United Nations A/69/397

General Assembly

Distr.: General
23 September 2014

Original: English

Sixty-ninth session
Agenda item 68 (a)
Promotion and protection of human rights: implementation of human right instruments

Promotion and protection of human rights and fundamental freedoms while countering terrorism*

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, submitted in accordance with General Assembly resolution 68/178 and Human Rights Council resolution 15/15.

* Late submission.

14-61490 (E) 021014

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Summary

The present report is the fourth annual report submitted to the General Assembly by the current Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson.

The key activities undertaken by the Special Rapporteur between 17 December 2013 and 31 July 2014 are listed in section II of the report. In section III, the Special Rapporteur examines the use of mass digital surveillance for counter-terrorism purposes, and considers the implications of bulk access technology for the right to privacy under article 17 of the International Covenant on Civil and Political Rights.

I. Introduction

1. The present report is submitted to the General Assembly by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, pursuant to General Assembly resolution 68/178 and Human Rights Council resolutions 15/15, 19/19, 22/8 and 25/7. It sets out the activities of the Special Rapporteur carried out between 17 December 2013 and 31 July 2014. It then examines the use of mass digital surveillance for counter-terrorism purposes, and considers the implications of bulk access technology for the right to privacy under article 17 of the International Covenant on Civil and Political Rights.

II. Activities related to the mandate

2. On 13 February 2014, the Special Rapporteur participated as a speaker in a panel discussion entitled "Debating *Kadi II*: United Nations Ombudsperson v. judicial review in Security Council sanctions decision-making", at the London School of Economics, in London.

3. From 23 to 25 February 2014, the Special Rapporteur participated in an expert seminar on the theme "The right to privacy in the digital age", hosted by the Permanent Missions of Austria, Brazil, Germany, Liechtenstein, Mexico, Norway and Switzerland in Geneva, and facilitated by the Geneva Academy of International Humanitarian Law and Human Rights, in Geneva.

4. On 11 March 2014, the Special Rapporteur presented his report on the use of remotely piloted aircraft, or drones, in extraterritorial lethal counter-terrorism operations, including in the context of asymmetrical armed conflict, and its civilian impact (A/HRC/25/59) to the Human Rights Council at its twenty-fifth session. He also held an interactive dialogue with the Council on his reports on his country visits to Burkina Faso (A/HRC/25/59/Add.1) and Chile (A/HCR/25/59/Add.2).

5. On 12 March 2014, Special Rapporteur participated as a panellist in a side event on the topic "Human rights and drones" and held a press conference at the twenty-fifth session of the Human Rights Council.

III. Counter-terrorism and mass digital surveillance

A. Introduction and overview

6. The exponential growth in States' technological capabilities over the past decade has improved the capacity of intelligence and law enforcement agencies to carry out targeted surveillance of suspected individuals and organizations. The interception of communications provides a valuable source of information by which States can investigate, forestall and prosecute acts of terrorism and other serious crime. Most States now have the capacity to intercept and monitor calls made on a landline or mobile telephone, enabling an individual's location to be determined, his or her movements to be tracked through cell site analysis and his or her text messages to be read and recorded. Targeted surveillance also enables intelligence and law enforcement agencies to monitor the online activity of particular

individuals, to penetrate databases and cloud facilities, and to capture the information stored on them. An increasing number of States are making use of malware systems that can be used to infiltrate an individual's computer or smartphone, to override its settings and to monitor its activity. Taken together, these forms of surveillance provide a mosaic of data from multiple sources that can generate valuable intelligence about particular individuals or organizations.

7. The common feature of these surveillance techniques is that they depend upon the existence of prior suspicion of the targeted individual or organization. In such cases, it is the almost invariable practice of States to require some form of prior authorization (whether judicial or executive), and in some States there is an additional tier of ex post facto independent review. In most States, therefore, there is at least one opportunity (and sometimes more than one) for scrutiny of the information alleged to give rise to the suspicion, and for an assessment of the legality and proportionality of surveillance measures by reference to the facts of a particular case. With targeted surveillance, it is possible to make an objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation.

8. The dynamic pace of technological change has, however, enabled some States to secure bulk access to communications and content data without prior suspicion. Relevant authorities in these States are now able to apply automated "data mining" algorithms to dragnet a potentially limitless universe of communications traffic. By placing taps on fibre-optic cables through which the majority of digital communications travel, relevant States have thus been able to conduct mass surveillance of communications content and metadata, providing intelligence and law enforcement agencies with the opportunity to monitor and record not only their own citizens' communications, but also the communications of individuals located in other States. This capacity is typically reinforced by mandatory data retention laws that require telecommunications and Internet service providers to preserve communications data for inspection and analysis. The use of scanning software, profiling criteria and specified search terms enables the relevant authorities then to filter vast quantities of stored information in order to identify patterns of communication between individuals and organizations. Automated data mining algorithms link common identifying names, locations, numbers and Internet protocol addresses and look for correlations, geographical intersections of location data and patterns in online social and other relationships.[1]

9. States with high levels of Internet penetration can thus gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites. All of this is possible without any prior suspicion related to a specific individual or organization. The communications of literally every Internet user are potentially open for inspection by intelligence and law enforcement agencies in the States concerned. This amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification.

10. From a law enforcement perspective, the added value of mass surveillance technology derives from the very fact that it permits the surveillance of the

[1] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

communications of individuals and organizations that have not previously come to the attention of the authorities. The public interest benefit in bulk access technology is said to derive precisely from the fact that it does not require prior suspicion. The circularity of this reasoning can be squared only by subjecting the practice of States in this sphere to the analysis mandated by article 17 of the International Covenant on Civil and Political Rights.

