OFFICE FOR FOREIGN AFFAIRS
PRINCIPALITY OF LIECHTENSTEIN

Response of the Principality of Liechtenstein

to the Note Verbale of the Office of the United Nations High Commissioner for Human Rights dated 26 February 2014 on the GA resolution 68/167 ("The right to privacy in the digital age") and the corresponding questionnaire

Q1: What measures have been taken at national level to ensure respect for and protection of the right to privacy, including in the context of digital communication?

The right to private life is protected by Article 32 of the **Constitution**, which guarantees personal liberty, the immunity of the home, and the inviolability of letters and written matter. According to the Constitution, searches of houses or persons, letters, or written matter, and seizure of letters or written matter may only be undertaken in the particular cases and manner specified by law. In a verdict of the Criminal Court it has been stated that "data protection or the protection of the "informational integrity" […] is a subsidiary aspect of the protection of privacy according to Art. 32 Para. 1 Constitution and Art. 8 ECHR".[1] This legal interpretation of the right to privacy as set out in Art. 32 Para. 1 Constitution and Art. 8 ECHR corresponds with the principle set out in paragraph 2 of Resolution 68/167, according to which people should have the same rights online as they have offline.

Legal provisions concerning searches of houses and persons, letters, and written matter (including digital communication), as well as their seizure and surveillance, can be found in the Criminal Code, the Code of Criminal Procedure, the Police Act, the Mutual Legal Assistance Act, the Persons and Companies Act, the Communications Act and the Data Protection Act. All permissible violations of the right to privacy are subject to the principle of proportionality and illegal violations are sanctioned by appropriate measures. Art. 118 of the Criminal Code for example makes the violation of the privacy of letters and telecommunications a punishable offense and sanctions it with up to three months in jail and a monetary penalty of up to 360 daily rates. Section 2 of the Persons and Companies Act regulates violations of personal rights such as one's personal and mental integrity and ensures the "determination of the circumstances, elimination (cessation) of the

[1] http://www.gerichtsentscheidungen.li/default.aspx?mode=suche&txt=Datenschutz&gericht=2&id=3214&backurl=?mode=suche%26txt=Datenschutz%26gericht=2

interference, restoration of the earlier state of affairs through revocation and the like, and omission of further interference (Art. 39 paragraph 1) and entitlement to damages (Art. 40 paragraph 1)."

The Liechtenstein **Data Protection Act**, which entered into force on 1 August 2002 (LGBl. 2002 No. 55) seeks to protect the personality and fundamental rights of those individuals about whom data is processed (Art. 1 Abs. 1 DSG). The act implements Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data into Liechtenstein law. It determines the principle according to which personal data resulting from the use of data entrusted or made accessible to a person for professional reasons are to be kept secret, to the extent that there is no lawful grounds for the transmission of the data. According to the Data Protection Act, data entitled to particular protection include data concerning religious, ideological, and political views or activities, health, the private sphere or racial affiliation, measures relating to social welfare, and administrative or criminal prosecutions and punishments. The Data Protection Act also created a control mechanism to supervise compliance with the provisions of this act. More detailed information can be found in the response to question 4.

In the context of digital communications, the **Communications Act** (Law of 17 March 2006 on Electronic Communications) foresees - on the one hand - minimum requirements for public communications networks and services. Art. 16 paragraph 1 of the Communications Act states that operators of public communications networks must ensure that - amongst others - the networks comply with the recognized technical rules, especially in regard to the safety of electronic communications services, safe network operations, network integrity and the avoidance of electromagnetic interference with other networks.

On the other hand Chapter XI. of the Communications Act sets out in particular the rights and duties relating to communications secrecy, data protection and participation duties. Pursuant to Art. 48 paragraph 2 Communications Act all providers and all persons participating in the activities of a provider shall be subject to the communications secrecy requirement. The basic principle as regards data protection is set out in Article 49 Communications Act, which allows the processing of traffic, location, content or subscriber data by a provider only to the absolutely necessary extent. Special requirements as regards the participation in the determination of a location are set out in Article 51. The following articles deal with the participation in a surveillance: According to Art. 53 paragraph 1 Communications Act providers of publicly available communications services shall record all subscriber data and store them for the entire duration of the contractual relationship as well as six months after the termination thereof. Art. 53 paragraph 2 Communications Act concerns the information providers are required to provide to the investigating judge upon his order or to the National Police upon their written request.

