联 合 国 A/HRC/46/37/Add.1

大 会

Distr.: General
22 June 2021
Chinese
Original: English

人权理事会
第四十六届会议
2021 年 2 月 22 日至 3 月 19 日
议程项目 3
促进和保护所有人权——公民权利、政治权利、
经济、社会及文化权利，包括发展权

对大不列颠及北爱尔兰联合王国的访问

隐私权问题特别报告员约瑟夫·卡纳塔奇的报告* ** ***

概要

隐私权问题特别报告员约瑟夫·卡纳塔奇于 2018 年 6 月 17 日至 28 日对大不列颠及北爱尔兰联合王国进行了正式访问。他满意地注意到隐私保护方面的重大改进，尤其是就情报机构和警察部门的监视而言，并建议进一步改革英国法律，以巩固现有和/或新的监督机构的权力。

* 本报告概要以所有正式语文分发。报告正文附于概要之后，仅以提交语文分发。

** 本报告逾期提交，以反映最新动态。

*** 附件中的两个表格原文照发。

Annex

Report of the Special Rapporteur on the right to privacy on his visit to the United Kingdom of Great Britain and Northern Ireland

I. Introduction

A. Starting off

1. The present report was finalized in March 2021 after evaluating the preliminary results of the country visit, as emerging from meetings held during the period on site in the United Kingdom of Great Britain and Northern Ireland from 17 to 28 June 2018 and cross-checking these with follow-up research and developments to date. The benchmarks used for the present report include those detailed in the privacy metrics document released by the Special Rapporteur on the right to privacy, Joseph A. Cannataci.[1]

2. Some of the content of the present report reflects and builds upon findings already published in the end-of-mission statement in June 2018[2] as further validated to 25 February 2021. The report also contains important updates gathered during close monitoring of the situation in the United Kingdom since June 2018.

3. The mandate holder has continued to have a very healthy dialogue with the Government on various matters – most latterly, encryption and the online sexual exploitation of children (November 2020–January 2021). The Government also assisted greatly in the hosting during October 2019 of the International Intelligence Oversight Forum, at Lancaster House in London.

B. Acknowledgements

4. The Special Rapporteur thanks the Government for the open way in which it greeted him and facilitated his visits. Discussions with government officials were held in a cordial, candid and productive atmosphere.

5. The Special Rapporteur likewise thanks civil society, members of the law enforcement and intelligence communities, government officials and other stakeholders who presented him with detailed documentation and organized several meetings with him in order to provide detailed briefings.

6. The Special Rapporteur thanks those members of the Parliament of the United Kingdom and of the devolved governments of Northern Ireland, Scotland and Wales, and their staff members, who met with him and answered several questions, providing insights into issues of primary concern regarding privacy.

[1] Joseph A. Cannataci, "Metrics for privacy – a starting point", available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf. This document was developed during the period 2017–2019 in order to enable the Special Rapporteur on the right to privacy to maximize the number of common standards against which a country's performance could be measured. It was refined at various stages and then changed its status from an internal checklist to a document released for public consultation in March 2019.

[2] Statement to the media by the Special Rapporteur at the conclusion of his official visit to the United Kingdom of Great Britain and Northern Ireland of 17 to 28 June 2018, available at www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E. The two documents should be read together, especially since, for reasons of available space and editing, some observations available in the 2018 text may have been omitted from the present report.

II. Constitutional and other legal protections of privacy

7. The United Kingdom does not have a formal written constitution, and thus there can be no explicit provision recognizing privacy in a national legal system that relies largely on constitutional conventions rather than on a unitary document. Some scholars claim that foundational works on privacy produced in the United States of America were actually based on a misreading of English common law, which historically does not seem to have allowed for a right or tort of privacy. An irony of history is that the United Kingdom was instrumental, through Sir David Maxwell Fyfe and others, in creating the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), yet it did not formally introduce some of those rights into domestic law, including the right to private and family life, until almost half a century later, in the Human Rights Act of 1998.

8. One needs to distinguish between the formal introduction of the more "generic" right to private and family life in 1998 and components or dimensions of the right. For example, the country's first Data Protection Act was introduced in 1984, while decisions of the European Court of Human Rights such as *Malone v. the United Kingdom*, arising out of the British case *Malone v. Commissioner of Police of the Metropolis*, led to privacy-relevant legislation such as that on telephone tapping in the Interception of Communications Act 1985. So, however important in its own right, and in putting the existence of a right to privacy in the United Kingdom beyond any form of reasonable doubt, the 1998 Act did not arrive into a vacuum. Privacy-relevant behaviour and sanctions can be found gradually emerging in the country's statute and case law over the preceding decades, even centuries.

9. The right to free development of personality, as protected by the Universal Declaration of Human Rights in articles 22 and 29 and as explicitly linked to privacy by the Human Rights Council,[3] is not explicitly articulated in British law. Discussion of "personality rights" in the United Kingdom, as in the United States, has largely been limited to the context of the right to one's identity and thus the commercial interest asserted in, for example, images of oneself.

A. Legislation regarding surveillance

10. Although the Special Rapporteur presented a draft legal instrument on government-led surveillance to the Human Rights Council in March 2018, and this may be used as an interim benchmark, there is as yet no universally agreed binding multilateral treaty regulating such matters. United Nations Member States have therefore been very much left to "do their own thing" on safeguards and remedies in the case of State-led surveillance. The British approach to this subject reflects a genuine concern to get to grips with the thorny problem of effective oversight of surveillance. The United Kingdom remains one of a select group of possibly less than 13 countries (out of 193 United Nations Member States) that have made serious attempts to address issues of adequate oversight of surveillance following the Snowden revelations of 2013 and since. The most significant of the legislative interventions is, without doubt, the debate, enactment and implementation of the Investigatory Powers Act 2016. This is treated at some length in the sections below.

11. Since undertaking the country visit in June 2018, the Special Rapporteur has maintained very close scrutiny over developments in the United Kingdom. On occasion, he has not had to wait long for evidence to become available through official (and often through at least partially redacted) reports. Thanks to the litigation instigated by Liberty and other organizations, for example, knowledge of the oversight by the Investigatory Powers Commissioner's Office (IPCO) of the British domestic intelligence agency MI5 during 2019, as mentioned below, was already in the public domain by the time of the Special Rapporteur co-organizing the International Intelligence Oversight Forum, held on 8 and 9 October 2019 in London. The establishment of oversight powers and the appropriate mechanisms were discussed at the Forum, co-hosted by the United Kingdom and the Special Rapporteur.

[3] Human Rights Council resolution 34/7.

Additional progress achieved was also discussed during informal talks held between the Special Rapporteur and senior inspectors of IPCO.

12. The Investigatory Powers Act is not perfect and there are several parts with which the Special Rapporteur is still unhappy, perhaps especially the involvement of politicians in deciding who is placed under surveillance or not. Without questioning the seriousness with which ministers in the United Kingdom take their duties, the system of having politicians involved in signing off on warrants of interception remains inherently open to abuse if a conflict of interest should arise as to who it is being proposed should be put under surveillance. Such decisions are better taken by completely independent third parties, such as the Investigatory Powers Commissioner's Office. To be clear: the exclusion of politicians from such decision-making about surveillance is undoubtedly a difficult decision to take, and would be a historic step for the United Kingdom to take, even if only partially (e.g. for domestic as opposed to foreign intelligence surveillance). Among other things, the issue needs a clear and very detailed answer to the question: "To what extent should an elected Government be directly accountable for the decisions taken about surveillance, both domestic and foreign? Completely or at arms-length?"

