



General Assembly

Distr.: General
17 April 2013

Original: English

Human Rights Council

Twenty-third session

Agenda item 3

**Promotion and protection of all human rights, civil,
political, economic, social and cultural rights,
including the right to development**

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*

Summary

The present report, submitted in accordance with Human Rights Council resolution 16/4, analyses the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression. While considering the impact of significant technological advances in communications, the report underlines the urgent need to further study new modalities of surveillance and to revise national laws regulating these practices in line with human rights standards.

* Late submission.

Contents

| | <i>Paragraphs</i> | <i>Page</i> |
|--|-------------------|-------------|
| I. Introduction | 1–6 | 3 |
| II. Activities of the Special Rapporteur | 7–10 | 4 |
| III. The evolution of technology of surveillance | 11–18 | 4 |
| IV. International human rights framework | 19–32 | 6 |
| A. Interrelations between the rights to privacy to freedom of opinion and expression | 24–27 | 7 |
| B. Permissible limitations to privacy and freedom of expression | 28–29 | 8 |
| C. Recent considerations by international mechanisms for the protection of human rights | 30–32 | 9 |
| V. Modalities of communications surveillance | 33–49 | 10 |
| A. Targeted communications surveillance | 34–37 | 10 |
| B. Mass communications surveillance | 38–40 | 11 |
| C. Access to communications data | 41–43 | 11 |
| D. Internet filtering and censorship | 44–46 | 12 |
| E. Restrictions on anonymity | 47–49 | 13 |
| VI. Concerns on national legal standards | 50–71 | 13 |
| A. Lack of judicial oversight | 54–57 | 14 |
| B. National security exceptions | 58–60 | 15 |
| C. Unregulated access to communications data | 61 | 16 |
| D. Extra-legal surveillance | 62–63 | 16 |
| E. Extra-territorial application of surveillance laws | 64 | 17 |
| F. Mandatory data retention | 65–67 | 17 |
| G. Identity disclosure laws | 68–70 | 18 |
| H. Restrictions on encryption and key disclosure laws | 71 | 19 |
| VII. The roles and responsibilities of the private sector | 72–77 | 19 |
| VIII. Conclusions and recommendations | 78–99 | 20 |
| A. Updating and strengthening laws and legal standards | 81–87 | 21 |
| B. Facilitating private, secure and anonymous communications | 88–90 | 22 |
| C. Increasing public access to information, understanding and awareness of threats to privacy | 91–94 | 22 |
| D. Regulating the commercialization of surveillance technology | 95–97 | 22 |
| E. Furthering the assessment of relevant international human rights obligations | 98–99 | 23 |

I. Introduction

1. The present report analyses the implications of States' surveillance of communications for the exercise of the human rights to privacy and to freedom of opinion and expression. While considering the impact of significant technological advances in communications, the report underlines the urgent need to further study new modalities of surveillance and to revise national laws regulating these practices in line with human rights standards.

2. Innovations in technology have increased the possibilities for communication and protections of free expression and opinion, enabling anonymity, rapid information-sharing and cross-cultural dialogues. Technological changes have concurrently increased opportunities for State surveillance and interventions into individuals' private communications.

3. Concerns about national security and criminal activity may justify the exceptional use of communications surveillance technologies. However, national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.

4. In previous reports (A/HRC/17/27 and A/66/290), the Special Rapporteur has analysed the unprecedented impact of the Internet on expanding the possibilities of individuals to exercise their right to freedom of opinion and expression. He expressed concerns at the multiple measures taken by States to prevent or restrict the flow of information online, and highlighted the inadequate protection of the right to privacy in the Internet.

5. Building on his previous analysis, the aim of this report is to identify the risks that the new means and modalities of communications surveillance pose to human rights, including the right to privacy and the freedom of opinion and expression.

6. The following terms are used in this report to describe the most common modalities of surveillance of communications:

(a) Communications surveillance: the monitoring, interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks;

(b) Communications data: information about an individual's communications (e-mails, phone calls and text messages sent and received, social networking messages and posts), identity, network accounts, addresses, websites visited, books and other materials read, watched or listened to, searches conducted, resources used, interactions (origins and destinations of communications, people interacted with, friends, family, acquaintances), and times and locations of an individual, including proximity to others);

(c) Internet filtering: automated or manual monitoring of Internet content (including websites, blogs and online media sources, as well as e-mail) to restrict or suppress particular text, images, websites, networks, protocols, services or activities.

II. Activities of the Special Rapporteur

7. During the reporting period, the Special Rapporteur participated in multiple international and national events related to the issues he addressed in his previous reports such as freedom of expression in the Internet, prevention of hate speech, and the protection of journalists. He paid particular attention to national initiatives promoting the protection of journalists; in this regard, he participated in meetings on initiatives developed in Brazil, Colombia, Honduras and Mexico. He also participated in the "United Nations Inter-Agency Meeting on the Safety of Journalists and the Issues of Impunity", held in November 2012 in Vienna.

8. His last report to the United Nations General Assembly focused on prevention of hate speech and incitement to hatred.¹ The same topic was addressed in a side event to the General Assembly jointly organized by the Special Rapporteur and the Special Adviser on the Prevention of Genocide in February 2013. In the same month, he further addressed these issues in the launch of the "Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" in Geneva and in the Fifth United Nations Alliance of Civilizations Global Forum in Vienna.

9. The Special Rapporteur undertook a mission to Honduras from 7 to 14 August 2012. His main findings and recommendations on this visit can be found in the addendum to this report (A/HRC/20/40/Add.1). He was invited by the Indonesian Government to visit the country in January 2013. Regrettably, the Government requested the visit to be postponed and new dates for the visit are yet to be confirmed.