In 2010 Liechtenstein decided to implement „Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC" into national law. Since then, pursuant to Art. 52 paragraph 1 c)

Communications Act providers of publicly available electronic communications services and operators of a public communications network are required to store retained data for the purpose of participating in a surveillance in accordance with article 52a. Retained data must be stored for a period of six months from the time the communication process is terminated and shall be deleted immediately upon expiry of this time period (Art. 52a paragraph 1 Communications Act). Additionally it is stated that retained data shall be of the same quality and subject to the same security and the same protection as the data available in the electronic communications network (Art. 52a paragraph 3 Communications Act). The European Court of Justice, in a judgement of 8 April 2014, declared the Directive 2006/24/EC to be invalid. This judgement has to be analysed. The necessary conclusions will be drawn subsequently.

The application of the provisions concerning data protection and data security in regard to the above mentioned purpose shall be verified by the **Data Protection Agency** (Art. 52b paragraph 1 Communications Act). Pursuant to the same article there are provisions regarding the logging of every enquiry and every participation in a surveillance.

For committing an infraction Art. 70 paragraph 2 Communications Act states that the regulatory authority shall punish with a fine up to 50'000 francs anyone who violates the duty set out in articles 51 to 53 Communications Act.

Q2: What measures have been taken to prevent violations of the right to privacy, including by ensuring that relevant national legislation complies with the obligations of Member States under international human rights law?

Ratification and implementation of human rights treaties

It is the standard practice of the Liechtenstein Government to decide on accession to a treaty only once the relevant legal and practical preconditions have been established domestically. This ensures that all provisions of the treaty may actually be applied from the time of entry into force. Liechtenstein follows a monistic tradition in relation to international agreements, i.e. a ratified agreement becomes part of national law from the date of entry into force, without any need for the creation of a special law. The agreement is also directly applicable if its provisions are sufficiently specific for that purpose.

Protection and enforcement of fundamental rights and freedoms

In Liechtenstein, the Constitutional Court is responsible for the effective protection and enforcement of fundamental rights and freedoms. Natural and legal persons in Liechtenstein have various legal remedies at their disposal to assert their fundamental rights and freedoms.

Anyone who believes that a final decision or decree of a court or public authority has violated one of his or her rights guaranteed under the Constitution or rights guaranteed under an international convention for which an individual right of complaint has been recognized by the legislative power[2] may appeal the decision or decree to the

[2] The Principality of Liechtenstein has recognized the individual right to complaint under the following conventions:

- European Convention of 4 November 1950 for the Protection of Human Rights and Fundamental

Constitutional Court. This also entails that various international conventions for the protection of human rights are considered substantive constitutional law.
Another means of enforcing constitutional laws is the Constitutional Court's review of the constitutionality of laws. This may occur on the application of the Government or municipality or on the application of a court. The Constitutional Court may also carry out a review on its own motion, if proceedings call for the application of a law the Constitutional Court believes to be unconstitutional. If a law or individual provisions thereof are incompatible with the Constitution, the Constitutional Court voids the law or the relevant provision.
Finally, Government ordinances may also be reviewed for compatibility with the Constitution, legislation, and international treaties. Such a review by the Constitutional Court may be demanded by a court, a municipal authority, or at least 100 eligible voters. The Constitutional Court may also review ordinances on its own motion. If the Constitutional Court finds that an ordinance violates the Constitution, a law, or an international treaty, it voids the ordinance in whole or in part.
Finally, the Constitutional Court also has jurisdiction to review the constitutionality of international treaties. The review may be carried out either on application by a court or an administrative authority or on the Constitutional Court's own motion.
Since Liechtenstein is a State Party to the European Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms, the possibility exists in some cases to appeal to the European Court of Human Rights if a violation of rights under the Convention is asserted. Before such an appeal is possible, however, all domestic remedies must be exhausted. The judgments of the European Court of Human Rights are binding.
Under conventions providing an individual right of complaint, affected persons may also submit a complaint to the competent treaty body.