B. Surveillance

13. It is important to set the proper context for past and current trends in levels of surveillance. The United Kingdom is a textbook case for the benefits of healthy tensions, especially those that exist between non-governmental organizations (NGOs), elected politicians, independent oversight authorities and career civil servants, including law enforcement agencies and intelligence services. As a result of these tensions, the situation in the United Kingdom continuously reads as one of "two steps forward and one step back", though some commentators regrettably have an inclination to misrepresent the situation as "one step forward and two steps back". The overall result is also a textbook illustration of the oft-repeated statement by the current Special Rapporteur that the governance and oversight of surveillance and the resultant threats to privacy are – and are very likely to remain – a work in progress, thus requiring constant vigilance by all concerned. This is a sector of activity which is characterized by very rapid developments in technologies. As a direct consequence of technological evolution and change, no sooner does society find some kind of a solution to the way that one type of technology is deployed, than a new technological deployment comes along posing another set of risks or variations on previously identified risks. The abstracts from the 2018 and 2019 IPCO reports reproduced below contain irrefutable evidence that technological development is making a huge difference, with – for example – intelligence agencies finding alternative means to covert human intelligence sources to carry out surveillance.

14. The United Kingdom is blessed with some of the finest, hardest-working and most litigious NGOs active on the privacy scene. Organizations such as Privacy International, Big Brother Watch, Liberty and others have played an invaluable role in bringing pressure to bear on the authorities nationally and internationally while also driving up public awareness about privacy risks and remedies. They have succeeded in keeping the Government on its toes while also engaging successfully with the increasingly more powerful oversight authorities, often persuading them to increase transparency about privacy risks and remedies. These NGOs carry out a role which is different from that of a Special Rapporteur and they have the means to carry out actions that a Special Rapporteur is not resourced to do. They are an essential component in the "tensions mix" that characterizes the privacy scene. All this, and more, being said, their militancy is necessary yet sometimes, regrettably, counterproductive. Before, during and after the Special Rapporteur's official visit to the United Kingdom in 2018, there have been meetings with excellent senior officials in NGOs. Yet there are others who did not properly understand the technologies they sought to regulate, and whose ultramilitant stand could potentially damage the credibility of the privacy cause. It would be enormously helpful to the promotion and protection of privacy if some activists made more of an effort to walk a mile in the shoes of the law enforcement agencies and intelligence services tasked with the maintenance of security and public order. This would help make

both expectations and timelines more realistic, gradually substituting mutual antagonism and distrust with increased collaboration and understanding.

15. Discussions about levels of surveillance will be ongoing. Arbitrary word-limit constraints do not allow for the Special Rapporteur to communicate here his current assessment of ongoing surveillance-related debates in the United Kingdom amid allegations on at least three significant subjects, namely law enforcement agencies' use of facial recognition, and of drones,[4] and the current row[5] over surveillance undertaken by the country's Department of Work and Pensions. Accordingly, taking one example of current healthy tensions, in the latter case, who is the public, or the international community and the Special Rapporteur, to believe? Privacy International, which claims that "suspected benefit fraudsters in the United Kingdom are being subjected to excessive surveillance techniques such as being tailed by government officers or identified in CCTV footage",[6] or the Government's Department of Work and Pensions, which counters that "Privacy International's report grossly mischaracterizes the use, and extent, of Department of Work and Pensions powers, which are subject to independent scrutiny. The limited powers that the department does possess are used to prevent and detect potential crime, with surveillance conducted only when the department is investigating potential fraud, and even then only in cases where all other relevant lines of inquiry have been exhausted."?[7] In this case, and indeed all cases, the facts need to be established and continuously assessed against the tests of lawfulness, necessity and proportionality in a democratic society. This also needs to occur in the context of an increasingly mature and nuanced public discussion about the links between privacy and free development of one's personality, with proper consideration being given to Privacy International's Eva Blum-Dumontet when she states: "Surveillance should never be the price anyone has to pay to live with dignity. Especially considering the current context we are going through, and the many deaths that have occurred as a result of people having their benefits cut, it is time for the Department of Work and Pensions to radically rethink how they deliver benefits and for them to become transparent about the algorithms they use."[8]

16. Within six months after the end of the Special Rapporteur's official visit, that is, by the end of 2018, the following key points of progress regarding surveillance could be noted, as summarized by the Investigatory Powers Commissioner in his report for 2018:

(a) 2018 saw the introduction of the "double lock" review, by a judicial commissioner, of approval by a Secretary of State for the use of the most intrusive investigatory powers. This additional safeguard has been introduced without hindering the work of the intelligence or law enforcement agencies;

(b) By the end of 2018, all applications submitted by British intelligence agencies to use intrusive investigatory powers were subject to the double lock;

(c) 2018 saw a decrease in the number of reported serious errors, as compared with previous years;

(d) Advances in technology have assisted the development of new techniques, which themselves can result in a reduction in inappropriate collateral intrusion (the unintentional gathering of intelligence material);

[4] See, for example, "Drones used by police to monitor political protests in England: BLM, Extinction Rebellion and animal rights protests all targeted as forces expand use of drones", available at www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion.

[5] Sarah Marsh, "DWP uses excessive surveillance on suspected fraudsters, report finds: claimants are tailed, identified on CCTV and their social media monitored, Privacy International finds", *The Guardian*, 14 February 2021, available at www.theguardian.com/society/2021/feb/14/dwp-excessive-surveillance-on-suspected-fraudsters-privacy-international.

[6] Ibid.

[7] Ibid.

[8] Ibid.

(e) Intelligence agencies are implementing good human rights safeguards when working with overseas partners, including providing training to local services to ensure that any capabilities provided by an agency are not abused;

(f) Overall, organizations showed good practice in safeguarding legally privileged material;

(g) Law enforcement agencies' use of undercover agents, or "covert human intelligence sources", has gradually declined in the past decade, largely due to the use of other covert tactics to gather necessary information;

(h) Law enforcement agencies' use of directed surveillance (the covert surveillance of a specific individual using non-intrusive means) has increased, highlighting the vital role that surveillance plays in the prevention and investigation of crime.

17. An important development in 2018, which appears to have been fully effective as of March 2019, was the establishment of the Office for Communications Data Authorizations (OCDA). The Investigatory Powers Commissioner is (also) the head of OCDA, and delegates his powers to authorize communications data requests to OCDA authorizing officers, who consider requests for communications data from law enforcement and public authorities and make independent decisions on whether to grant or refuse communications data requests, ensuring that all requests are lawful, necessary and proportionate.[9]

18. Four years down the line from the Investigatory Powers Act coming into force, the Special Rapporteur can find no evidence that substantively contradicts the assessment about surveillance summarized by IPCO in 2020. The following are some of the key points in the 2019 IPCO report, published in December 2020:

(a) The use of covert human intelligence sources by law enforcement agencies has continued to decrease year on year since 2017, falling from 1,958 approvals in 2018 to 1,866 in 2019. Though the number of authorizations for covert human intelligence sources for wider public authorities (public authorities aside from local councils and law enforcement agencies) has increased, from four in 2018 to eleven in 2019, IPCO inspections into the use of covert human intelligence sources by wider public authorities also revealed that while many have the authority to use covert human intelligence sources, they choose not to, and opt to use less intrusive powers to achieve their means;