10. For the preparation of this report, the Special Rapporteur revised relevant studies and consulted with experts on matters related to the surveillance of communications. In December 2012, he participated in the Workshop on Electronic Surveillance and Human Rights organized by the Electronic Frontier Foundation. In February 2013, he organized an expert consultation for the preparation of this report which took place in parallel to the activities of the "World Summit on the Information Society+10 Meeting" held at the United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, where he also participated in the opening plenary panel.

III. The evolution of technology of surveillance

11. Innovations in technology have facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have also provided new opportunities for State surveillance and intervention into individuals' private lives.

12. From the inception of the first form of remote communications, States have sought to intercept and monitor individuals' private communications to serve law enforcement and national security interests. Through communications, the most personal and intimate information, including about an individual's or group's past or future actions, can be revealed. Communications represent a valuable source of evidence upon which the State can draw to prevent or prosecute serious crimes or forestall potential national security emergencies.

¹ A/67/357.

13. Innovations in technology throughout the twentieth century changed the nature and implications of communication surveillance. The means by, and frequency with which people are able to communicate expanded significantly. The transition from fixed-line telephone systems to mobile telecommunication and the declining costs of communications services resulted in dramatic growth in telephone usage. The advent of the Internet saw the birth of a number of new tools and applications to communicate at no cost, or at very affordable rates. These advancements have enabled greater connectivity, facilitated the global flow of information and ideas, and increased the opportunities for economic growth and societal change.

14. As information and communication technologies evolved, so did the means by which States sought to monitor private communications. With increased use of telephones came the use of wiretapping, which consists of placing a tap on a telephone wire to listen to private phone conversations. With the replacement of analogue telephone networks with fibre optics and digital switches in the 1990s, States redesigned the networking technology to include interception capabilities (“backdoors”) to permit State surveillance, rendering modern telephone networks remotely accessible and controllable.

15. The dynamic nature of technology has not only changed how surveillance can be carried out, but also “what” can be monitored. In enabling the creation of various opportunities for communication and information-sharing, the Internet has also facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive. Communications data are storable, accessible and searchable, and their disclosure to and use by State authorities are largely unregulated. Analysis of this data can be both highly revelatory and invasive, particularly when data is combined and aggregated. As such, States are increasingly drawing on communications data to support law enforcement or national security investigations. States are also compelling the preservation and retention of communication data to enable them to conduct historical surveillance.

16. Changes in technology have been paralleled by changes in attitudes towards communications surveillance. When the practice of official wiretapping first commenced in the United States of America, it was conducted on a restricted basis, and was only reluctantly sanctioned by the courts.² It was viewed as such a serious threat to the right to privacy that its use had to be restricted to detecting and prosecuting the most serious crimes. Over time, however, States have expanded their powers to conduct surveillance, lowering the threshold and increasing the justifications for such surveillance.

17. In many countries, existing legislation and practices have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age. Traditional notions of access to written correspondence, for example, have been imported into laws permitting access to personal computers and other information and communications technologies, without consideration of the expanded uses of such devices

² In the first judicial validation of wiretapping, Justice Brandeis of the United States Supreme Court wrote a scathing dissent that noted that wiretapping was a “subtler and more far-reaching means of invading privacy” that could not be justified under the Constitution. In a chillingly accurate forecast, the eminent jurist predicted: “Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrence of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.” *Olmstead v. United States*, 277 U.S. 438 (1928).

and the implications for individuals' rights. At the same time, the absence of laws to regulate global communications surveillance and sharing arrangements has resulted in ad hoc practices that are beyond the supervision of any independent authority. Today, in many States, access to communications data can be conducted by a wide range of public bodies for a wide range of purposes, often without judicial authorization and independent oversight. In addition, States have sought to adopt surveillance arrangements that purport to have extra-territorial effect.

18. Human rights mechanisms have been equally slow to assess the human rights implications of the Internet and new technologies on communications surveillance and access to communications data. The consequences of expanding States' surveillance powers and practices for the rights to privacy and freedom of opinion and expression, and the interdependence of those two rights, have yet to be comprehensively considered by the Human Rights Council, special procedures mandate holders or human rights treaty bodies. This report seeks to rectify this.

IV. International human rights framework

19. The right to freedom of opinion and expression is guaranteed under articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which affirm that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of all kinds through any media and regardless of frontiers. At the regional level, the right is protected by the African Charter on Human and Peoples' Rights (art. 9), the American Convention on Human Rights (art. 13); and the Convention for the Protection of Human Rights and Fundamental Freedoms (art. 10).

20. At both the international and regional levels, privacy is also unequivocally recognized as a fundamental human right. The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (ICCPR, art. 17), the Convention on the Rights of the Child (art. 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14). At the regional level, the right to privacy is protected by the European Convention on Human Rights (art. 8) and the American Convention on Human Rights (art. 11).

21. Despite the widespread recognition of the obligation to protect privacy, the specific content of this right was not fully developed by international human rights protection mechanisms at the time of its inclusion in the above-mentioned human rights instruments. The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement.³ As the right to privacy is a qualified right, its interpretation raises challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest. The rapid and monumental changes to communications and information technologies experienced in recent decades have also irreversibly affected our understandings of the boundaries between private and public spheres.

22. Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited

³ UNESCO, Global Survey on Internet Privacy and Freedom of Expression, 2012, p. 51.

intervention by other uninvited individuals.⁴ The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used.