11. Article 17 of the Covenant provides that any interference with private communications must be prescribed by law, and must be a necessary and proportionate means of achieving a legitimate public policy objective (see paras. 28-31 below). The prevention of terrorism is plainly a legitimate aim for this purpose (see paras. 33 and 34 below), but the activities of intelligence and law enforcement agencies in this field must still comply with international human rights law.[2] Merely to assert — without particularization — that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law) (see A/HRC/27/37, para. 24).

12. International human rights law requires States to provide an articulable and evidence-based justification for any interference with the right to privacy, whether on an individual or mass scale. It is a central axiom of proportionality that the greater the interference with protected human rights, the more compelling the justification must be if it is to meet the requirements of the Covenant. The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether. By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis. It permits intrusion on private communications without independent (or any) prior authorization based on suspicion directed at a particular individual or organization. Ex ante scrutiny is therefore possible only at the highest level of generality.

13. Since there is no target-specific justification for measures of mass surveillance, it is incumbent upon relevant States to justify the general practice of seeking bulk access to digital communications. The proportionality analysis thus shifts from the micro level (assessing the justification for invading a particular individual's or organization's privacy) to the macro level (assessing the justification for adopting a system that involves wholesale interference with the individual and collective privacy rights of all Internet users). The sheer scale of the interference with privacy rights calls for a competing public policy justification of analogical magnitude.

14. As an absolute minimum, article 17 requires States using mass surveillance technology to give a meaningful public account of the tangible benefits that accrue from its use. Without such a justification, there is simply no means to measure the compatibility of this emerging State practice with the requirements of the Covenant. An assessment of proportionality in this context involves striking a balance between the societal interest in the protection of online privacy, on the one hand, and the undoubted imperatives of effective counter-terrorism and law enforcement, on the

[2] See the compilation of good practices on legal and institutional frameworks for intelligence services and their oversight, promulgated by the former Special Rapporteur (A/HRC/14/46, paras. 9-50).

other. Determining where that balance is to be struck requires an informed public debate to take place within and between States. The international community needs to squarely confront this revolution in our collective understanding of the relationship between the individual and the State.[3] It is a prerequisite for any assessment of the lawfulness of these measures that the States using the technology be transparent about their methodology and its justification.[4] Otherwise, there is a risk that systematic interference with the security of digital communications will continue to proliferate without any serious consideration being given to the implications of the wholesale abandonment of the right to online privacy. If States deploying this technology retain a monopoly of information about its impact, a form of conceptual censorship will prevail that precludes informed debate.

15. Some argue that users of the Internet have no reasonable expectation of privacy in the first place, and must assume that their communications are available to be monitored by corporate and State entities alike. The classic analogy drawn by those who support this view is between sending an unencrypted email and sending a postcard. Whatever the merits of this comparison, it does not answer the key questions of legality, necessity and proportionality. The very purpose of the Covenant's requirement for explicit and publicly accessible legislation governing State interference with communications is to enable individuals to know the extent of the privacy rights they actually enjoy and to foresee the circumstances in which their communications may be subjected to surveillance (see paras. 35-39 below). Yet the value of this technology as a counter-terrorism and law enforcement tool rests in the fact that users of the Internet assume their communications to be confidential (otherwise there would be no purpose in intruding upon them). This is reflected in the assertions made by members of the intelligence communities of the United States of America and the United Kingdom of Great Britain and Northern Ireland following the disclosure of mass surveillance programmes operated by these two States, in which the disclosures were said to have damaged national security by alerting potential terrorists to the fact that their communications were under surveillance.[5]

16. Any assessment of proportionality must also take full account of the fact that the Internet now represents the ubiquitous means of communication for many millions of people around the world. The revolution in digital technology has brought about a quantum shift in the way we communicate with one another. Digital communications technologies that use the Internet (including handheld devices and smartphones) have become part of everyday life (see A/HRC/27/37, para. 1). Anyone who wishes to participate in the exchange of information and ideas in the modern world of global communications is nowadays obliged to use transnational

[3] As the United States Privacy and Civil Liberties Oversight Board has observed: "[P]ermitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens"; "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court".

[4] In her report on the right to privacy in the digital age (A/HRC/27/37, para. 48), the High Commissioner for Human Rights noted "the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability".

[5] See http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388 and www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations/.

digital communication technology. Internet traffic is frequently routed through servers located in foreign jurisdictions. The suggestion that users have voluntarily forfeited their right to privacy is plainly unwarranted (ibid., para. 18). It is a general principle of international human rights law that individuals can be regarded as having given up a protected human right only through an express and unequivocal waiver, voluntarily given on an informed basis. In the modern digital world, merely using the Internet as a means of private communication cannot conceivably constitute an informed waiver of the right to privacy under article 17 of the Covenant.

17. The Internet is not a purely public space. It is composed of many layers of private as well as social and public realms.[1] Those making informed use of social media platforms in which messages are posted in full public view obviously have no reasonable expectation of privacy. The postcard analogy is entirely apposite for the dissemination of information through the public dimensions of Twitter and Facebook, for example, or postings on public websites. But reading a postcard is not an apposite analogy for intercepting private messages sent by e-mail, whether they are encrypted or unencrypted.

18. Assuming therefore that there remains a legal right to respect for the privacy of digital communications (and this cannot be disputed (see General Assembly resolution 68/167)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right (see paras. 51 and 52 below). It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights (see para. 51 below); it excludes any individualized proportionality assessment (see para. 52 below); and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult (see paras. 51 and 52 below). The States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity, and almost no States have enacted explicit domestic legislation to authorize its use (see para. 37 below). Viewed from the perspective of article 17 of the Covenant, this comes close to derogating from the right to privacy altogether in relation to digital communications. For all these reasons, mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law. In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy.[6] Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis (see para. 51 below).