(b) Serious errors have decreased since 2018. Of the 14 serious error investigations reviewed by the Investigatory Powers Commissioner in 2019, the Commissioner determined that serious harm or prejudice had occurred in four out of the 14 cases;

(c) Since commencing its operations on 26 March 2019, by the end of 2019 OCDA had received 71,610 applications for the use of communications data;

(d) 2019 saw a continuation in trends regarding law enforcement agencies' acquisition of communications data. As with the IPCO findings from 2018, drug-related offences were the most common offence for which communications data were requested;

(e) The Investigatory Powers Commissioner is responsible for overseeing MI5's compliance with its internal policies governing participation in criminality by covert human intelligence sources. In 2019, IPCO inspectors were content that MI5 policies were correctly followed in every case that was inspected;

(f) Her Majesty's Revenue and Customs reported a significant error by covert human intelligence sources in 2019. This was the result of an outdated policy being applied to their interaction with witnesses. Following an internal review by Her Majesty's Revenue and Customs and a follow-up inspection by IPCO, Her Majesty's Revenue and Customs is implementing an extensive retraining and re-education programme;

(g) After a challenge by Privacy International in 2018, the Investigatory Powers Tribunal ruled that Government Communications Headquarters (GCHQ) should review its existing procedures relating to sharing intelligence and bulk datasets under IPCO

[9] The Investigatory Powers Commissioner oversees both the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000.

supervision. To provide oversight that satisfies this judgment, IPCO reviewed the use of bulk data at GCHQ, and has now incorporated the sharing of bulk data with foreign partners into its regular oversight and inspection arrangements;

(h) Following discussions with NGOs, IPCO identified and published, for the first time, a set of statistics in its 2019 annual report to illustrate how the Consolidated Guidance was used in practice by the Ministry of Defence and British intelligence agencies;

(i) Law enforcement agencies' use of property interference, such as where there is a need covertly to interfere with physical property to install a listening device in a person's house, fell in 2019 from 2018, with some law enforcement agencies opting to submit applications for equipment interference instead. Equipment interference, the process by which an individual's electronic equipment may be interfered with to obtain information or communications, has been available to law enforcement agencies since November 2018;

(j) 2019 saw an increase in the number of requests to retain legal professional privilege material. In 2019, 98 requests were submitted and 97 were approved; this is an increase from 77 requests submitted and 76 approved in 2018.

C. Surveillance for purposes of law enforcement

19. The law reform of 2015 and 2016 puts surveillance and the oversight of surveillance for the purposes of law enforcement under the same regime as that for intelligence services. The comments made in the present report with respect to one sector are therefore generally applicable to the other.

D. Surveillance for purposes of national security (domestic and foreign surveillance)

20. The law reform of 2015 and 2016 puts oversight of surveillance for the purposes of intelligence services, whether domestic or foreign, under the same regime as that for law enforcement agencies. The comments made in the present report with respect to one sector are therefore generally applicable to the other.

E. Oversight of agencies carrying out surveillance

21. Before considering the impact of the Investigatory Powers Act on the oversight of surveillance in more detail, it is worth considering the way that oversight was structured in the United Kingdom before the Investigatory Powers Act came into being and highlighting some key changes made. The following table illustrates the five pillars of oversight of surveillance in the United Kingdom.[10]

[10] Partially abstracted and adapted from the not yet updated website of the Investigatory Powers Tribunal, www.ipt-uk.com/content.asp?id=20.

The five pillars of Oversight of Surveillance in the United Kingdom pre and post IPA-2016

Type of Oversight	*Situation pre-IPA 2016*	*Situation post-IPA 2016*
Independent Authorisations for interception of content	Privacy-Intrusive powers should only be exercised upon the authority of a warrant or an authorisation given by a "designated person" with authority to do so. Applications to use these powers must be scrutinised with great care, for they must be granted only if the particular power sought is in all the circumstances: (a) lawfully available; (b) necessary; and (c) proportionate Prior to IPA 2016, the designated person were Ministers of the UK Government, in effect, these would usually be elected politicians, whose independence (not the seriousness with which they undertook such duties) was and remains questionable.	Privacy –intrusive measures such as interception of communications must still meet the tests of lawfulness, necessity and proportionality and they are still given, in the first instance by Ministers of the UK Government. Post-2016, the most intrusive of these are now subject to the double-lock procedure where a decision authorising interception of communication content is reviewed by a Judicial Commissioner, i.e. a retired or serving senior Judge. The questionability of the independence of politicians and the appropriateness of their participation in such decision-making was thus partially addressed by the double-lock system.
Independent Authorisations for access to metadata	There was no independent authorisation for access to metadata. RIPA essentially allowed requests for comms data disclosure to be self-certified within the organisation that was requesting it. This was a practice which was eventually formally found to be inadequately independent by the European Court of Justice in December 2016.	Part 3 of IPA 2016 was introduced to provide a lawful basis Authorisations for obtaining communications data. The powers under sections 60A-85 of the IPA reside in the new Investigatory Powers Commissioner (IPC) created under the IPA who in turn delegates the day-to-day exercise of these powers to the Office of Data Communications Authorisation. (OCDA) which started operations on the 26 March 2019
Independent Specialist Oversight Authority	The Commissioners: The role of many separate Commissioners which existed prior to the reform ushered in by the IPA was to provide oversight of the way in which all public authorities in the United Kingdom carry out covert surveillance. They visited relevant public authorities, interviewed officers who authorize covert techniques, examine paperwork and give advice as to compliance with the law. These techniques were governed by Part III of the Police Act 1997 and Parts II and III of RIPA. The Commissioners, all eminent and very senior judges, included: Interception of Communications Commissioner: responsible for	On September 1, 2017, the offices of Intelligence Services Commissioner and the Chief Surveillance, Interception of Communications were combined into the Investigatory Powers Commissioner's Office (IPCO) who at law appears to be the *primus inter pares* of the Judicial Commissioners entrusted with independent oversight and has a number of specified duties which the other Judicial Commissioners do not have. Section 240 of the IPA abolished the following offices. (a) the Interception of Communications Commissioner, (b)the Intelligence Services Commissioner,

	keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities. (Section 57 RIPA). The Intelligence Services Commissioner: responsible for providing independent judicial oversight of the conduct of the security and intelligence agencies (SIS, also known as MI6, Security Service (MI5), Government Communications Headquarters (GCHQ)) and a number of other public authorities (Section 59 RIPA). Chief Surveillance Commissioner and Assistants: responsible for overseeing the conduct of covert surveillance and covert human intelligence sources (other than the security services) by public authorities. (Police Act 1997 and Sections 62 and 63 RIPA).	(c) the Chief Surveillance Commissioner, (d) the other Surveillance Commissioners, (e) the Scottish Chief Surveillance Commissioner, and (f) the other Scottish Surveillance Commissioners.
Parliamentary Oversight	Intelligence and Security Committee of Parliament. This is a statutory Committee made up of distinguished Parliamentarians who have further responsibility for the oversight of the security and intelligence agencies (MI5, MI6, and GCHQ) and other parts of the UK intelligence community. Their duties include overseeing the agencies' activities, policies, expenditure, administration and operations.	No change
Specialist Judicial Oversight	The Investigatory Powers Tribunal (IPT), as of 2000, replaced the Interception of Communications Tribunal, the Security Service Tribunal, and the Intelligence Services Tribunal.. The Tribunal was established by RIPA Sections 65-69 to consider, and if necessary, investigate, any complaints	The role of the IPT was maintained and extended to specifically include: aa) conduct for or in connection with the obtaining of secondary data from communications transmitted by means of such a service or system;