23. In order for individuals to exercise their right to privacy in communications, they must be able to ensure that these remain private, secure and, if they choose, anonymous. Privacy of communications infers that individuals are able to exchange information and ideas in a space that is beyond the reach of other members of society, the private sector, and ultimately the State itself. Security of communications means that individuals should be able to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion. Anonymity of communications is one of the most important advances enabled by the Internet, and allows individuals to express themselves freely without fear of retribution or condemnation.

A. Interrelations between the rights to privacy to freedom of opinion and expression

24. The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization. In this regard, article 17 of ICCPR refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communication, both online and offline.⁵ As the Special Rapporteur noted in a previous report,⁶ the right to private correspondence gives rise to a comprehensive obligation of the State to ensure that e-mails and other forms of online communication are actually delivered to the desired recipient without the interference or inspection by State organs or by third parties.⁷

25. The Human Rights Committee analysed the content of the right to privacy (art. 17) in its General Comment No. 16 (1988), according to which article 17 aims to protect individuals from any unlawful and arbitrary interferences with their privacy, family, home, or correspondence, and national legal frameworks must provide for the protection of this right. This provision imposes specific obligations relating to the protection of privacy in communications, underlining that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read. "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited."⁸ The General Comment also indicates that "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."⁹ At the time this General Comment was

⁴ Lord Lester and D. Pannick (eds.). *Human Rights Law and Practice*. London, Butterworth, 2004, para. 4.82.

⁵ ICCPR commentary, p.401.

⁶ A/HRC/17/23.

⁷ ICCPR commentary, p.401.

⁸ Centre for Civil and Political Rights (CCPR) General Comment No. 16. (General Comments), p.8.

⁹ *Ibid.*, p.10.

adopted, the impact of advances in information and communications technologies on the right to privacy was barely understood.

26. In its General Comment No. 34 (2011) on the right to freedom of expression, the Human Rights Committee indicated that States parties should take account of the extent to which developments in information and communication technologies have substantially changed communication practices. The Committee also called on States parties to take all necessary steps to foster the independence of these new media. The General Comment also analyses the relationship between the protection of privacy and freedom of expression, and recommends that States parties respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose information sources.¹⁰

27. Tensions also exist between the right to privacy and the right to freedom of expression, for example, when information considered to be private is disseminated through the media. In this sense, article 19 (3) provides for restrictions on freedom of expression and information to protect the rights of others. However, as it happens for all permissible limitations to the right to freedom of expression (see below), the principle of proportionality must be strictly observed, since there is otherwise danger that freedom of expression would be undermined. Particularly in the political arena, not every attack on the good reputation of politicians must be permitted, since freedom of expression and information would otherwise be stripped of their crucial importance for the process of forming political opinions,¹¹ advocating for transparency and combating corruption. The international jurisprudence at regional level indicates that in situations of conflict between privacy and freedom of expression, reference should be made to the overall public interest on the matters reported.¹²

B. Permissible limitations to privacy and freedom of expression

28. The framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations. In contrast with the provisions of article 19, paragraph 3, which spell out elements of a test for permissible limitations,¹³ the formulation of article 17 does not contain a limitation clause. Despite these differences in wording, it is understood that article 17 of the Covenant should also be interpreted as containing elements of a permissible limitations test already described in other General Comments of the Human Rights Committee.¹⁴

29. In this regard, the Special Rapporteur takes the position that the right to privacy should be subject to the same permissible limitations test as the right to freedom of movement, as elucidated in General Comment 27.¹⁵ The test as expressed in the comment includes, *inter alia*, the following elements:

- (a) Any restrictions must be provided by the law (paras. 11-12);
- (b) The essence of a human right is not subject to restrictions (para. 13);

¹⁰ CCPR General Comment No. 34.

¹¹ Nowak, Manfred, *United Nations Covenant on Civil and Political Rights: CCPR Commentary* (1993), p.462

¹² UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, pp. 53 and 99.

¹³ Lists of permissible limitations are also included in art. 12, (3), on the right to liberty of movement and freedom to choose his residence; art. 18, (3), on the right to freedom of thought, conscience and religion; art. 21, on the right of peaceful assembly; and art. 22, (2), on the right to freedom of association.

¹⁴ *Ibid.*

¹⁵ See also CCPR General Comment No. 34.

- (c) Restrictions must be necessary in a democratic society (para. 11);
- (d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
- (e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim (para. 14);
- (f) Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected (paras. 14-15).

C. Recent considerations by international mechanisms for the protection of human rights

30. In previous reports, the Special Rapporteur has assessed the impact of the Internet on the realization of the right to freedom of opinion and expression (A/HRC/17/27 and A/66/290). He noted that, while Internet users can enjoy relative anonymity on the Internet, States and private actors also have access to new technologies to monitor and collect information about individuals' communications and activities. Such technologies have the potential to violate the right to privacy, thereby undermining people's confidence and security on the Internet and impeding the free flow of information and ideas online. The Special Rapporteur urged States to adopt effective privacy and data protection laws in accordance with human rights standards, and to adopt all appropriate measures to ensure that individuals can express themselves anonymously online.¹⁶

31. Other Special Procedures mandate holders considered the issue of interferences with the right to privacy. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism studied developments in surveillance practices and technologies that have adversely affected the right to privacy using the justification of combating terrorism.¹⁷ The Special Rapporteur underscored that these measures have not only led to violations of the right to privacy, but have also had an impact on due process rights and the rights to freedom of movement, freedom of association and freedom of expression. He urged Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to protect against abuse. The Special Rapporteur also called for the adoption of comprehensive data protection and privacy laws and the establishment of strong independent oversight bodies mandated to review the use of intrusive surveillance techniques and the processing of personal information. He further called for research and development resources to be devoted to privacy-enhancing technologies.