19. There may be a compelling counter-terrorism justification for the radical re-evaluation of Internet privacy rights that these practices necessitate. However, the arguments in favour of a complete abrogation of the right to privacy on the Internet have not been made publicly by the States concerned or subjected to informed scrutiny and debate. The threat of terrorism can provide a justification for mass surveillance only if the States using the technology can demonstrate with particularity the tangible counter-terrorism advantages shown to have accrued from its use. Moreover, measures justified by reference to States' duties to protect against

[6] See also the view of the High Commissioner for Human Rights, A/HRC/27/37, paras. 20 and 25.

the threat of terrorism should never be used as a Trojan horse to usher in wider powers of surveillance for unrelated governmental functions. There is an ever present danger of "purpose creep", by which measures justified on counter-terrorism grounds are made available for use by public authorities for much less weighty public interest purposes (see para. 55 below). In the present report, the Special Rapporteur builds upon the work of his predecessor (A/HRC/13/37) and the former Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion (A/HRC/23/40). He argues that there is now an onus on States deploying bulk access surveillance technology to explain promptly, precisely and publicly why this wholesale intrusion into collective privacy is justified for the prevention of terrorism or other serious crime.

B. Recent disclosures concerning the nature and extent of States' digital surveillance capabilities

20. On 5 June 2013, a national newspaper in the United Kingdom published the content of a classified court order authorized by the United States Foreign Intelligence Surveillance Court under section 215 of the Patriot Act. The order reportedly required one of the largest telecommunications providers in the United States to hand over to the National Security Agency all "telephony metadata" on a daily basis for a three-month period and prohibited the company from disclosing the existence of the request or the order itself. On 6 June 2013, a United States newspaper published a separate story disclosing the existence of a covert National Security Agency digital programme called PRISM. The programme, reportedly authorized pursuant to section 702 of the United States Foreign Intelligence Surveillance Act, was said to involve the collection of content data from the central servers of nine leading United States technology companies.

21. According to reports in both newspapers, the material retrieved through PRISM was made available to other intelligence agencies, including the Government Communications Headquarters of the United Kingdom. Subsequent disclosures reported the existence of a separate data collection programme called Upstream, which is said to involve the capture of both telephone and Internet communications passing through fibre-optic cables and infrastructure owned by United States service providers. Much of the world's Internet traffic is routed through servers physically located in the United States.

22. The media have subsequently reported that the National Security Agency's Systems Intelligence Directorate includes an applications vulnerabilities branch that collects data from communications systems around the world. The Agency is said to operate an Internet exploitation mechanism called Quantum, which enables it to compromise third-party computers. The methodology reportedly involves taking secret control (or "ownership") over servers in key locations on the "backbone" of the Internet. By impersonating chosen websites (including such common sites as the Google search page), Quantum is able to inject unauthorized remote control software into the computers and Wi-Fi-enabled devices of those who visit the clone site (who will, of course, have no reason to doubt the clone site's authenticity). Technology experts assess that this methodology can permanently compromise the user's computer, ensuring that it continues to provide intelligence to the National Security Agency in the United States indefinitely.

23. The United States Executive and Legislative branches have subsequently taken a number of steps in response to these disclosures. One issue to have emerged from this process is the difference in treatment between United States citizens and non-citizens (even those located within the territorial jurisdiction of the United States). The key developments may be summarized as follows:

(a) On 9 August 2013, President Barack Obama announced that he had requested the Privacy and Civil Liberties Oversight Board[7] to undertake a review of existing counter-terrorism efforts.[8] In late August 2013, the Board called upon the Director of National Intelligence and the Attorney-General to update the intelligence community's procedures on collecting, retaining and disseminating information relating to United States citizens;[9]

(b) On 12 December 2013, the President's Review Group released its report entitled "Liberty and security in a changing world", in which the Group made a number of significant recommendations for reform. In response to that report, on 17 January 2014 President Obama announced a series of proposed legislative and administrative changes.[10] The Administration concurrently released a new Presidential Policy Directive, "PPD-28", to strengthen the oversight of the signals intelligence activities of the intelligence community, both within and outside the United States;[11]

(c) On 23 January 2014, the Privacy and Civil Liberties Oversight Board released the first of two reports in which the majority concluded that the telephone metadata programme was inconsistent with domestic law because section 215 of the Patriot Act did not provide an adequate basis to support it.[12] On 27 March, President Obama announced a set of new proposals to end the existing programme.[13] On 22 May 2014, the House of Representatives adopted the United States Freedom Act, incorporating some of the President's proposals;

(d) On 2 July 2014, the Privacy and Civil Liberties Oversight Board released a second report setting out in detail how surveillance operations under section 702 of the Foreign Intelligence Surveillance Act work in practice.[14] While the report's chief concern was the compatibility of these programmes with United States statutory and constitutional requirements, the Board recognized that they also raised "important but difficult legal and policy questions" concerning the treatment of non-United States persons.[15] The Board took the view that the application of the

[7] The Board is an independent agency within the executive branch with authority to review and analyse counter-terrorism operations and to ensure that they are balanced with the need to protect privacy and civil liberties; see www.pclob.gov/.

[8] See www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

[9] See www.pclob.gov/newsroom.

[10] See www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[11] See www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[12] "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court".

[13] See www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[14] "Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA", see www.pclob.gov/meetings-and-events/2014meetingsevents/02-july-2014-public-meeting.