	made by members of the public who believe that they have been the victim of unlawful action under RIPA, or that their rights have been breached by any unlawful activity under RIPA or wider human rights infringements in breach of the Human Rights Act 1998. The Tribunal then decides if the complaint has been justified, making one of a number of possible Orders.	(bb) the issue, modification, renewal or service of a warrant under Part 2 or Chapter 1 of Part 6 of the Investigatory Powers Act 2016 (interception of communications);", More specifically under Section 243 of the IPA the IPT is explicitly empowered to look into: conduct of a kind which may be permitted or required by an authorisation or notice under Part 3 of that Act or a warrant under Chapter 2 of Part 6 of that Act (acquisition of communications data); (cza) the giving of an authorisation or notice under Part 3 of that Act or the issue, modification, renewal or service of a warrant under Chapter 2 of Part 6 of that Act; (czb) conduct of a kind which may be required or permitted by a retention notice under Part 4 of that Act (retention of communications data) but excluding any conduct which is subject to review by the Information Commissioner; (czc) the giving or varying of a retention notice under that Part of that Act; (czd) conduct of a kind which may be required or permitted by a warrant under Part 5 or Chapter 3 of Part 6 of that Act (equipment interference); (cze) the issue, modification, renewal or service of a warrant under Part 5 or Chapter 3 of Part 6 of that Act; (czf) the issue, modification, renewal or service of a warrant under Part 7 of that Act (bulk personal dataset warrants); (czg) the giving of an authorisation under section 219(3)(b) (authorisation for the retention, or retention and examination, of material following expiry of bulk personal dataset warrant); (czh) the giving or varying of a direction under section 225 of that Act (directions

		where no bulk personal dataset warrant required); (czi) conduct of a kind which may be required by a notice under section 252 or 253 of that Act (national security or technical capability notices); (czj) the giving or varying of such a notice; (czk) the giving of an authorisation under section 152(5)(c) or 193(5)(c) of that Act (certain authorisations to examine intercepted content or protected material); (czl)any failure to— (i)cancel a warrant under Part 2, 5, 6 or 7 of that Act or an authorisation under Part 3 of that Act; (ii)cancel a notice under Part 3 of that Act; (iii)revoke a notice under Part 4, or section 252 or 253, of that Act; or (iv)revoke a direction under section 225 of that Act; (czm)any conduct in connection with any conduct falling within paragraph (c), (czb), (czd) or (czi);”,

22. From the summary table above, it is apparent that the Investigatory Powers Act introduced significant change to the key structures and human resources tasked with oversight of surveillance in the United Kingdom. The table does not purport to represent all significant changes introduced by the Investigatory Powers Act, and especially not the explicit legal basis that the Act gives to bulk powers, which was and remains one of the areas raising most controversy, and which is treated separately in the present report.

23. The next several sections examine the extent to which the reforms in the oversight of surveillance in the United Kingdom wrought by the Investigatory Powers Act can be considered to be successful or at least to travel in the right direction. Before doing so, it is essential to enter an important caveat. One of the very serious concerns the Special Rapporteur has had about all aspects of his mandate, and perhaps especially that of country visits, is the accuracy of his assessments in the context of the paucity and timeliness of the evidence base. The time dimension is an extremely important one and is a recurrent theme in the present report. It would be extremely dangerous and unfair to all concerned if the assessment of the situation of privacy in a given country were simply based on a snapshot taken in ten short days and frozen in time on a particular date. This would be extremely superficial and would not do justice to the situation and all the actors involved. This is even more so in the case of privacy and security, where oversight of intelligence services and other entities involves much classified material, which is understandably and justifiably not

appropriate to be put into the public domain and requires multiple stages of vetting before any of it can be published. This normally means that by the time an oversight agency makes its reports or other findings public, at least one and sometimes even two years have passed since the period reviewed. Credible evidence about the performance of an intelligence agency in terms of privacy protection and safeguards is further complicated by the rapid development of privacy-relevant technologies, and especially by the very recent reform of oversight mechanisms in some countries under review.

24. Moreover, under the best of circumstances (and that is so rarely the case), it takes time to put flesh on the bones of legislative vision. For example, even if a law ushering in strong, privacy-friendly reform is backed by a broad social consensus,[11] it takes time to create and establish the institutions which are the essential prerequisites for oversight. This understandably has an impact on the timing of when one can say that the new or amended law works well or not. It makes a huge difference if a Special Rapporteur visits a country where oversight agencies and other mechanisms have been, for example, gradually developed over four decades since the 1970s, compared to one that is in the throes of a full-fledged revamp and reform of the sector. The United Kingdom falls into the latter category, and especially so as regards oversight of surveillance. There were ad hoc attempts at introducing various forms of oversight in the two decades preceding 2016, but the end result in October 2016 is best characterized as fragmented and weak. A great deal of energy has been devoted to highlighting the less positive aspects of the Investigatory Powers Act, and perhaps insufficient to the earth-shaking change it induced in the creation of IPCO. The latter not only consolidated the functions of – and partially recruited from – the different commissioners previously responsible for various elements of oversight. The creation of IPCO also coincided with the introduction into British law by the Investigatory Powers Act of structured and consistent judicial review of administrative discretion, in matters of authorization of surveillance. This important substantive and logistical dimension actually ushered in a culture change led by the new Investigatory Powers Commissioner, Lord Justice Fulford, who succeeded in promoting "joined-up thinking" inside the newly structured IPCO, something far more difficult to achieve given the fragmented previous arrangement of different commissioners. This is why it is important to place the visit of the Special Rapporteur firmly in the context of a relatively short timeline:

[11] The Investigatory Powers Act 2016 eventually found relatively broad backing in the British Parliament. In March 2016, the House of Commons passed the Investigatory Powers Bill on its second reading by 281 votes to 15, moving the bill to the committee stage. Labour abstained, as did the Scottish nationalists, with the Liberals voting against.

Table 2 – From gestation to implementation: five years of the Investigative Powers Act 2016

2015 November: publication of draft IPA

2016 January: Parliamentary hearings and discussion – Appointment of Joint Committee of House of Commons and House of Lords

2016 March: Joint Committee published its pre-legislative scrutiny report and House of Commons passes IPA Bill in its second reading

2016 August: Report of the Independent Reviewer of Terrorism Legislation is published outlining the further operational case for the use of bulk powers

2016 November: IPA approved by House of Lords and given Royal Assent

2017 March: Lord Justice Sir Adrian Fulford appointed first IPC

2018 June: UN Special Rapporteur on Privacy carries out official visit of UK

2018: Office of Communications Data Authorisations (OCDA) established with Andrew Bailley as CEO

2019 March: OCDA commences operations

2019 October: Sir Adrian Fulford steps down to be replaced by Sir Brian Leveson

2020 March: COVID-19 strikes, requiring that during the year the UK Government takes action to appoint additional Judicial Commissioners to IPCO in order to enable IPCO to function in a situation where most senior judges serving as Judicial Commissioners were confined to their homes on account of their being considered vulnerable persons under lockdown and other pandemic rules