32. Other human rights protection mechanisms have also recently paid attention to the impact of the surveillance of communications on the protection of the rights to privacy and freedom of expression. The Human Rights Committee voiced concerns, for example, at allegations of State monitoring the use of the Internet and blocking access to some websites¹⁸ and recommended the review of legislation providing the executive with wide powers of surveillance in respect of electronic communications.¹⁹ The Universal Periodic

¹⁶ A/HRC/17/27, p.22.

¹⁷ A/HRC/13/37.

¹⁸ CCPR/C/IRN/CO/3.

¹⁹ CCPR/C/SWE/CO/6.

Review has also included recommendations to ensure, for example, that legislation relating to the Internet and other new communication technologies respects international human rights obligations.²⁰

V. Modalities of communications surveillance

33. Modern surveillance technologies and arrangements that enable States to intrude into an individual's private life threaten to blur the divide between the private and the public spheres. They facilitate invasive and arbitrary monitoring of individuals, who may not be able to even know they have been subjected to such surveillance, let alone challenge it. Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.

A. Targeted communications surveillance

34. States have access to a number of different techniques and technologies to conduct communications surveillance of a targeted individual's private communications. Real-time interception capabilities allow States to listen to and record the phone calls of any individual using a fixed line or mobile telephone, through the use of interception capabilities for State surveillance that all communications networks are required to build into their systems.²¹ An individual's location can be ascertained, and their text messages read and recorded. By placing a tap on an Internet cable relating to a certain location or person, State authorities can also monitor an individual's online activity, including the websites he or she visits.

35. Access to the stored content of an individual's e-mails and messages, in addition to other related communications data, can be obtained through Internet companies and service providers. The initiative of the European standards-setting authority, the European Telecommunications Standards Institute, to compel cloud providers²² to build "lawful interception capabilities" into cloud technology to enable State authorities to have direct access to content stored by these providers, including e-mails, messages and voicemails, raises concerns.²³

36. States can track the movements of specific mobile phones, identify all individuals with a mobile phone within a designated area, and intercept calls and text messages, through various methods. Some States use off-the-air mobile monitoring devices called International Mobile Subscriber Identity (IMSI) catchers, which can be installed in a location temporarily (such as at a protest or march) or permanently (such as at an airport or other border crossings). These catchers imitate a mobile phone tower by sending and

²⁰ A/HRC/14/10.

²¹ See, for example, the United States Communications Assistance for Law Enforcement Act 1994 (United States); Telecommunications Act 1997, Part 15 (Australia); Regulation of Investigatory Powers Act 2000, ss12-14 (United Kingdom); Telecommunications (Interception Capability) Act 2004.

²² A cloud provider offers services of networked online storage of data.

²³ ETSI DTR 101 567 VO.0.5 (2012-14), Draft Technical Report: Lawful Interception (LI); Cloud/Virtual Services (CLI).

responding to mobile phone signals in order to extract the unique subscriber identification module (SIM) card number of all mobile phones within a certain territory.

37. States are also increasingly acquiring software that can be used to infiltrate an individual's computer, mobile phone or other digital device.²⁴ Offensive intrusion software, including so-called "Trojans" (also known as spyware or malware), can be used to turn on the microphone or camera of a device, to track the activity conducted on the device, and to access, alter or delete any information stored on the device. Such software enables a State to have complete control of the device infiltrated, and is virtually undetectable.

B. Mass communications surveillance

38. Costs and logistical hurdles to conduct surveillance on a mass scale continue to decline rapidly, as technologies allowing for broad interception, monitoring and analysis of communications proliferate. Today, some States have the capability to track and record Internet and telephone communications on a national scale. By placing taps on the fibre-optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications. Such systems were reportedly adopted, for example, by the Egyptian and Libyan Governments in the lead-up to the Arab Spring.²⁵

39. In many States, mandatory data retention is facilitating massive collection of communications data that can later be filtered and analysed. Technologies enable the State to scan phone calls and text messages to identify the use of certain words, voices or phrases, or filter Internet activity to determine when an individual visits certain websites or accesses particular online resources. "Black boxes" can be designed to inspect the data flowing through the Internet in order to filter through and deconstruct all information about online activity. This method, called "deep-packet inspection", allows the State to go beyond gaining simple knowledge about the sites that individuals visit, and instead analyse the content of websites visited. Deep-packed inspection, for example, has been reportedly employed by States confronted with recent popular uprisings in the Middle East and North Africa region.²⁶

40. Another tool used regularly by States today is social media monitoring. States have the capacity physically to monitor activities on social networking sites, blogs and media outlets to map connections and relationships, opinions and associations, and even locations. States can also apply highly sophisticated data mining technologies to publicly available information or to communications data provided by third party service providers. At a more basic level, States have also acquired technical means to obtain usernames and passwords from social networking sites such as Facebook.²⁷

C. Access to communications data

41. In addition to intercepting and tracking the content of individuals' communications, States may also seek access to communications data held by third party service providers and Internet companies. As the private sector collects progressively larger amounts of

²⁴ Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, and Natalia Torres, *Global Survey on Internet Privacy and Freedom of Expression*, *UNESCO Series on Internet Freedom* (2012), p. 41.

²⁵ European Parliament, Directorate-General for External Policies, Policy Department, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), pp. 9-10.

²⁶ Mendel *et al.*, *op. cit.*, p. 43.

²⁷ European Parliament, *op. cit.*, p. 6.

varied data that reveal sensitive information about peoples' daily lives, and individuals and businesses choose to store the content of their communications, such as voicemails, e-mails and documents, with third party service providers, access to communications data is an increasingly valuable surveillance technique employed by States.

