

6/ <https://www.theguardian.com/uk-news/2017/oct/03/amber-rudd-viewers-of-online-terrorist-material-face-15-years-in-jail>; <https://www.ft.com/content/efe6a790-67f4-11e8-b6eb-4acfcfb08c11>