Legitimate violations of the right to privacy
Legitimate violations of the right to privacy are regulated by several different laws (see above). Only in exceptional circumstances and subject to the principle of proportionality the right to privacy may be compromised and personal data may be processed.

The national police and the criminal prosecution authorities may interfere with a person’s right to privacy under the following circumstances:

1. Defence against threat: Based on the Police Act (Art. 25b paragraph 2), the National Police may enter premises that are not open to the public and search such premises as well as real property not open to the public without the consent of the authorized person if necessary to defend against a serious and immediate threat to life, limb, or liberty of a person or to protect objects of substantial value. This is also permissible in the case of suspicion that a person is located there who must be presented or taken into police custody or in the case of suspicion that an object is located there that must be secured in order to defend against an immediate threat. Finally, the National Police may also

---

Freedoms;
- International Covenant of 16 December 1966 on Civil and Political Rights;
- International Convention of 21 December 1965 on the Elimination of All Forms of Racial Discrimination;
- Convention of 18 December 1979 on the Elimination of All Forms of Discrimination against Women;
- Convention of 10 December 1984 against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

interfere with the sanctity of the home in the case of urgent suspicion that persons there are arranging, preparing, or perpetrating crimes. In the cases enumerated above, these intervention measures do not require approval by a court. When searching premises, the owner or – if the owner is absent – an adult member of the owner's family, a housemate, or a neighbour must be involved where the circumstances allow. The owner or the owner's representative must be informed immediately of the grounds for the search, unless this would thwart the purpose of the measure. A log must be kept of the search.

If indispensable in order to prevent a direct and serious threat to life, limb, or liberty of a person (e.g., hostage-taking) or such a threat to substantial material or financial assets (e.g., central electricity, gas supply, or communication facilities), the National Police may also obtain data in or from premises that are not open to the public using the concealed use of technical means to make photographic or video images as well as to tap or record spoken words without consent of the authorized party and without court approval. This measure may be ordered only by the Chief of Police. But in all cases, the confidentiality of letters, post, and communications shall be preserved.

For all measures, the National Police shall comply strictly with the principle of proportionality (see Art. 23 of the Police Act). Affected persons may subsequently submit all measures to the Administrative Court for judicial review.

2. State security: In this domain, the National Police may intervene in non-public space through the concealed use of technical means to make photographic or video images or to tap or record spoken words without consent of the authorized party if the following conditions apply cumulatively: a certain person, organization, or group is suspected of posing a specific threat to the State and its institutions (alleged potential attacker); the gravity and type of the threat justifies such measures; specific and present facts and incidents give rise to the assumption that an alleged potential attacker is using non-public space to meet third parties, or to hide himself or herself or third parties, or to store material there, or in other ways is pursuing activities conducive to his or her purposes; and finally, where intervention affects the fundamental rights of the person concerned, only to the extent necessary (Art. 34b paragraph 3 of the Police Act). Ordering such a measure requires approval by a court in advance (Art. 34a paragraph 4 of the Police Act). The measure may subsequently be submitted for judicial review by way of legal remedies.

3. Criminal Prosecution: Interventions in the sanctity of the home within the framework of criminal proceedings under § 92 of the Code of Criminal Procedure are only permitted if there is an urgent suspicion that persons are located there who are suspected of a crime or misdemeanour or that objects or clues are located there that are important for the criminal investigation. This measure must be ordered in advance by the investigating judge (§ 93 paragraph 3 of the Code of Criminal Procedure). This ruling must be handed over to the person concerned, and that person may have the ruling reviewed by way of legal remedies. In house searches, the court must also involve court witnesses and a recording clerk. The search must in principle be carried out in the presence of the owner of the searched premises. The owner also has the right to involve a person of confidence (see § 95 of the Code of Criminal Procedure).