42. The communications data collected by third party service providers, including large Internet companies, can be used by the State to compose an extensive profile of concerned individuals. When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone.²⁸ By combining information about relationships, location, identity and activity, States are able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with.

43. Instances of access to communications data by States are growing rapidly. In the three years that Google has been reporting the numbers of requests for communications data it receives, such requests have almost doubled, from 12,539 in the last six months of 2009, to 21,389 in the last six months of 2012.²⁹ In the United Kingdom, where law enforcement authorities are empowered to self-authorize their own requests for communications information, approximately 500,000 such requests were reported every year.³⁰ In the Republic of Korea, a country of nearly 50 million people, there are approximately 37 million requests for communications data reported every year.³¹

D. Internet filtering and censorship

44. Advances in technology have not only facilitated interception of and access to communications in specific cases, but have also enabled States to conduct widespread, even nationwide, filtering of online activity. In many countries, Internet filtering is conducted under the guise of maintaining social harmony or eradicating hate speech, but is in fact used to eradicate dissent, criticism or activism.

45. Filtering technologies mentioned above also facilitate the monitoring of web activity in order to enable the State to detect forbidden images, words, site addresses or other content, and censor or alter it. States can use such technologies to detect the use of specific words and phrases, in order to censor or regulate their use, or identify the individuals using them. In countries with high levels of Internet penetration, Internet filtering reportedly enables the censorship of website content and communications and facilitates the surveillance of human rights defenders and activists.³²

46. In addition to technologies that facilitate filtering and censorship, many States are conducting manual Internet filtering, by creating online police forces and inspectors in order to physically monitor the content of websites, social networks, blogs and other forms

²⁸ Alberto Escudero-Pascual and Gus Hosein, "Questioning lawful access to traffic data", *Communications of the ACM*, Volume 47 Issue 3, March 2004, pp. 77–82.

²⁹ See <http://www.google.com/transparencyreport/userdatarequests/>.

³⁰ See <http://www.intelligencecommissioners.com/docs/0496.pdf>.

³¹ Money Today, 23 October, 2012, citing the disclosure made by the Korean Communication Commission for the Annual National Audit of 2013 to Assemblywoman Yoo Seung-Hui, <http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1>.

³² European Parliament, Directorate-General for External Policies, Policy Department, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), p. 12.

of media. In some States, “cyber police forces” are tasked with inspecting and controlling the Internet, searching websites and critical nodes within websites (particularly online discussion forums) with a view to block or shut down websites whenever they contain content the Government disapproves of, including or criticism of the country’s leadership. The burden of such policing is transferred to private intermediaries, such as search engines and social network platforms, through laws that widen liability for proscribed content from the original speaker to all intermediaries.

E. Restrictions on anonymity

47. One of the most important advances facilitated by the advent of the Internet was the ability to anonymously access and impart information, and to communicate securely without having to be identified. Initially, this was possible given that there was no “identity layer” to the Internet; originally, it was not possible to know who was behind a specific communication, e-mail address, or even a given computer. However, in the name of security and law enforcement, gradually States have been eradicating the opportunities for anonymous communication. In many States, individuals must identify themselves at cybercafés and have their transactions on public computers recorded. Increasingly, identification and registration are also required when buying a SIM card or mobile telephone device, for visiting certain major websites, or for making comments on media sites or blogs.

48. Restrictions on anonymity facilitate State communications surveillance by simplifying the identification of individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of State surveillance.

49. In this sense, restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas. They can also result in individuals’ de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities. Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate actors to protect the privacy and security of such data.

VI. Concerns on national legal standards

50. Generally, legislation has not kept pace with the changes in technology. In most States, legal standards are either non-existent or inadequate to deal with the modern communications surveillance environment. As a result, States are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognizing that the expanded capabilities they now possess go far beyond what such frameworks envisaged. In many countries, this means that vague and broadly conceived legal provisions are being invoked to legitimize and sanction the use of seriously intrusive techniques. Without explicit laws authorizing such technologies and techniques, and defining the scope of their use, individuals are not able to foresee – or even know about – their application. At the same time, laws are being adopted to broaden the breadth of national security exceptions, providing for the legitimization of intrusive surveillance techniques without oversight or independent review.

51. Inadequate legal standards increase the risk of individuals being exposed to violation of their human rights, including the right to privacy and the right to freedom of expression. They also have an adverse impact on certain groups of individuals – for example, members of certain political parties, trade unionists or national, ethnic and linguistic minorities – who

may be more vulnerable to State communications surveillance. Without strong legal protections in place, journalists, human rights defenders and political activists risk being subjected to arbitrary surveillance activities.

52. Surveillance of human rights defenders in many countries has been well documented. On these occasions, human rights defenders and political activists report having their phone calls and e-mails monitored, and their movements tracked. Journalists are also particularly vulnerable to becoming targets of communications surveillance because of their reliance on online communication. In order to receive and pursue information from confidential sources, including whistleblowers, journalists must be able to rely on the privacy, security and anonymity of their communications. An environment where surveillance is widespread, and unlimited by due process or judicial oversight, cannot sustain the presumption of protection of sources. Even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse.

53. The following subsections list common concerns regarding laws that allow State surveillance of communications surveillance in circumstances that threaten the rights to freedom of expression and privacy.

A. Lack of judicial oversight

54. Whereas traditionally communications surveillance was required to be authorized by the judiciary, increasingly this requirement is being weakened or removed. In some countries, interception of communications can be authorized by a governmental minister, their delegate, or a committee. In the United Kingdom, for example, interception of communications is authorized by the Secretary of State;³³ in Zimbabwe, interception of communications is authorized by the Minister for Transport and Communication.³⁴ Progressively, communications surveillance can also be authorized on a broad and indiscriminate basis, without the need for law enforcement authorities to establish the factual basis for the surveillance on a case-by-case basis.