[15] Ibid., p. 98.

right to privacy to national security surveillance conducted in one country that might affect residents of another country is not "settled" among States parties to the International Covenant on Civil and Political Rights, a proposition that was said to be evidenced by the "ongoing spirited debate".[16]

24. A parallel process of review has taken place within the United Kingdom. On 10 June 2013, in response to allegations that Government Communications Headquarters had circumvented United Kingdom law by using the National Security Agency's PRISM programme to access the content of communications that could not be accessed under domestic law, the Foreign Secretary made a statement in Parliament indicating that any data obtained from the United States involving United Kingdom nationals is "subject to proper United Kingdom statutory controls and safeguards", including the relevant provisions of the Intelligence Services Act of 1994, the Human Rights Act of 1998 and the Regulation of Investigatory Powers Act of 2000.[17]

25. On 21 June 2013, the media reported on the existence of a separate programme operated by Government Communications Headquarters ("Tempora"), under which data interceptors were reportedly placed on fibre-optic cables running between the United Kingdom and the United States to facilitate the interception of both metadata and content information. Whether existing legislation provides Government Communications Headquarters with the lawful authority to conduct such operations, and whether they conform to the right to privacy as guaranteed under article 8 of the European Convention on Human Rights, has been questioned within and outside the United Kingdom Parliament.[18] Subsequent disclosures have focused on the role of the Joint Threat Intelligence Group in Government Communications Headquarters. This agency is reported to have deployed a computer virus called Ambassador's Reception for the purposes of online covert action. This virus is said to be able to encrypt itself and act as a "chameleon" imitating communications by other Internet users.

26. Following a preliminary investigation into Government Communications Headquarters' access to communications and content data, the Intelligence and Security Committee (a Parliamentary committee with responsibility for the oversight of the intelligence community)[19] issued a statement on 17 July 2013. Having taken account of the legal framework governing information-sharing arrangements between Government Communications Headquarters and its overseas counterparts, the Committee concluded that no United Kingdom law had been violated and that Government Communications Headquarters had conformed to its statutory duties under the Intelligence Services Act of 1994. The Committee nevertheless concluded that further investigations were merited to consider whether the existing statutory framework governing access to private communications was adequate given the "complex interaction" among the Intelligence Services Act of 1994, the Human Rights Act of 1998 and the Regulation of Investigatory Powers Act of 2000. On 17 October 2013, the Intelligence and Security Committee

[16] Ibid., p. 100.

[17] See www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.

[18] See www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance; and www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm.

[19] See http://isc.independent.gov.uk/.

announced that it would broaden the scope of its inquiry following concerns about the extent of intelligence service capabilities and the impact of their operations on the right to privacy.[20]

27. On 8 April 2014, the Court of Justice of the European Union released its judgement in the case of *Digital Rights Ireland*, in which it declared the European Union Data Retention Directive to be incompatible with the right to respect for private life and the right to the protection of personal data, both of which are guaranteed under the Charter of Fundamental Rights of the European Union.[21] The Directive required communication service providers to retain traffic data so as to permit access by the competent national authorities for the purpose of preventing, investigating, detecting and prosecuting serious crime, including terrorism. In holding that the retention of, and access to, traffic data constituted a "particularly serious interference" with both rights, the Court of Justice of the European Union found that the Directive failed to satisfy the principle of proportionality. On 10 July 2014, the United Kingdom Government introduced the Data Retention and Investigatory Powers Bill in response to the ruling. The Government characterized the Bill (now an Act) as a measure to "clarify" the nature and extent of obligations that can be imposed on telecommunications and Internet service providers based in the United Kingdom.[22]

C. Mass surveillance, counter-terrorism and the right to privacy

1. The right to privacy under article 17 of the International Covenant on Civil and Political Rights

28. Privacy can be defined as the presumption that individuals should have an area of personal autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals (see A/HRC/23/40, para. 22; and A/HRC/13/37, para. 11). The duty to respect the privacy and security of communications implies that individuals have the right to share information and ideas with one another without interference by the State (or a private actor), secure in the knowledge that their communications will reach and be read by the intended recipients alone.[23] The right to privacy also encompasses the right of individuals to know who holds information about them and how that information is used.[24]

29. Article 17 of the International Covenant on Civil and Political Rights is the most important legally binding treaty provision guaranteeing the right to privacy at the universal level. It provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home and correspondence, nor to unlawful attacks on his or her honour and reputation". It further provides that "everyone has the right to the protection of the law against such interference or attacks". Other international human rights instruments contain similar provisions;

[20] See http://isc.independent.gov.uk/news-archive/17october2013.

[21] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014.

[22] See www.gov.uk/government/speeches/communications-data-and-interception.

[23] Human Rights Committee general comment No. 16, para. 8.

[24] Ibid., para. 10; see A/HRC/23/40, para. 22.

and laws at the regional and national levels also reflect the right of all people to respect for their private and family life, home and correspondence.

30. The right to privacy is not, however, an absolute right. Once an individual is under suspicion and subject to formal investigation by intelligence or law enforcement agencies, that individual may be subjected to surveillance for entirely legitimate counter-terrorism and law enforcement purposes (see A/HRC/13/37, para. 13). Although article 17 of the Covenant does not contain a specific limitation clause outlining the circumstances in which interference with the right to privacy may be compatible with the Covenant, it is universally understood as permitting such measures providing that (a) they are authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant,[25] (b) they pursue a legitimate aim and (c) they meet the tests of necessity and proportionality.[26]

31. The realization that a large part of the world's Internet traffic is at some point routed through the United States prompted a number of States to express concerns as to whether the right to privacy of their citizens had been violated by the PRISM programme. In December 2013, the General Assembly adopted resolution 68/167, on the right to privacy in the digital age, which was co-sponsored by 57 Member States and adopted without a vote. In that resolution, the Assembly affirmed that the right to privacy must be protected online, and called upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law.

32. In the same resolution, the General Assembly also mandated the Office of the United Nations High Commissioner for Human Rights to report to the Human Rights Council and the General Assembly on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance, and/or the interception of digital communications and the collection of personal data, including on a mass scale. In paragraph 47 of her report published on 30 June 2014 (A/HRC/27/37), the High Commissioner concluded that international human rights law provided a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data. She noted, however, that the practice of many States revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which had contributed to a lack of accountability for arbitrary or unlawful interference with the right to privacy. The High Commissioner emphasized that information was still emerging on the nature and extent of digital surveillance operations but expressed her concern at the "disturbing lack of governmental transparency associated with surveillance policies, laws and practices,

[25] Human Rights Committee general comment No. 16, para. 3.