If the investigating judge cannot be reached and a house search is urgently necessary, or otherwise success of the measure would be threatened, the National Police may, on an

exceptional basis, carry out this measure *ex officio* (see § 94 paragraph 1 of the Code of Criminal Procedure). The procedure outlined above applies *mutatis mutandis*.

Q3: What specific measures have been taken to ensure that procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, are coherent with the obligations of Member States under international human rights law?

Surveillance of communications in Liechtenstein is possible only within the framework of criminal proceedings. Such proceedings are described in §§ 103 et seq. of the Code of Criminal Procedure. According to those provisions, it is possible to order surveillance of electronic communications, including recording of the content, without the owner's consent only if it must be expected that doing so can help solve a wilfully committed offence punishable by more than one year of imprisonment and if the owner of the means of communication is urgently suspected of having committed the offence, or if there are reasons to assume that a person urgently suspected of the offence can be found with the owner of the means of communication or will use the means of communication to contact the owner (§ 103 paragraph 1 of the Code of Criminal Procedure). However, surveillance of the communication of a defence counsel, lawyer, legal agent, auditor, or patent lawyer is not permissible. The order of surveillance must be issued by the investigating judge. The investigating judge must also immediately obtain approval of the measure from the President of the Court of Appeal (§ 103 paragraph 2 of the Code of Criminal Procedure). The surveillance may be approved initially for at most three months, but the order may be extended if the same procedure is followed as for the initial order (§ 103 paragraph 4 of the Code of Criminal Procedure). Upon conclusion of the surveillance, the owner of the means of communication under surveillance must be notified and given access to the recordings (§ 104 paragraph 2 of the Code of Criminal Procedure). The order of surveillance may subsequently be subjected to judicial review by way of legal remedies (§ 104 paragraph 4 of the Code of Criminal Procedure).

The **seizure and opening of letters and other shipments** is only permissible if the accused is already in custody for a wilfully committed offence punishable with more than one year of imprisonment or if presentation or arrest for such an offence has been ordered. The measure must be ordered by the investigating judge. The seizure of shipments must be announced to the accused immediately or within at most 24 hours or, if the accused is absent, to one of the accused's relatives, and the documents must be handed over as soon as the criminal proceedings are no longer at risk (see §§ 99 et seq. of the Code of Criminal Procedure).

With respect to **data processing by the National Police**, the National Police may process data only if necessary to fulfil the responsibilities provided in the Police Act. These legal provisions are in accordance with Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector (Council of Europe). Every person may demand information from the National Police concerning which data is being processed about that person (Article 34g of the Police Act). Additionally, any person may have the National Police correct or even delete any data that may have been processed incorrectly. If the National Police does not grant the application,

it must justify its decision in a formal decree. This decree may be presented for review to the Data Protection Commission and ultimately the Administrative Court (Article 34i of the Police Act).

In the event of **immediate threat to the bodily integrity of a person,** the National Police is authorized to determine the **location of a specific mobile communications network connection** for purposes of deploying emergency, rescue, or security forces. Operators of mobile communications networks are required to immediately help determine such a location. The National Police must immediately notify the owner of the mobile communications network connection of the fact that determination of the location was attempted or successful. All data obtained on the basis of the attempted or successful determination of the location may not be used for other purposes. In the case of wrongful determination of a location, the owner of the mobile communications network connection is entitled to adequate compensation (see Article 51 of the Communications Act).

Q4: What measures have been taken to establish and maintain independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data?

The Data Protection Act of 14 March 2002 implements EU Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data. It seeks to protect the personality and fundamental rights of persons about whom data is processed (Art. 1 paragraph 1 of the Data Protection Act). To supervise the legal provisions of the Data Protection Act, two bodies have been created: the Data Protection Agency and the Data Protection Commission.

The **Data Protection Agency** supervises compliance by authorities with the Data Protection Act and may conduct investigations *ex officio* or at the request of third parties and make recommendations (Art. 29). The Data Protection Agency also plays an advisory role for private persons and authorities (2013: total of 669 enquiries), submits opinions on questions of data protection, supervises compliance with Directive 95/46/EC, and informs the public of current developments in the field of data protection.