55. Many States have dispensed with the need for law enforcement agencies to return to the court for ongoing supervision after an interception order is issued. Under the Kenyan Prevention of Terrorism Act 2012, for example, interception of communications can be conducted over an indefinite period of time, without any requirement that law enforcement agencies report back to a court or seek an extension. Some States impose time limits on the execution of interception orders but enable law enforcement authorities to renew such orders repeatedly and indefinitely.

56. Even when judicial authorization is required by law, often it is de facto an arbitrary approval of law enforcement requests. This is particularly the case where the threshold required to be established by law enforcement is low. For example, the Ugandan Regulation of Interception of Communications Act 2010 only requires law enforcement authorities to demonstrate that “reasonable” grounds exist to allow the interception to take place. In such instances, the burden of proof to establish the necessity for surveillance is extremely low, given the potential for surveillance to result in investigation, discrimination or violations of human rights. In other countries, a complex array of laws authorizes access to and surveillance of communications under a range of different circumstances. In Indonesia, for example, the Psychotropic Law, Narcotics Law, Electronic Information and Transaction

³³ Section 5, Regulation of Investigatory Powers Act 2000.

³⁴ Section 5, Interception of Communications Act 2006.

Law, Telecommunications Law and the Corruption Law all contain communications surveillance components. In the United Kingdom, over 200 agencies, police forces and prison authorities are authorized to acquire communications data under the Regulation of Investigatory Powers Act, 2000. As a result, it is difficult for individuals to foresee when and by which State agency they might be subjected to surveillance.

57. In many States, communication service providers are being compelled to modify their infrastructure to enable direct surveillance, eliminating the opportunity for judicial oversight. For example, in 2012 the Colombian Ministries of Justice, and Information and Communication Technologies, issued a decree that required telecommunication service providers to put in place infrastructure allowing direct access to communications by judicial police, without an order from the Attorney General.³⁵ The above-mentioned Uganda's Regulation of Interception of Communications Act 2010 (s3) provides for the establishment of a monitoring centre and mandates that telecommunications providers ensure that intercepted communications are transmitted to the monitoring centre (s8(1)(f)). The Government of India is proposing to install a Centralized Monitoring System that will route all communications to the central Government, allowing security agencies to bypass interaction with the service provider.³⁶ Such arrangements take communications surveillance out of the realm of judicial authorization and allow unregulated, secret surveillance, eliminating any transparency or accountability on the part of the State.

B. National security exceptions

58. Vague and unspecified notions of "national security" have become an acceptable justification for the interception of and access to communications in many countries. In India, for example, the Information Technology Act of 2008 allows interception of communications in the interest of, *inter alia*, "the sovereignty, integrity, or defense of India, friendly relations with foreign States, public order and the investigation of any offence" (section 69).

59. In many cases, national intelligence agencies also enjoy blanket exceptions to the requirement for judicial authorization. For example, in the United States, the Foreign Intelligence Surveillance Act empowers the National Security Agency to intercept communications without judicial authorization where one party to the communication is located outside the United States, and one participant is reasonably believed to be a member of a State-designated terrorist organization. German law allows warrantless automated wiretaps of domestic and international communications by the State's intelligence services for the purposes of protecting the free democratic order, existence or security of the State.³⁷ In Sweden, the Law on Signals Intelligence in Defense Operations authorizes the Swedish intelligence agency to intercept without any warrant or court order all telephone and Internet traffic that take place within Sweden's borders. In the United Republic of Tanzania, the Intelligence and Security Service Act 1996 enables the country's intelligence services to conduct any investigations and investigate any person or body which it has reasonable cause to consider a risk or a source of risk or a threat to the State security.

60. The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern.³⁸ The concept is broadly defined

³⁵ Ministries of Justice and ICTs Decree 1704. Rooted in the Criminal Procedure Code of 2004.

³⁶ Department of Communications. Government of India. Annual Report 2011-2012 pg. 58 – <http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf>.

³⁷ G-10 law.

³⁸ Counter-terrorism Human Rights Council resolutions.

and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.

C. Unregulated access to communications data

61. Access to communications data held by domestic communications service providers is often mandated by legislation or a condition upon which licences are issued. As a result, States are generally provided with *carte blanche* access to communications data with little oversight or regulation. For example, a 2012 Brazilian law on money laundering gives police the power to access registration information from Internet and communication providers without a court order.³⁹ At the international level, the provision of access to communications data is regulated by bilateral Mutual Legal Assistance Treaties. However, this cooperation also often occurs outside of the law on the basis of the voluntary compliance of the service provider or Internet company. As such, access to communications data can be obtained in many States without independent authorization and with limited oversight.

D. Extra-legal surveillance

62. A number of the surveillance capabilities listed above fall outside of existing legal frameworks, but have nevertheless been widely adopted by States. Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings. Mass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception.