[26] See A/HRC/27/37, paras. 22-25, and the sources there cited; A/HRC/23/40, paras. 28 and 29; A/HRC/13/37, paras. 13-17; Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, E/CN.4/1985/4, annex; Human Rights Committee general comments Nos. 16, 27, 29, 34 and 31; Human Rights Committee, *Van Hulst v. Netherlands*, Communication No. 903/2999, 2004; *Madafferi v. Australia*, Communication No. 1011/2001, 2004; *Toonen v. Australia*, Communication No. 488/1992, para. 8.3; *MG v. Germany*, Communication No. 1482/2006, 2008; and CCPR/C/USA/CO/4.

which hinders any effort to assess their coherence with international human rights law and to ensure accountability" (ibid., para. 48). She called upon States to review their national law and practice for conformity with international human rights norms, and to make amendments, where necessary. She also called upon the international community to carry out further in-depth study into the issues (ibid., paras. 49 and 51).

2. Counter-terrorism as a legitimate aim

33. Unlike a number of the qualified rights protected by the Covenant, article 17 does not enumerate an exhaustive list of legitimate public policy objectives that may form the basis of a justification for interfering with the right to privacy. Nonetheless, the prevention, suppression and investigation of acts of terrorism clearly amount to a legitimate aim for the purposes of article 17. Terrorism can destabilize communities, threaten social and economic development, fracture the territorial integrity of States, and undermine international peace and security. Under article 6 of the Covenant, States are under a positive obligation to protect citizens and others within their jurisdiction against acts of terrorism. One aspect of this obligation is the duty to establish effective mechanisms for identifying potential terrorist threats before they have materialized. States discharge this duty through the gathering and analysis of relevant information by intelligence and law enforcement agencies (see A/HRC/20/14, para. 21).

34. The enhanced capacity of States to monitor all Internet traffic is said to be of particular significance in the counter-terrorism context because communications via the Internet have played an important part in the financing and perpetration of acts of international terrorism; because the Internet has been used for the purpose of recruitment to terrorist organizations; and because the identification in advance of those involved in the planning or instigation of acts of terrorism may otherwise be hampered by intelligence limitations. Since terrorism is a global activity, the search for those involved must extend beyond national borders. The prevention and suppression of terrorism is thus a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the Internet.

3. Mass surveillance and the quality of law requirement

35. Article 17 of the Covenant explicitly provides that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This imports a "quality of law" requirement that imposes three conditions: (a) the measure must have some basis in domestic law; (b) the domestic law itself must be compatible with the rule of law and the requirements of the Covenant; and (c) the relevant provisions of domestic law must be accessible, clear and precise. An interference that is authorized by domestic law may nonetheless be "unlawful" and/or "arbitrary" for the purposes of article 17 if the relevant domestic legislation does not meet the core requirements of accessibility, specificity and foreseeability,[27] or if domestic law otherwise fails to meet the standards of necessity and proportionality.[28] Accordingly, domestic law must contain provisions that ensure that intrusive surveillance powers are tailored to specific legitimate aims (see

[27] Human Rights Committee general comment No. 16, para. 3.

[28] Ibid., para. 8.

A/HRC/13/37, para. 60; and A/HRC/27/37, para. 28), and afford effective safeguards against abuse.[29] Moreover, the exercise of executive discretion must be circumscribed with reasonable clarity by the applicable law or binding published guidelines.[30]

36. Accessibility requires not only that domestic law be published, but also that it meet a standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur. In paragraph 8 of its general comment No. 16 on the right to privacy, the Human Rights Committee stressed that legislation authorizing interference with private communications "must specify in detail the precise circumstances in which such interference may be permitted". Prior to the introduction of mass surveillance programmes outlined in the present report, this stipulation had always been understood as requiring domestic legislation to spell out clearly the conditions under which, and the procedures by which, any interference may be authorized; the categories of person whose communications may be intercepted; the limits on the duration of surveillance; and the procedures for the use and storage of the data collected.[29] The European Court of Human Rights has also stressed the need for clear detailed rules on the subject.[31]

37. Mass surveillance programmes pose a significant challenge to the legality requirements of article 17 of the Covenant. Where bulk access programmes are in operation, there are no limits to the categories of persons who may be subject to surveillance, and no limits on its duration. These conditions cannot therefore be spelled out in legislation. The detailed legal and administrative frameworks for mass surveillance often remain classified, and little is still publicly known about the ways in which captured data are operationalized. Very few States have so far enacted primary legislation explicitly authorizing such programmes. Instead, outdated domestic laws that were designed to deal with more rudimentary forms of surveillance have been applied to new digital technology without modification to reflect the vastly increased capabilities now employed by some States. Indeed, it has been suggested that certain States have "intentionally sought to apply older and weaker safeguard regimes to ever more sensitive information" (see A/HRC/13/37, para. 57).

38. The Special Rapporteur considers that there is an urgent need for States to revise national laws regulating modern forms of surveillance to ensure that these practices are consistent with international human rights law. Domestic laws governing the interception of communications should be updated to reflect modern forms of digital surveillance that are far broader in scope, and involve far deeper penetration into the private sphere, than those envisaged when much of the existing domestic legislation was enacted. The absence of clear and up-to-date legislation creates an environment in which arbitrary interferences with the right to privacy can occur without commensurate safeguards. Explicit and detailed laws are essential for

[29] CCPR/C/USA/CO/4, para. 22; *Malone v. United Kingdom*, Application No. 8691/79, Judgment of 2 August 1984, paras. 67-68; and *Weber and Saravia v. Germany*, Application No. 54934/00, Judgment of 29 June 2006.

[30] A/HRC/27/37, para. 29; and Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (see E/CN.4/1985/4, annex), paras. 16 and 18.