With the Law of 17 September 2008 amending the Data Protection Act, the Data Protection Agency was formally attached to Parliament (Art. 28 paragraph 1). It had previously been subordinate to the Government. At the same time, the appointment and dismissal of the Data Protection Commissioner was transferred to Parliament (Art. 28a paragraph 1). Art. 28a paragraph 2 stipulates that “2) The Data Protection Commissioner may not be a member of Parliament, the Government, a court, or an administrative authority, nor may he be the head of a Liechtenstein municipality or sit on a Liechtenstein municipal council. He shall lose such offices upon being appointed Data Protection Commissioner.” Concerning supervision, the Agency does not have the power to issue decisions, but can issue recommendations. If a recommendation is not complied with or is rejected, the Data Protection Agency may refer the matter to the Data Protection Commission for decision (Article 29 and 30 of the Data Protection Act). The Data

Protection Agency also has a right of complaint, on the basis of which it may appeal a recommendation of the Data Protection Commission (see below) (Art. 29 paragraph 5).

Appointment of the staff of the Data Protection Agency is the responsibility of Parliament in consultation with the Data Protection Commissioner (Art. 28b paragraph 1). The latter may, in the Commissioner's function as the head of an administrative agency, make personnel decisions within the scope of powers assigned under the State Employees Act (Art. 28b paragraph 2a); in all other cases, Parliament decides in consultation with the Data Protection Commissioner (Art. 28b paragraph 2b).

The Data Protection Agency is also financially independent. The budget of the Data Protection Agency is drafted by the Data Protection Agency itself and, after preliminary consideration by the Audit Commission of Parliament, submitted to the Government. The Government forwards the budget to Parliament for consideration and approval (Art. 28c paragraph 1).

The **Data Protection Commission** decides on recommendations of the Data Protection Agency, appeals against decrees by authorities relating to data protection matters, and appeals against decisions of the Data Protection Agency (Art. 34). It consists of three members and two alternate members, each appointed by Parliament for a term of four years (Art. 33 paragraph 1).

Q5: Any other information on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data

We refer to the common response of Austria, Liechtenstein, Slovenia and Switzerland under question/issue no. 5, which has been submitted to the OHCHR on 10 April 2014 as a separate document:

Common response of Austria, Liechtenstein, Slovenia and Switzerland to the OHCHR request regarding „The right to privacy in the digital age" (dated 26 February 2014)

Issue 5: "Any other information on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data"

The mandate given by General Assembly resolution 68/167 to the UN High Commissioner for Human Rights to submit a report on the right to privacy in the digital age provides an important and timely opportunity to submit legal and policy considerations that will help the international community to make much-needed progress. **In this context, Austria, Liechtenstein, Slovenia and Switzerland would like to jointly highlight the following aspects**:

During the last years, international media outlets have reported extensively about far-reaching practices involving domestic and extraterritorial surveillance, interception of

digital communications and the collection of personal data, including on a mass scale and without any showing of need or probable cause. These revelations have raised serious concerns among governments, civil society, the private sector and the public at large regarding the legal and policy implications of these practices. The concerns expressed relate primarily to the right to privacy, though other fundamental rights (such as the right to freedom of expression and the right to non-discrimination) are also at stake, as are other norms of international law. Austria, Liechtenstein, Slovenia and Switzerland therefore fully support UN General Assembly Resolution 68/167, which calls upon States to "respect and protect the right to privacy, including in the context of digital communication" and suggest a number of concrete measures for this purpose.

Respecting and protecting the right to privacy in the digital age is a formidable long-term challenge. In this context, the upcoming report by the UN High Commissioner for Human Rights can provide crucial views and recommendations. Such guidance is particularly necessary as there is currently very limited material to draw from at the inter-governmental level, and jurisprudence on the core issues at hand is either not existent or not publicly available, not least due to the secret nature of relevant activities. Going forward, an open discussion on the concrete legal and policy parameters of the right to privacy in the digital age will be necessary and has indeed started, as evidenced by the expert seminar held in Geneva on 24-25 February 2014.