63. Governments often do not acknowledge the use of such technologies to conduct surveillance, or argue that such technologies are being legitimately employed under the ambit of existing surveillance legislation. Although it is clear that many States possess offensive intrusion software, such as Trojan technology, the legal basis for its use has not been publicly debated in any State, with the exception of Germany. In that context, the province of North Rhine-Westphalia passed legislation in 2006 authorizing the “secret access to an information technology system” (§ 5.2 no. 11, North Rhine-Westphalia Constitution Protection Act), which was understood to be technical infiltration which is effected either by installing a spy programme or taking advantage of the security loopholes of the system. The German Federal Constitutional Court quashed the law in February 2008, ruling that such measures would only be in conformity with human rights if they were

³⁹ Brazilian Federal Law 12683/2012. Article 17-B. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

subject to judicial authorization and review, and occurred only in situations where there might be a concrete danger to a predominantly important legal interest.⁴⁰

E. Extra-territorial application of surveillance laws

64. In response to the increased data flows across borders and the fact the majority of communications are stored with foreign third party service providers, a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions. This raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies. In South Africa, for example, the General Intelligence Laws Amendment Bill allows for surveillance of foreign communications outside of South Africa or passing through South Africa.⁴¹ In October 2012, the Dutch Ministry of Justice and Security proposed legislative amendments to the Dutch Parliament that would allow the police to break into computers and mobile phones both within the Netherlands and abroad in order to install spyware and search and destroy data.⁴² In December 2012, Pakistan's National Assembly passed the Fair Trial Act of 2012, paragraph 31 of which provides for the execution of surveillance warrants in foreign jurisdictions. Later that month, the United States renewed the Foreign Intelligence Surveillance Amendment Act of 2008 extending the Government's power to conduct surveillance of non-American persons located outside the United States (§1881a), including any foreign individual whose communications are hosted by cloud services located in the United States (such as Google and other large Internet companies).⁴³ Also in 2012, the European Telecommunications Standards Institute created draft standards for interception of foreign cloud-based services by European Governments.⁴⁴ These developments suggest an alarming trend towards the extension of surveillance powers beyond territorial borders, increasing the risk of cooperative agreements between State law enforcement and security agencies to enable the evasion of domestic legal restrictions.

F. Mandatory data retention

65. In order to increase the storage of communications data that they are able to access, some States are adopting mandatory data retention laws requiring Internet and telecom service providers (collectively, "communications service providers") continuously to collect and preserve communications content and information about users' online activities. Such laws enable the compilation of historical records about individuals' e-mails and messages, locations, interactions with friends and family, etc.

⁴⁰ Available in German. BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

⁴¹ Section 1. c. General Intelligence Laws Amendment Bill. Available at: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

⁴² See <http://www.edri.org/edriagram/number10.20/dutch-proposal-state-spyware>.

⁴³ See European Parliament Directorate-General for Internal Policies Policy Department C: Citizens Rights and Constitutional Affairs, *Fighting crime and protecting privacy in the cloud: study*, 2012.

⁴⁴ Draft ESTI DTR 101 567 Lawful Interception (LI) Vo.1.0 (2012 - 05); Cloud/Virtual Services (CLI). Available at: www.3gpp.org.

66. In delivering services to their users, communications service providers give subscribers' devices or network an Internet Protocol (IP) address⁴⁵ that changes periodically. Information about an IP address can be used to ascertain the identity and location of an individual and track their online activity. Mandatory data retention laws force communications service providers to keep records of their IP address allocations for a certain period of time, allowing the State greater ability to require communications service providers to identify an individual on the basis of who had a given IP address at a particular date and time. Some States are also now seeking to compel third party service providers to collect and retain information that they would not normally collect.

67. National data retention laws are invasive and costly, and threaten the rights to privacy and free expression. By compelling communications service providers to create large databases of information about who communicates with whom via a telephone or the Internet, the duration of the exchange, and the users' location, and to keep such information (sometimes for years), mandatory data retention laws greatly increase the scope of State surveillance, and thus the scope for infringements upon human rights. Databases of communications data become vulnerable to theft, fraud and accidental disclosure.

G. Identity disclosure laws

68. In many States, laws require the provision of identification at cybercafés. Such laws are particularly problematic in countries where personal computer ownership is low and individuals rely heavily on publicly available computers. In India, for example, the Information Technology (Guidelines for Cyber Cafes) Rules 2011 require that cybercafé owners obtain identification documents from any individual visiting the cybercafé, which records must be kept for at least one year (Rule 4(2)). The cybercafé must maintain a log-register, containing, among other information, log in time and log out time, and computer terminal identification for a minimum period of one year (Rule 5(1) & 5(2)); store and maintain backups of log records of each access or login by any user for at least one year (Rule 5(4)).

69. Individuals are now also required to use their real names online in many States, and to provide official identification in order to establish their identity. In the Republic of Korea, the Information Communications Law, adopted in 2007, required users to register their real names before accessing websites with more than 100,000 visitors per day, ostensibly in order to reduce online bullying and hate speech. The law was recently overturned by the Constitutional Court on the basis that it restricted freedom of speech and undermined democracy.⁴⁶ China recently adopted the Decision to Strengthen the Protection of Online Information, requiring Internet and telecommunications providers to collect personal information about users when they sign up for Internet access, landline, or mobile phone service. Service providers allowing users to publish online are required to be able to link screen names and real identities. These real name registration requirements allow authorities to more easily identify online commentators or tie mobile use to specific individuals, eradicating anonymous expression.⁴⁷

⁴⁵ An IP address is a unique numeric code that identifies all computers or other devices connected to the Internet.

⁴⁶ Constitutional Court Decision 2010Hun-Ma47 ("Real names" decision), 23 August 2012. An official summary of the Court's decision is available on the Court's website at http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp only in Korean.

⁴⁷ "China to Strengthen Internet Information Protection" - <http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm>.

70. A further initiative preventing communications anonymity is the gradual adoption of policies that require the registration of SIM cards with a subscriber's real name or government-issued identity document. In 48 countries in Africa, laws requiring individuals to register their personal information with their network provider prior to activation of pre-paid SIM cards are reportedly facilitating the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location-tracking, and simplifying communications surveillance.⁴⁸ In the absence of data protection legislation, SIM users' information can be shared with Government departments and matched with other private and public databases, enabling the State to create comprehensive profiles of individual citizens. Individuals are also at risk of being excluded from use of mobile phone services (which may enable not only communication but also access to financial services) if they are unable or unwilling to provide identification to register.