[31] *Weber and Saravia v. Germany*, Application No. 54934/00, Judgment 29 June 2006; *Uzun v. Germany* (2012) 54 EHRR 121 para. 35.

ensuring legality and proportionality in this context. They are also an indispensable means of enabling individuals to foresee whether and in what circumstances their communications may be the subject of surveillance.

39. A public legislative process provides an opportunity for Governments to justify mass surveillance measures to the public. Open debate enables the public to appreciate the balance that is being struck between privacy and security (ibid., para. 56). A transparent law-making process should also identify the vulnerabilities inherent in digital communications systems, enabling users to make informed choices. This is not only a core ingredient of the requirement for legal certainty under article 17 of the Covenant; it is also a valuable means of ensuring effective public participation in a debate on a matter of national and international public interest (see A/HRC/27/37, para. 29; and A/HRC/14/46). In the view of the Special Rapporteur, where the privacy rights of the digital community as a whole are subject to systematic interference, nothing short of detailed and explicit authorization in primary legislation suffices to meet the principle of legality.

40. By contrast, the use of delegated legislation (instruments enacted by the executive under delegated powers) has already permitted the adoption of secret legal frameworks for mass surveillance, inhibiting the ability of the legislature, the judiciary and the public to scrutinize the use of these new powers (see A/HRC/13/37, para. 54). Such provisions do not meet the quality of law requirements in article 17 of the Covenant because they are not sufficiently accessible to the public (see CCPR/C/USA/CO/4). While there may be legitimate public interest reasons for maintaining the secrecy of technical and operational specifications, these do not justify withholding from the public generic information about the nature and extent of a State's Internet penetration. Without such information, it is impossible to assess the legality, necessity and proportionality of these measures. States should therefore be transparent about the use and scope of mass communications surveillance (see A/HRC/23/40, para. 91).

4. Extraterritorial mass surveillance programmes

41. Certain States have the technical capability to conduct mass surveillance of communications between individuals not resident within their jurisdiction, and have thus implemented surveillance arrangements that have extraterritorial effect. Some of these activities are physically conducted on the territory of the State concerned and therefore engage the principles of territorial jurisdiction under the Covenant. This is the case not only where State agents place data interceptors on fibre-optic cables travelling through their jurisdiction, but also where a State exercises regulatory authority over the telecommunications or Internet service providers that physically control the data (A/HRC/27/37, para. 34). In either case, human rights protections must be extended to those whose privacy is being interfered with, whether or not they are physically located in the country in which the service provider is incorporated. The same is true where legislation on mandatory data retention imposes obligations on service providers located within a State's territorial or legal jurisdiction. Even where States penetrate infrastructure located wholly outside their territorial jurisdiction the relevant authorities nevertheless remain bound by the State's obligations under the Covenant (ibid., paras. 32-35 and the sources cited therein).

42. Extraterritorial surveillance operations pose unique challenges for the application of the "quality of law" requirements in article 17 of the Covenant. Domestic legislation governing the interception of external (international) communications often affords less protection than comparable provisions protecting purely domestic communications.[32] Of even greater concern, some States (including the United States) continue to permit asymmetrical protection regimes for nationals and non-nationals. This difference of treatment affects all digital communications since messages are often routed through servers located in other jurisdictions. However, it has particularly significant ramifications for the penetration of cloud-based computing.[33]

43. Either form of differential treatment is incompatible with the principle of non-discrimination in article 26 of the Covenant, a principle that is also inherent in the very notion of proportionality.[34] Moreover, the use of mass surveillance programmes to intercept communications of those located in other jurisdictions raises serious questions about the accessibility and foreseeability of the law governing the interference with privacy rights, and the inability of individuals to know that they might be subject to foreign surveillance or to interception of communications in foreign jurisdictions. The Special Rapporteur considers that States are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction.

5. International cooperation between intelligence agencies

44. Similar concerns arise in relation to international intelligence-sharing arrangements. The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority (see A/HRC/13/37). Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards. Following a wide process of consultation, the High Commissioner for Human Rights recently found credible evidence that some Governments have systematically routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy (see A/HRC/27/37, para. 30). Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant.

---

[32] In her report on privacy in the digital age the High Commissioner identified a number of such provisions: in the United States, the Foreign Intelligence Surveillance Act, sect.1881(a); in the United Kingdom, the Regulation of Investigatory Powers Act of 2000, sect.8(4); in New Zealand the Government Security Bureau Act of 2003 sect.15A; in Australia the Intelligence Services Act sect.9; and in Canada the National Defence Act, sect.273.64(1) (see A/HRC/27/37, para. 35, note 30).

[33] European Parliament Directorate General for Internal Policies and Casper Bowden, "The US surveillance programmes and their impact on EU citizens' fundamental rights", 2013.

[34] The Human Rights Committee has also emphasized the importance of "measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of individuals whose communications are under direct surveillance", CCPR/C/USA/CO/4, para. 22 (a).

6. Safeguards and supervision

45. One of the core protections afforded by article 17 is that covert surveillance systems must be attended by adequate procedural safeguards to protect against abuse.[29] These safeguards may take a variety of forms, but generally include independent prior authorization and/or subsequent independent review. Best practice requires the involvement of the executive, the legislature and the judiciary, as well as independent civilian oversight (see A/HRC/27/37). The absence of adequate safeguards can lead to a lack of accountability for arbitrary or unlawful intrusions on the right to Internet privacy (ibid.).

46. Where targeted surveillance programmes are in operation, many States make provision for prior judicial authorization. Judicial involvement that meets international standards is an important safeguard, although there is evidence that in some jurisdictions the degree and effectiveness of such scrutiny has been circumscribed by judicial deference to the executive (ibid., para. 38). In other States, such as the United Kingdom, warrants of interception directed at particular targets are granted by government ministers without prior judicial authority. This is said to be justified on the basis that ministers are democratically accountable to the electorate. The Executive's use of these powers is then subject to review by an independent Interception of Communications Commissioner, and individuals can also bring complaints to a judicial body, the Investigatory Powers Tribunal, which has authority to consider classified information in closed proceedings.