(1) Understanding the right to privacy

GA Resolution 68/167 refers to the right to privacy as the right "according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights". The right to privacy clearly applies to activities both in the physical environment as well as in the digital sphere. Interferences with the right to privacy or the sanctity of correspondence are only lawful to the extent that they are provided by law, justified in the public interest or for the protection of the fundamental rights of others and proportionate. It is immaterial for this proportionality test whether or not a person subject to surveillance, interception or data collection may be aware of the existence of such measures. Some States, however, tend to apply a very narrow interpretation of the scope of the right to privacy, and/or an overly broad interpretation of legitimate limitations. The High Commissioner's report should therefore pay great attention to these important aspects and should focus on what forms of interference are "arbitrary".

(2) Extraterritorial surveillance, interception and data collection

GA Resolution 68/167 specifically refers to the extraterritorial dimension of interferences with the right to privacy. The nature of modern communication technology is such that even seemingly local communications – their content as well as related metadata – can be accessed from elsewhere in the world. In today's digital age, the right to privacy is, broadly speaking, under greater threat from abroad than from within a State. This is *inter alia* due

to the fact that States typically apply more stringent restrictions to domestic surveillance, interception and data collection, and that States generally simply collect more data abroad, especially in a national security context. This raises the crucial question of whether and to what extent States are obliged by article 17 ICCPR to respect and protect the right to privacy in the context of extraterritorial surveillance, interception and data collection. During the negotiations leading to the adoption of GA Resolution 68/167, States informally advanced different views in this regard. Austria, Liechtenstein, Slovenia and Switzerland therefore hope that the High Commissioner's report will provide guidance on this crucial question. Such guidance should take into account the following:

- The Human Rights Committee has already recognized that there are situations in which the obligations under the ICCPR apply extraterritorially. General Comment No. 31 on the nature of the general legal obligation imposed on States Parties to the Covenant stated that States Parties "must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. […] This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained."
- This principle also applies, *mutatis mutandis*, to the actions of a State Party whereby it interferes extraterritorially with the right to privacy of a person. In such situations, the protected value associated with that person, namely his or her privacy, is indeed under the effective control of that State. While the General Comment No. 31 was clearly formulated against the background of past cases involving various degrees of physical control by a State Party over a person outside its territory, the underlying logic of the principle stated therein makes it applicable to situations of <u>partial</u> control, i.e. control over certain aspects of a person's human rights.
- In other words, the extraterritoriality of States Parties' human rights obligations is not categorical. A State Party is subject to some human rights obligations even in situations in which it does not exercise full physical control over an individual and the entire corpus of human rights. If it exercises effective control over the ability of the individual to enjoy that right, then the obligation applies extraterritorially.

(3) The role of the Human Rights Committee

As outlined above, the right to privacy in the digital era raises important issues regarding the interpretation of the ICCPR. Austria, Liechtenstein, Slovenia and Switzerland would therefore support any efforts by the Human Rights Committee to pronounce itself on related matters, in particular by updating its relevant General Comments (GC), primarily GC no. 16, further also GC no. 31. Most importantly, the Human Rights Committee should work to translate the concepts and principles of effective control in the physical world into a standard of virtual control over the right to privacy and its related rights in the digital world.

(4) The role of Special Procedure mandate holders

Austria, Liechtenstein, Slovenia and Switzerland are convinced that those Special Rapporteurs whose mandates are concerned with the right to privacy and the issue of national security practices (such as the UN Special Rapporteurs on the right to freedom of opinion and expression, and on human rights and fundamental freedoms while countering terrorism) should be encouraged to come together for a joint initiative and issue for example guidelines clarifying the legal regimes, and develop best practices on ensuring respect for the right to privacy in the digital age. In full support of Human Rights Council (HRC) Decision A/HRC/25/L.12 convening a panel discussion on the promotion and protection of the rights to privacy in the digital age 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 at the 27th Session of the HRC, the contributions of Special Rapporteurs will be very important to inform and further this important debate.

Vaduz, 11 April 2014