25. Grasping the brevity of this timeline is essential in order to understand many things. The first of these is that when the Special Rapporteur carried out the official country visit in June 2018, the Investigatory Powers Commissioner had been in office for slightly over a year and was only just recovering from the not inconsiderable challenges of putting together a new 50-person-plus organization tasked with overseeing some of the largest and most powerful intelligence agencies in "the West". To mention one logistical issue alone: locating, securing and adapting secure premises in such a short time in any civil service is a tall order. Congratulations are due to the United Kingdom for undoubtedly choosing the right person for the job. What Lord Justice Fulford managed to achieve in the 30 short months that he served as Investigatory Powers Commissioner should not be underestimated. By all accounts, he contributed significantly in establishing its élan and esprit de corps, and left solid foundations for his successor to build upon. Those initial 30 months saw successes such as the building of relationships with the intelligence agencies which were much less adversarial and more collaborative than they could have been. This feat in relationship management was achieved despite admonition to MI5 that no more interception warrants would be granted if it did not get its house in order. The language used in correspondence by Lord Justice Fulford with MI5 is instructive as to the effectiveness of the oversight exercised by IPCO:

> Without seeking to be emotive, I consider that MI5's use of warranted data … is currently, in effect, in 'special measures', and the historical lack of compliance … is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is 'fit for purpose'.

26. The full extent of the efficacy of the oversight system emerged, as often happens in the United Kingdom, thanks to NGO-instigated litigation, on this occasion in 2019. Ben Jaffey, for Liberty, said there were "ungoverned spaces" in MI5's operations where MI5 did not know what it held. In written submissions, Mr. Jaffey said: "Fulford's generic warrant decision notes that warrants were issued to MI5 on a basis that MI5 knew to be incorrect and the judicial commissioners[12] were given false information." Lord Justice Fulford said MI5's description of the problem as "compliance difficulties" was a "misleading euphemism". He stressed that in the absence of improvements, future applications by MI5 for interception warrants would not be approved by the judicial commissioners. The Special Rapporteur was delighted to note this serious failure by MI5 was remedied within 9 to 12 months. On 23 October 2019, the Special Rapporteur was directly advised by IPCO as follows:

[12] The watchdogs.

> Compliance inspections of MI5 complete: The Investigatory Powers Commissioner has now finished a series of targeted inspections of MI5 in the wake of the IT compliance issues identified earlier this year and has concluded that MI5's use of the IT system in question is now fit for purpose.

27. The above is a polite way of saying that the "MI5 data lake" issue had been resolved, and that, with this being confirmed, the Investigatory Powers Commissioner would feel more comfortable in granting interception warrants to MI5. This news was further confirmed in the official IPCO report for 2019, which became available in December 2020. Examining the details made public by IPCO in October 2019, as follows, also gives valuable insights into the inspection process in the oversight of surveillance:

(a) In the wake of IT compliance issues identified earlier in the year, the Investigatory Powers Commissioner has now concluded a series of targeted inspections of MI5.

(b) The Investigatory Powers Commissioner asked a team of inspectors and technical experts to examine the mitigations that MI5 had put in place. This series of inspections lasted six months and led to the Investigatory Powers Commissioner's conclusion that MI5's use of the IT system in question is now fit for purpose.

(c) The Investigatory Powers Commissioner, Lord Justice Fulford, said:

> "MI5 has devoted substantial resources both to the programme of work to fix the compliance problems identified and to service this intensive inspection regime."
>
> "I am confident that MI5's remediation work has secured compliance with the standards required."
>
> "I have been impressed by MI5's reaction to our criticisms, in particular the speed, focus and dedication with which they acted to rectify the situation."

(d) Inspectors spent a total of 48 days over the course of four inspections at MI5 between March and September. The Investigatory Powers Commissioner and his deputy were closely involved throughout, and a member of the Technology Advisory Panel has scrutinized technical aspects of the system inspected.

(e) MI5 has introduced a range of automatic and manual processes to ensure its staff use the technology in a compliant way. Changes have also been made to the technology itself to enforce compliance requirements.

(f) When it released the news on 22 October 2019, IPCO also advised that:

> "Inspectors from IPCO will continue to work with MI5 and other agencies to ensure that all systems have appropriate safeguards, processes and policies in place."

(g) The Investigatory Powers Commissioner is now writing to all organizations that use investigatory powers, requesting them to conduct an internal review and provide assurances on their use of data. This will enable IPCO to determine whether similar issues exist at other authorities. Where necessary, IPCO will support United Kingdom authorities to ensure that all covertly obtained data is handled in compliance with the law, and that this can be appropriately demonstrated.

(h) The Investigatory Powers Commissioner was first made aware of the compliance risks identified by MI5 on 27 February 2019, and issued a statement shortly thereafter. The Home Secretary laid a further written ministerial statement on the issue on 9 May 2019.[13]

28. The United Kingdom also moved towards compliance with the principle promoted by the Special Rapporteur that "what is transferable to other countries should also be subject to oversight". New regulations have been introduced requiring the Investigatory Powers Commissioner to oversee British use of the United Kingdom-United States Bilateral Data Access Agreement. The Agreement, signed by both Governments in October 2019 although

[13] See https://questions-statements.parliament.uk/written-statements/detail/2019-05-09/hcws1552 and https://questions-statements.parliament.uk/written-statements/detail/2019-07-15/HCWS1722.

not yet in force, enables each country's public authorities to access electronic data held by communications service providers in the other country. Access to such data is subject to safeguards set out in domestic legislation, such as a signed warrant. The regulations, introduced on 6 July 2020,[14] amend section 229 of the Investigatory Powers Act 2016, enabling the Investigatory Powers Commissioner to oversee compliance with the Agreement and ensure its proper use.

F. Benchmarks for measuring progress in the United Kingdom and controversy over bulk powers

29. Following his visit in June 2018, the Special Rapporteur received correspondence from a number of NGOs questioning his overall positive assessment of developments in the United Kingdom. This section encapsulates the gist of his response and should be self-explanatory.

30. The benchmark for measuring progress in the United Kingdom, used by the Special Rapporteur, was not how much the Investigatory Powers Act had improved from when the first draft was published in November 2015, but rather how much progress had been made in effective oversight in the United Kingdom since August 2015 when he had described its oversight system as "a joke" and even as "a bad joke at its citizens' expense". Without doubt, the new system being introduced through the creation and resourcing of IPCO (a by-product of the Investigatory Powers Act) has resulted in the United Kingdom having a more vigorous, robust and effective oversight regime in October 2018 and in April 2021 than it had in October 2015. The Special Rapporteur asked the NGOs the following questions about life before IPCO and life since IPCO:

(a) How many full-time equivalent staff were dedicated to independent oversight in the United Kingdom in October 2015 and how many are there in October 2018, and how many more are expected to be in post by 2019–2020?

(b) How many of the full-time equivalent staff were dedicated to authorization, how many were dedicated to inspection and how many were dedicated to ex post review in 2015 and how many are dedicated to authorization, inspection and ex post review in 2018, and how many are expected to be in post by 2019–2020?

(c) How many times a week or a month did an inspector sit down in a sealed-off security access room with a judicial commissioner and/or a technical expert in 2015 and how many times has this happened in 2018 or 2021? Where there is a substantial difference, is this not at least partially due to the legal reforms of 2015 and 2016, imperfect as they may be?