47. In the context of targeted surveillance, whichever method of prior authorization is adopted (judicial or executive), there is at least an opportunity for ex ante review of the necessity and proportionality of a measure of intrusive surveillance by reference to the particular circumstances of the case and the individual or organization whose communications are to be intercepted. Neither of these opportunities exists in the context of mass surveillance schemes since they do not depend on individual suspicion. Ex ante review is thus limited to authorizing the continuation of the scheme as a whole, rather than its application to a particular individual. The Special Rapporteur considers that those States using mass surveillance technology must establish strong independent oversight bodies that are adequately resourced and mandated to conduct ex ante review of the use of intrusive surveillance techniques against the requirements of legality, necessity and proportionality in article 17 of the Covenant (A/HRC/13/37, para. 62).

48. The other procedural dimension of article 17 is the requirement for ex post facto review of intrusive surveillance measures. Some States provide for an independent reviewer to monitor the operation of surveillance legislation by analysing the manner and extent of its use and the justification therefor. Such reviews should always incorporate an analysis of the compatibility of State practice with the requirements of the Covenant.

49. In addition to this type of general overview, States are under a specific obligation to provide a remedy to individuals whose Covenant rights have arguably been violated. Article 2, paragraph 3(b), of the Covenant requires States parties to ensure that any person claiming a remedy has an enforceable right to have his or her claim determined by a competent domestic judicial, administrative or legislative authority. In order to render this right effective, domestic law must provide an independent mechanism capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process

guarantees, which has power to grant a binding remedy (including, where appropriate, an order for the cessation of surveillance or the destruction of the product) (see A/HRC/14/46; and A/HRC/27/37, para. 39).

50. In order to invoke the right to an effective remedy, it is generally necessary for an individual to establish that he or she has been the victim of a violation. In the context of secret surveillance measures, this requirement can be difficult or impossible to meet. Very few States have provisions in place requiring ex post notification of surveillance to the suspect. The European Court of Human Rights has, accordingly, relaxed the requirement for individuals to prove that they have been the subject of secret surveillance. It has drawn a distinction between complaints directed towards the existence of a regime that is alleged to fall short of the requirements of the European Convention on Human Rights, and complaints concerning specific instances of unlawful activity by the State. In the former situation, the Court has been prepared to examine the impugned provisions on their face,[35] whereas in the latter situation, it has generally required applicants to show a "reasonable likelihood" that they have been the subject of unlawful surveillance.[36] In the context of mass surveillance regimes, the Special Rapporteur considers that any Internet user should have standing to challenge the legality, necessity and proportionality of the measures at issue.

7. The necessity and proportionality of mass surveillance programmes

51. It is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the Covenant is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result" (see CCPR/C/21/Rev.1/Add.9; and A/HRC/13/37, para. 60). The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest. However, there are limits to the extent of permissible interference with a Covenant right. As the Human Rights Committee has emphasized, "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right".[37] In the context of covert surveillance, the Committee has therefore stressed that any decision to allow interference with communications must be taken by the authority designated by law "on a case-by-case basis".[38] The proportionality of any interference with the right to privacy should therefore be judged on the particular circumstances of the individual case.[39]

52. None of these principles sits comfortably with the use of mass surveillance technology by States. The technical ability to run vast data collection and analysis programmes undoubtedly offers an additional means by which to pursue counter-terrorism and law enforcement investigations. But an assessment of the

[35] *Klass v. Germany* (1979-80) 2 EHRR 214.
[36] *Halford v. United Kingdom* (1997) 24 EHRR 523.
[37] Human Rights Committee general comments Nos. 27 and 31.
[38] Human Rights Committee general comment No. 16, para. 8.
[39] Human Rights Committee general comment No. 16, para. 4, *Van Hulst v. The Netherlands*, Communication No. 903/1999, 2004, para 7.3; *Toonen v. Australia*, Communication No. 488/1992, para. 8.3.

proportionality of these programmes must also take account of the collateral damage to collective privacy rights. Mass data collection programmes appear to offend against the requirement that intelligence agencies must select the measure that is least intrusive on human rights (unless relevant States are in a position to demonstrate that nothing less than blanket access to all Internet-based communication is sufficient to protect against the threat of terrorism and other serious crime). Since there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy. They exclude altogether the "case-by-case" analysis that the Human Rights Committee has regarded as essential, and they may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime (see A/HRC/27/37, para. 25). The Special Rapporteur, accordingly, concludes that such programmes can be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world.[40]

8. Mandatory retention legislation and the automated mining of communications data held by telecommunications and Internet service providers

53. Mass surveillance programmes are not confined to the interception of communications content. Digital communications generate large amounts of transactional data. These communications data (or metadata) include personal information on individuals, their location and online activities. Many States have adopted legislation compelling telecommunications and Internet service providers to collect and preserve communications data in order to make them available for subsequent analysis. Such laws typically require service providers to furnish State authorities with Internet protocol allocations, enabling the user of a particular Internet protocol address at any given time to be identified. The capture of communications data has become an increasingly valuable surveillance technique for States. Communications data are easily stored and searched, and can be used to compile profiles of individuals that are just as privacy-sensitive as the content of communications (see A/HRC/27/37, para. 19). By combining and aggregating information derived from communications data, it is possible to identify an individual's location, associations and activities (see A/HRC/23/40, para. 15). In the absence of special safeguards, there is virtually no secret dimension of a person's private life that would withstand close metadata analysis.[1] Automated data-mining thus has a particularly corrosive effect on privacy.