H. Restrictions on encryption and key disclosure laws

71. The security and anonymity of communications are also undermined by laws that limit the use of privacy-enhancing tools that can be used to protect communications, such as encryption. Many States have now adopted laws that mandate an individual enable decryption when so ordered. The South African Regulation of Interception of Communications and Provisions of Communication-Related Information Act of 2002 requires decryption assistance from any person who possesses the decryption key.⁴⁹ Similar laws exist in Finland (Section 4(4)(a) Coercive Measures Act 1987/450), Belgium (Art. 9, Law on computer crime of 28 November 2000), and Australia (Sections 12 and 28 Cybercrime Act 2001).

VII. The roles and responsibilities of the private sector

72. The vital developments in technology that have enabled new and dynamic forms of communication have been occurred primarily in the private sector. In this sense, many of the changes in the way we communicate, receive and impart information are based on the research and innovations of corporate actors.

73. The private sector has also played a key role in facilitating State surveillance of individuals, in a number of ways. Corporate actors have had to respond to requirements that digital networks and communications infrastructure be designed to enable intrusion by the State. Such requirements were originally adopted by States in the 1990s and are becoming compulsory for all communications services providers. Increasingly, States are adopting legislation requiring that communications service providers allow States direct access to communications data or modify infrastructure to facilitate new forms of State intrusion.

74. In developing and deploying new technologies and communications tools in specific ways, corporate actors have also voluntarily taken measures that facilitate State surveillance of communications. In its simplest manifestation, this collaboration has taken the form of decisions on how corporate actors collect and process information, which allows them to

⁴⁸ Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance," Information Systems and Innovation Group Working Paper Series, no. 186, London School of Economics and Political Science (2012).

⁴⁹ Section 29. South African Regulation of Interception of Communications and Provisions of Communication - Related Information Act 2002. Available at: <http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf>.

become massive repositories of personal information that are then accessible to States upon demand. Corporate actors have adopted specifications that enable State access or intrusion, collect excessive and revelatory information, or restrict the application of encryption and other techniques that could limit access to information by both the companies and governments. The private sector has also often failed to deploy privacy-enhancing technologies, or has implemented them less than secure ways that do not represent the state of the art.

75. In the most serious circumstances, the private sector has been complicit in developing technologies that enable mass or invasive surveillance in contravention of existing legal standards.⁵⁰ The corporate sector has generated a global industry focused on the exchange of surveillance technologies. Such technologies are often sold to countries in which there is a serious risk that they will be used to violate human rights, particularly those of human rights defenders, journalists or other vulnerable groups. This industry is virtually unregulated as States have failed to keep pace with technological and political developments.

76. States' human rights obligations require that they not only respect and promote the rights to freedom of expression and privacy, but protect individuals from violations of human rights perpetrated by corporate actors. In addition, States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights.⁵¹ Human rights obligations in this regard apply when corporate actors are operating abroad.⁵²

77. States must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard.

VIII. Conclusions and recommendations

78. **Communications techniques and technologies have evolved significantly, changing the way in which communications surveillance is conducted by States. States must therefore update their understandings and regulation of communications surveillance and modify their practices in order to ensure that individuals' human rights are respected and protected.**

79. **States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.**

⁵⁰ For some examples of surveillance technology designed by the private sector and utilized in Libya, Bahrain, the Syrian Arab Republic, Egypt and Tunisia, see European Parliament, Directorate-General for External Policies, Policy Department, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), pp. 9-10.

⁵¹ Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Principle 5.

⁵² Human Rights Committee, Concluding Observations, Germany, December 2012.

80. In order to meet their human rights obligations, States must ensure that the rights to freedom of expression and privacy are at the heart of their communications surveillance frameworks. To this end, the Special Rapporteur recommends the following:

A. Updating and strengthening laws and legal standards

81. Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.

82. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.

83. Legal frameworks must ensure that communications surveillance measures:

- (a) Are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application;
- (b) Are strictly and demonstrably necessary to achieve a legitimate aim; and
- (c) Adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

84. States should criminalize illegal surveillance by public or private actors. Such laws must not be used to target whistleblowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens.

85. The provision of communications data by the private sector to States should be sufficiently regulated to ensure that individuals' human rights are prioritized at all times. Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted.

86. The provision of communications data to the State should be monitored by an independent authority, such as a court or oversight mechanism. At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors.

87. Surveillance techniques and practices that are employed outside of the rule of law must be brought under legislative control. Their extra-legal usage undermines basic principles of democracy and is likely to have harmful political and social effects.

B. Facilitating private, secure and anonymous communications

88. States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés or mobile telephony.

89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys.

90. States should not retain or require the retention of particular information purely for surveillance purposes.

C. Increasing public access to information, understanding and awareness of threats to privacy

91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications.

94. States should raise public awareness on the uses of new communication technologies in order to support individuals in properly assessing, managing, mitigating and making informed decisions on communications-related risks.

D. Regulating the commercialization of surveillance technology

95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection.

96. States must refrain from forcing the private sector to implement measures compromising the privacy, security and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations.

E. Furthering the assessment of relevant international human rights obligations

98. There is a significant need to advance international understanding on the protection of the right to privacy in light of technological advancements. The Human Rights Committee should consider issuing a new General Comment on the right to privacy, to replace General Comment No. 16 (1988).

99. Human rights mechanisms should further assess the obligations of private actors developing and supplying surveillance technologies.