(d) Was there any form of oversight of a privacy-intrusive decision by a politician in 2015 and is there a form of judicial oversight of the most intrusive of such decisions in 2018? The Special Rapporteur had, in June 2018, counted at least 15 part-time judicial commissioners – after asking for their terms of service, he calculated their work as being approximately equivalent to that of five full-time senior judges – whose job it is to double-check that which was never checked before from a judicial point of view. So the whole point of adding significant judicial oversight to the executive oversight existing previously, through the double-lock scheme, seems to have bolstered the number of judicial commissioners coming through or expected to come through the system.

(e) Is IPCO free to go into the electronic systems within the agencies and check on things directly at will, using technical means not available in the past, and does it now have the human resources as well as the legal powers to do so?

(f) How many actions by the intelligence agencies were subjected to real effective oversight (not just in theory) in August 2015 and how many are subjected to it now in 2018?

[14] The Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of functions exercisable under the Crime (Overseas Production Orders) Act 2019) Regulations 2020.

(g) Has the Regulation of Investigatory Powers Act 2000, declared disproportionate by the European Court of Justice on 21 December 2016, and since replaced by the Investigatory Powers Act, not given way to a system where any request for use of bulk powers previously subjected exclusively to executive review is now also subject to judicial review?

(h) Are the officers responsible for privacy and data protection within the intelligence agencies and the police aware of the above seven safeguards and do they take them into account for internal sign-off and/or when applying for any type of warrant or other permission required under the Investigatory Powers Act or other legislation or jurisprudence? Does this mean that a considerable level of privacy protection is "baked into" the procedures at the executive level before they are subjected to the scrutiny of the ministerial advisers, the Secretary of State, IPCO and the judicial commissioners?

31. The answers to the above questions do not mean that the Investigatory Powers Act is perfect or very good, but in 2018 the Special Rapporteur asked: "Were the above safeguards, especially in paragraph 30 (a)–(h) above, in place and working three years ago when the first mandate started?"

32. As the operator of the largest signals intelligence and other intelligence services in Western Europe, the United Kingdom appears to be finally beefing up its oversight regime to provide resourcing capable of meeting the task of ensuring that interference with privacy is only permitted if necessary and proportionate in a democratic society.

33. The Special Rapporteur characterizes his current thinking on bulk powers as being mostly along the lines articulated by the European Court of Human Rights based on his readings of two 2018 judgments in *Big Brother Watch and others v. the United Kingdom* (13 September 2018) and *Centrum för Rättvisa v. Sweden* (19 June 2018). Neither of these judgments found bulk powers to be, by definition, incompatible with the human rights standards established under European law, and, to date, neither has the Special Rapporteur.

34. It should be noted that the Special Rapporteur's base position remains as stated in his 2016 and 2017 reports to the Human Rights Council and the General Assembly, that is, if at all possible, bulk acquisition should not occur. This is also reflected in the draft legal instrument on surveillance, version 0.7, at lines 654–656. The Special Rapporteur's position is "privacy by default" as 'well as "privacy by design". And, from this foundation, his default position would understandably be "no bulk acquisition".

35. Bulk powers are not something that the Special Rapporteur is terribly comfortable with. Their use would, in many cases, appear to be prima facie disproportionate, and he would have written the British law differently, outlawing their use, unless and until certain very specific conditions apply and adequate safeguards kick in. This is another way of saying that his default position is that "for many normal situations required by intelligence, no bulk powers should be used". This is not the same as saying, however, that bulk powers should never, under any circumstances, be used, or that they are incompatible with European human rights norms or indeed with the United Nations human rights framework. He would prefer them not to be used, and would try hard to see if alternative, less privacy-intrusive measures would achieve satisfactory results, but, if persuaded that bulk powers are the only way in given circumstances and that they are necessary to detect, prevent, investigate or prosecute a serious crime such as terrorism, and also all the possible and imaginable safeguards are put in place to prevent abuse of bulk powers and to minimize risk and collateral damage to individual citizens, then his mind admits the possibility of relatively exceptional circumstances where the use of bulk powers under the strictest conditions may possibly be compatible with the standards of European and indeed global human rights law principles. What upset the Special Rapporteur most about the position of the then British Government was the apparent willingness to accept bulk as being "the new normal", whereas his emphasis remains that it should be the exception in those cases where well-thought-out arguments persuade the oversight authorities that no other way could provide the same levels of security and investigative efficacy that bulk could afford.

36. The Special Rapporteur is not at all happy with bulk acquisition, as he believes the very collection of personal data, even without analysis, has significant risks for society which should be avoided if at all possible. The Special Rapporteur would be precipitate, though, if

he were to categorically exclude the possibility of any form of bulk powers satisfying the requirements of human rights law. He takes inspiration from the justices of the European Court of Human Rights who went into fine detail (see paras. 340–357 of *Big Brother Watch and others v. the United Kingdom*) as to what kind of safeguards and attention to minutiae they would have expected to see in order to be satisfied that a government agency had properly done its homework on the question of necessity, proportionality and adequate safeguards in a democratic society. The Special Rapporteur directs the reader's attention to the following paragraphs of this decision, since they reflect his more detailed thinking on the subject: 314–320, 356, 357, 384–386, 446 and 447.

G. Privacy laws not directly concerned with government-led surveillance, including on health-related data

37. The United Kingdom possesses one of the most up-to-date and comprehensive regulatory systems for privacy and data protection, having updated its relevant laws. The Data Protection Act 2018, together with the General Data Protection Regulation (of 2021), puts privacy safeguards and remedies in the United Kingdom on par with the currently highest international standards, that is, those established in the European Union's General Data Protection Regulation and the Council of Europe's Convention 108+. Its data protection agency, the Information Commissioner's Office, is one of the best resourced and most respected in the world, and has led several important privacy-protective actions, especially the Cambridge Analytica investigations.

III. Conclusions and recommendations

A. On intelligence oversight, security and surveillance

38. **Three years before his June 2018 official country visit, the Special Rapporteur had openly criticized the British system of oversight of its intelligent services as "a joke". In August 2015, he had said: "That is precisely one of the problems we have to tackle." Three years down the line, in the end-of-mission statement released on 29 June 2018, he stated that he was pleased to see that people seemed to have been listening and that, thanks largely to pressure from civil society, and the conscientious efforts of many officials and concerned Members of Parliament, the oversight regime had 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 the Special Rapporteur 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 which involves the equivalent of five full-time judicial commissioners who are tasked with reviewing the most sensitive authorization decisions signed off on by politicians such as the Home Secretary or the Foreign Secretary.**

39. **The Investigatory Powers Act regulates interception and bulk acquisition of communications and other forms of data by intelligence and law enforcement agencies. When it created IPCO as an oversight mechanism, it replaced and consolidated the work of previously fragmented oversight authorities, enabling IPCO to better complement 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 surveillance authorization by IPCO, newly independent authorization of access to metadata by OCDA, and a significantly**

increased involvement of retired judges of the greatest integrity in the authorization and review processes.