54. In many States, a wide range of public bodies have access to communications data, for a wide variety of purposes, often without judicial authorization or meaningful independent oversight. In the United Kingdom, for example, more than 200 agencies are authorized to seek communications data under the Regulation of Investigatory Powers Act of 2000,[41] and there were 514,608 requests by public

[40] See A/HRC/27/37, para. 25, where the High Commissioner for Human Rights observed: "[I]t will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely whether the measure is necessary and proportionate."

[41] The list of agencies authorized to seek communications data includes tax authorities and local government agencies, and may be extended by delegated legislation (executive order).

authorities for communications data in 2013 alone.[42] Courts have for some time recognized that the release of metadata to a public authority constitutes an interference with the right to privacy, and the Court of Justice of the European Union recently held that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right,[43] (with the grant of access to retained metadata for the purpose of analysis constituting a further and distinct interference).[44] In reaching this conclusion, the Court of Justice of the European Union emphasized that communications metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained".[45]

55. Applying the approach adopted by the Court of Justice of the European Union, it follows that the collection and retention of communications data constitute an interference with the right to privacy, whether or not the data are subsequently accessed or analysed by a public authority. Neither the capture of communications data under mandatory data retention legislation, nor its subsequent disclosure to (and analysis by) State authorities, requires a prior suspicion directed at any particular individual or organization. The Special Rapporteur therefore shares the reservations expressed by the High Commissioner as to the necessity and proportionality of mandatory data retention laws (see A/HRC/27/37, para. 26).

9. Purpose specification

56. Many States lack "purpose specification" provisions restricting information gathered for one purpose from being used for other unrelated governmental objectives. As a result, data that were ostensibly collected for national security purposes may be shared between intelligence agencies, law enforcement agencies and other State entities, including tax authorities, local councils and licensing bodies.[46] National security and law enforcement agencies are typically excluded from provisions of data protection legislation that limit the sharing of personal data. As a result, it may be difficult for individuals to foresee when and by which State agency they might be subjected to surveillance. This "purpose creep" risks violating article 17 of the Covenant, not only because relevant laws lack foreseeability, but also because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another (ibid., para. 27). The Special Rapporteur therefore endorses the recommendation of his predecessor that States must be obliged to provide a legal basis for the reuse of personal information, in accordance with human rights principles (see A/HRC/13/37, paras. 50 and 66). This is particularly important where information is shared across borders or between States.

---

[42] See www.intelligencecommissioners.com/.

[43] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Judgment of 8 April 2014, para. 34.

[44] Ibid., para. 35.

[45] Ibid., paras. 26, 27 and 37.

[46] For an analysis of the ways in which such purpose creep has occurred in the United Kingdom, see www.whatdotheyknow.com/request/127491/response/315758/attach/html/2/Summay%20of%20Counsels%20advice.pdf.html.

10. The private sector

57. States increasingly rely on the private sector to facilitate digital surveillance. This is not confined to the enactment of mandatory data retention legislation. Corporates have also been directly complicit in operationalizing bulk access technology through the design of communications infrastructure that facilitates mass surveillance. Telecommunications and Internet service providers have been required to incorporate vulnerabilities into their technologies to ensure that they are wiretap-ready. The High Commissioner for Human Rights has characterized these practices as "a delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of self-regulation and cooperation" (see A/HRC/27/37, para. 42). The Special Rapporteur concurs with this assessment. In order to ensure that they do not become complicit in human rights violations, service providers should ensure that their operations comply with the Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011 (ibid., paras. 43-46).

IV. Conclusions and recommendations

58. **States' obligations under article 17 of the International Covenant on Civil and Political Rights include the obligation to respect the privacy and security of digital communications. This implies in principle that individuals have the right to share information and ideas with one another without interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone. Measures that interfere with this right must by authorized by domestic law that is accessible and precise and that conforms with the requirements of the Covenant. They must also pursue a legitimate aim and meet the tests of necessity and proportionality.**

59. **The prevention and suppression of terrorism is a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the Internet. However, the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law.**

60. **The Special Rapporteur concurs with the High Commissioner for Human Rights that there is an urgent need for States using this technology to revise and update national legislation to ensure consistency with international human rights law. Not only is this a requirement of article 17, but it also provides an important opportunity for informed debate that can raise public awareness and enable individuals to make informed choices. Where the privacy rights of the entire digital community are at stake, nothing short of detailed and explicit primary legislation should suffice. Appropriate restrictions should be imposed**

on the use that can be made of captured data, requiring relevant public authorities to provide a legal basis for the reuse of personal information.

61. **States should establish strong and independent oversight bodies that are adequately resourced and mandated to conduct ex ante review, considering applications for authorization not only against the requirements of domestic law, but also against the necessity and proportionality requirements of the Covenant. In addition, individuals should have the right to seek an effective remedy for any alleged violation of their online privacy rights. This requires a means by which affected individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees. Accountability mechanisms can take a variety of forms, but must have the power to order a binding remedy. States should not impose standing requirements that undermine the right to an effective remedy.**

62. **The Special Rapporteur concurs with the High Commissioner for Human Rights that where States penetrate infrastructure located outside their territorial jurisdiction, they remain bound by their obligations under the Covenant. Moreover, article 26 of the Covenant prohibits discrimination on grounds of, inter alia, nationality and citizenship. The Special Rapporteur thus considers that States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant.**

63. **The Special Rapporteur calls upon all States that currently operate mass digital surveillance technology to provide a detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community by reference to the requirements of article 17 of the Covenant. States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use.**

64. **The Special Rapporteur concurs with his predecessor (see A/HRC/13/37, para. 19) and with the former Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion (see A/HRC/23/40, para. 98) that the Human Rights Committee should develop and adopt a new general comment on the right to online privacy, which would reflect developments in the surveillance of digital communications that have taken place since general comment 16 was adopted in 1988.**