40. **In his meetings with intelligence agencies, police officers and all other public officials, the Special Rapporteur received a consensus view that the right to privacy needed 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 and 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.**

41. **The views that the Special Rapporteur received on bulk data operations, however, remain more controversial. 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. On the other hand, government officials remain convinced that certain scenarios warrant the bulk acquisition of data, which might in fact allow intelligence agencies to find the information they need for the prevention of crime with a lesser infringement of privacy. It has been submitted to the Special Rapporteur that the negative filtering of large-scale information may often greatly reduce the need for one-by-one, human processing of information (which is more intrusive than algorithm-based processing).**

42. **The Special Rapporteur finds that, as soon as a degree of normalcy returns, once immunization and other measures help bring the coronavirus disease (COVID-19) pandemic under control, a more in-depth evaluation of the surveillance operations authorized under the first few years' application of the new law is needed to resolve the dilemma posed by bulk processing. The Special Rapporteur reiterates his recommendation made to the then-Chair of the Intelligence and Security Committee of Parliament that it should, in due course, review these cases. This review should closely examine the workings in practice of the existing safeguards regarding the use of bulk acquisition and processing, with a view to confirming or disproving the necessity and proportionality of such measures. The Special Rapporteur would expect that such an in-depth evaluation by the Intelligence and Security Committee would complement the special attention to bulk acquisition that is already being given by IPCO, which has, inter alia, already held a public consultation about the matter. In the meantime, there is a very important development that has taken place since the Special Rapporteur's visit of June 2018: during 2019, in order to provide oversight that satisfies the relevant judgment of the Investigatory Powers Tribunal, IPCO reviewed the use of bulk data at GCHQ and has now incorporated the sharing of bulk data with foreign partners into its regular oversight and inspection arrangements.**

43. **In the new surveillance oversight regime created by the Investigatory Powers Act, there is a "double lock" system, so that all the more sensitive or intrusive requests to conduct surveillance need to be authorized both by a Cabinet minister and by IPCO, the latter being staffed by technical experts and retired judges. This element of judicial oversight, assisted by a better-resourced team of experienced inspectors and technology experts, is a significant new safeguard introduced by the Investigatory Powers Act.**

44. **IPCO began its operations 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. However, this does not detract from the need to ensure that it is quickly and sufficiently resourced to enable it to be proactive in its audit functions, and especially that it has a capacity to carry out technology audits at source code level. The events since 2018 and the inspections required, for example of MI5 in 2019 and of GCHQ with regard to bulk powers, as documented above, reinforce the preliminary recommendation made by the Special Rapporteur in June 2018 that the IPCO and OCDA staff complement be expanded by at least 30 additional staff members, including a strong contingent of technologically competent individuals. The latter should be able**

and willing to "get their hands dirty" with the nitty-gritty of checking ICT systems deployed by intelligence services and law enforcement agencies.

45. **The Special Rapporteur remains concerned, however, about certain possible deficiencies inherent in the new Investigatory Powers Act, of 2016. Before commenting further, he would like to make it abundantly clear that he has no reason to doubt the integrity and competence of the leadership and staff of the new oversight authorities, IPCO and OCDA. On the contrary, he is very impressed by the strenuous efforts they are making in so many areas and looks forward to continuing to work closely with them in order to be able to take the many good practices that they are developing and share them with other United Nations Member States. His concern about the new oversight authorities therefore is not about the people who staff them or the efficiency with which they are carrying out their job. It would seem to him that the relatively extensive safeguards now provided by British law are in very good hands indeed.**

46. **The residual concern, which the Special Rapporteur has expressed to various authorities in the United Kingdom, lies with those parts of the Investigatory Powers Act that impose on the Investigatory Powers Commissioner the dual tasks of authorizing surveillance or access to metadata and then providing oversight of the way that the very same surveillance is carried out. It is important that things be nuanced further at this stage: IPCO provides the double lock on interception of content through its judicial commissioners, and OCDA deals with communications data. Communications data is the who, where, when and how of a communication, but not the content. In other words, OCDA decides who is to get access to metadata – it could possibly have been given an alternative name along the lines of Office for Metadata Access Authorization. At first reading, this arrangement possibly still smacks of the new UK law creating a position where somebody is expected to be possibly marking his own homework. It is clear that the Investigatory Powers Commissioner is well aware of this danger, at least in terms of perception if nothing else, and, indeed, his 2019 report, published in December 2020, emphasized the setting up of OCDA as a semi-independent entity, but ultimately under his personal jurisdiction. The Investigatory Powers Commissioner, currently Sir Brian Leveson, is the head of OCDA, but he delegates his powers to authorize communications data requests to OCDA authorizing officers and OCDA has its own full-time chief executive. Several years down the line, and after reading and rereading the Investigatory Powers Act several times, the Special Rapporteur keeps asking himself the question: "Is this really the best way to handle matters – that is – to create what are in effect two separate entities, IPCO and OCDA, but which are joined in the person of their overall line manager and internal arbiter, the Investigatory Powers Commissioner? What should – and what does – the Investigatory Powers Commissioner do when IPCO discovers that OCDA was at fault in granting an authorization to access metadata? Put differently: *Quis custodiet ipsos custodes*? Who watches the watchers? One should not need a court action to regularly and periodically review the actions of OCDA. Its procedures, operations and decisions should be subject to regular reviews, some carried out through spot checks and random sampling of case files. IPCO should have the properly qualified staff, who have clearance to carry out this task of oversight over OCDA, but even if this is done properly, it is possible there will be occasions where OCDA will be found to be at fault. It seems odd that in such cases, the head of IPCO – the Investigatory Powers Commissioner – would have to take the matter up with the head of OCDA – again, the Investigatory Powers Commissioner. The Special Rapporteur already, in 2018, suggested that the new law may be requiring far too much, more than is humanly possible, from one single commissioner, whoever the person holding the post may be. This is rather undesirable, since justice should not only be done but also be seen to be done, and this formulation potentially detracts from the ability to utilize the British 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 integrity.**

47. **The Special Rapporteur again recommends that the *Quis custodiet ipsos custodes*? aspect of the Investigatory Powers Act be subjected to special attention when the law is reviewed 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**

review process – one which the Investigatory Powers Act already envisages – should ensure that the workings of the current oversight arrangements are 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 Investigatory Powers Act is not a process to be rushed, but neither is it one to be neglected. It may prove advisable to resolve the issue through the creation of a new commissioner known as the Commissioner for Data Access Authorization, responsible for OCDA. A post-2021 review would doubtless examine any advantages derived from cross-fertilization between IPCO and OCDA and especially from the sharing of expertise. One of the practical issues raised with the Special Rapporteur since 2016 on this matter has been the not inconsequential task of finding enough of the right people with the right level of clearance to staff two completely independent organizations. The Special Rapporteur would wish to consider all the evidence available at the time of review before venturing further opinion on the matter. At this moment in time, it should suffice that he is putting the subject on the agenda for future discussion. It may transpire that this is totally what the French would call *un faux problème* and that the current system is fine as it is because it has raised no real conflicts of interest in everyday practice. On the other hand, it could be that current misgivings are well founded and need to be well addressed. The Special Rapporteur would recommend that particular attention be paid to the testimony that past and serving Investigatory Powers Commissioners may care to share during the review process.

B. Eight good practices to take away from the United Kingdom country visit regarding surveillance

48. **The foregoing should illustrate the following summary set of good practices that one can take away from the United Kingdom country visit. The United Kingdom is not unique in setting up effective oversight agencies, but it is one of a very rare few that have achieved so much progress in so short a time period, and from this one can draw the following lessons:**

(a) **If the country's size (i.e. the size of its intelligence services and law enforcement agencies) so permits, reduce fragmentation in oversight of surveillance and consolidate all oversight capability into one, maximum two, truly independent oversight agencies. The United Kingdom has done so, independently though very much in line with the Special Rapporteur's recommendations in his draft legal instrument developed from 2016 to 2018, by creating IPCO and OCDA, though there remains the interrelated question of whether it is sensible to have both IPCO and OCDA answering to the same person and who, in addition to the Investigatory Powers Tribunal, should carry out oversight of IPCO and OCDA.**

(b) **Set up a truly independent oversight agency (or at a maximum, two) which is a specialist agency capable of dealing with all kinds of surveillance, irrespective of whether the surveillance is carried out by law enforcement agencies or intelligence services. This strategy permits more joined-up thinking and the best utilization of scant human resources. The pool from which one can recruit to such an agency is, almost by definition, quite small in any country, and smaller still in some countries.**

(c) **Resource that agency sufficiently and in a timely manner, with the right mix of senior legal judicial skills, senior operational inspection know-how and technological expertise to be able to carry out effective on-site inspections in a large intelligence agency. In the case of an emergency, such as the COVID-19 pandemic, be prepared to quickly take all steps to ensure that key human resources are still available to that agency.**

(d) **Give that agency (or at least one of them, if you have two agencies) the power to grant warrants of interception or other investigatory warrants, and the corollary power to refuse the granting of such warrants.**

(e) **Give that agency (or at least one of them, if you have two agencies) unfettered power of inspection of the entities that it oversees.**

(f) **Improve credibility through transparency, by publishing at least some of the details, the bare bones if nothing else, of the inspections carried out by an oversight agency, including the substantial number of working days merited by the complexity of the task and the seriousness of the matter.**

(g) **Build periodic review of surveillance oversight legislation into the legislation itself.**

(h) **"What is transferable is oversightable" is a principle discussed and further developed during the 2018 International Intelligence Oversight Forum held in Malta. The Special Rapporteur recommends that other States follow the example of the United Kingdom, where its oversight authority (IPCO) reviews the use of bulk data by its signals intelligence agency and other agencies and has now incorporated the sharing of bulk data with foreign partners into its regular oversight and inspection arrangements.**

C. Five good practices to take away from the United Kingdom country visit regarding generic privacy and data protection

49. **The comprehensive review of its privacy and data protection laws undertaken by the United Kingdom provokes reflections about five good practices which should be brought to the attention of other United Nations Member States:**

(a) **Reduce historic fragmentation of privacy-relevant laws by reviewing them and, very preferably, codifying them into one comprehensive law where coherence and consistency are easier to achieve. This approach makes it easier for officials to understand what they need to do to ensure compliance, for companies to understand what is required from them to achieve compliance and for citizens to find the provisions that are intended to protect their privacy. The United Kingdom partially achieved this step through the development and adoption of its Data Protection Act 2018.**

(b) **The Government of the United Kingdom is upfront about which international standards it wishes its national law(s) to comply with, which is refreshing. "The Data Protection Act 2018 is the United Kingdom's implementation of the General Data Protection Regulation", one can read on the Government's own website. Even in an atmosphere riven by the debate over Brexit, there is no hesitation in acknowledging that "a good idea is a good idea is a good idea", wherever it comes from. In this case, the good idea – the comprehensive set of good practices about privacy measures to be taken everywhere except in the national security sector – comes from the European Union, which the United Kingdom voted to leave in 2016 and effectively left as of 31 January 2020. History will be the best judge of whether leaving the European Union was a good idea for the United Kingdom, but at least the country carries the European Union's good ideas about privacy and data protection with it into its future outside the Union.**

(c) **Don't be shy about admitting which international gold standards you wish your national law(s) about privacy to comply with, including those which establish or reinforce standards about protection of privacy in areas that are not covered by the General Data Protection Regulation, such as national security and defence. During their meetings with the Special Rapporteur, British government officials did not hide their laudable goal of trying to ensure that the country's Data Protection Act was also 100 per cent compatible with the updated Convention 108+, the international gold standard in which 70 United Nations Member States are actively involved, and to which 55 are signatories (Convention 108) or are on the way to becoming signatories (Convention 108+). The Data Protection Act is arguably the very first law in the world to be brought**

into line with all the provisions of Convention 108+, in fact, six months before Convention 108+ was opened for signature on October 2018. The standards established by article 9 of Convention 108 and article 11 of Convention 108+, and especially those which require that measures that interfere with privacy must be provided for by law and must pass the tests of necessity and proportionality in a democratic society, are fundamental standards against which British intelligence services and police forces are held on a daily basis. The vigilance of the law enforcement agencies and the intelligence services themselves allies itself with the vigilance of the oversight authorities such as OCDA and IPCO and the vigilance of NGOs to ensure that these international gold standards are met. There will be, from time to time, undoubtedly, instances where they are not met, but eternal vigilance will hopefully remedy that, sooner or later.

(d) **Ensure that your national law provides for a strong, independent data protection authority that is adequately resourced to carry out its mission proactively. The United Kingdom is blessed with the existence of its Information Commissioner's Office.**

(e) **Ensure that your law provides the independent data protection authority with the teeth to carry out its mission effectively. The Information Commissioner's Office applied the maximum penalty against Facebook in the Cambridge Analytica saga but, since that case was handled before the Data Protection Act came into force in May 2018, the penalty applied was nowhere near as prohibitive as could now be applied under the new British law. The deterrent effect of such legislation, enabling sanction as a sizable percentage of global turnover, should not be underestimated. It is one of the chief measures that really makes the corporate world sit up and pay attention. Such a hit to one's bottom line should be avoided at all costs, and privacy protection can only benefit from more attention being paid to the provisions of data protection law.**

D. On privacy and health-related data

50. **The COVID-19 pandemic has provided an opportunity for reflection. Most, if not all, of the issues raised by wearables, the computerization of health records, the related use of artificial intelligence, technology applications in contact tracing, and standards to be respected, even in a pandemic, are addressed by the Special Rapporteur's recommendations on the subject as explained in an explanatory memorandum.**[15] **The Special Rapporteur therefore respectfully draws the attention of the Government to the recommendations on the protection of health data, which he presented to the General Assembly in October 2019. He also urges the Government to reflect about the successes – and failures – in attempts to use applied technologies and especially smartphone apps in efforts to fight the COVID-19 pandemic.**

E. On gender and privacy

51. **During the course of his visit, the Special Rapporteur observed instances where individual and collective experiences of privacy could be determined by gender. He therefore respectfully draws the attention of the Government to his findings and recommendations on gender and privacy, which he presented to the Human Rights Council in March 2020.**[16] **The principles outlined therein should be closely respected and implemented.**

[15] Available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

[16] See A/HRC/43/52.

F. On big data analytics, open data, children and privacy

52. **The Special Rapporteur respectfully draws the attention of the Government to his findings and recommendations on big data and open data, to the recommendations on gender and privacy that he presented to the General Assembly in October 2018**[17] **and October 2017**[18] **and to his findings and recommendations presented to the Human Rights Council on privacy and children.**[19]

G. On the role of the United Kingdom on the international stage

53. **The Special Rapporteur has noted a number of international statements by the United Kingdom on the subject of encryption. He again directs the attention of the Government to the identification of relevant risks, outlined in the paper published by the Government of the Netherlands on 4 January 2016. The Special Rapporteur invites the Government of the United Kingdom to continue the discussions that it is having with his mandate regarding how best to combine regulatory and technical approaches that are designed to address both privacy and security concerns while permitting effective action against criminals. The Special Rapporteur sees the United Kingdom as being especially well positioned to take a leadership role in building bridges with Europe, the United States and other democratic countries around the world in matters concerning privacy, encryption and surveillance.**

[17] See A/73/438.
[18] See A/72/540.
[19] See A/HRC/46/37.