Questionnaire of the *Office of the High Commissioner for Human Rights (OHCHR)*
of 26 February 2013
Re.: *General Assembly Resolution 68/167, "The right to privacy in the digital age"*

Reply by the Federal Republic of Germany

Question 1:
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 informational self-determination, protected by the constitution of the Federal Republic, the Basic Law (*Grundgesetz*), guarantees individuals the power to themselves decide whether or not they wish to disclose personal data and how such data are to be used (cf. Rulings of the Federal Constitutional Court (*Entscheidungen des Bundesverfassungsgerichts*), BVerfGE, 117, p. 202, citation on p. 228). This is one of the essential forms in which the principle of human dignity (Article 1 para. 1 of the Basic Law) and the general freedom of action (Article 2 para. 1 of the Basic Law) have taken shape.

The sphere of protection afforded by Article 2 para. 1 of the Basic Law, in conjunction with Article 1 para. 1 of the Basic Law, comprises all data containing individual information on the personal or factual circumstances of a specific or identifiable person. According to the adjudication handed down by the Federal Constitutional Court, there is no such thing as irrelevant data since the technical possibilities of linking data allow conclusions to be drawn, based on any information (including data that, in and of themselves, have no importance), concerning the data subject, his or her path in life and personality (cf. Rulings of the Federal Constitutional Court, BVerfGE 65, p. 1, citation on p. 45). Both the transmission and the collection of such data, and likewise their storage, represent an intrusion into the right of informational self-determination. Under constitutional law, such intrusions are justified only in those cases in which they occur based on a law that defines the purpose for which such data are to be used in a precise manner, while also determining the specific procedural context of such purpose. The data collected and stored must be suited and required for this purpose. In this context, the use of the data must absolutely be limited to the purpose defined by law. Concurrently, the law must also provide for obligations to provide elucidation and information, as well as the duty to delete data (cf. Rulings of the Federal Constitutional Court (BVerfGE) 65, p. 1, citation on p. 46). By contrast, what is strictly prohibited is the retention of personal

data for undetermined purposes or purposes that cannot yet be determined (cf. Rulings of the Federal Constitutional Court (BVerfGE) 130, p. 151, citation on p. 187).

Furthermore, Article 2 para. 1 of the Basic Law also protects the confidentiality and integrity of the data of information technology systems (cf. Rulings of the Federal Constitutional Court (BVerfGE) 120, p. 274, citation on p. 314). Secretly accessing technical information systems, and in particular computers, for preventive reasons is possible only in those cases in which there actually are indications of a specific danger to a legal interest of exceptionally high importance (cf. Rulings of the Federal Constitutional Court (BVerfGE) 120, p. 274, citation on p. 328).

Pursuant to Article 10 para. 1 of the Basic Law, the privacy of telecommunications likewise enjoys constitutional protection.
Said Article guarantees the privacy of digital communications, which protects the non-physical transfer of information to individual recipients using telecommunications means against public authorities becoming aware of such information (cf. Rulings of the Federal Constitutional Court (BVerfGE) 130, p. 151, citation on p. 179, with further references). The intention is to ensure that the persons involved do not refrain from exchanging their opinions or information using telecommunications facilities, or do so only in a different form or with modified content, because they must count on governmental authorities becoming involved in such communications and obtaining knowledge about their communications relationships and the content they communicate. According to the consistent case law of the Federal Constitutional Court, this provision covers more than just the content of the communications. Rather, it also governs the privacy of the more exact circumstances of the communications process, which particularly include whether, when, and how often which persons or telecommunications facilities entered into telecommunications, or attempted to do so (cf. Rulings of the Federal Constitutional Court, BVerfGE 130, p. 151, citation on p. 179 with further references).

Since the right to informational self-determination, the integrity of the data of information technology systems, and the privacy of telecommunications are protected by the Constitution, the state is obligated, furthermore, to make provisions wherever necessary that protect the individual against any impairments of these rights by third parties.

According to section 88 (2), first sentence, of the Telecommunications Act (*Telekommunikationsgesetz*, TKG), it is not only governmental authorities who are obligated to comply with this law; rather, private providers of telecommunications services have the

same obligation. The privacy of telecommunications covers the content of telecommunications and their detailed circumstances, in particular the fact of whether or not a person is or was engaged in a telecommunications activity (cf. section 88 (1), first sentence, of the Telecommunications Act). Pursuant to section 88 (3), first sentence, of the Telecommunications Act, service providers are basically prohibited from procuring, for themselves or for other parties, any information regarding the content or detailed circumstances of telecommunications beyond that which is necessary for the commercial provision of their telecommunications services, including the protection of their technical systems (as regards permissible intrusions into the privacy of telecommunications, cf. the answer to Question 4).

At the level of ordinary, non-constitutional legislation, the right to determine the use of one's personal data is ensured by data protection regulations integrated in specialist statutes or, where these do not exist, by the Federal Data Protection Act or the applicable state (Länder) data protection act. The Federal Data Protection Act is intended to protect individuals against privacy violations resulting from the use of their personal data.

In Germany, the protection of digital privacy is also ensured by the stipulations of the Criminal Code (*Strafgesetzbuch*, StGB). The following are liable to punishment under criminal law: data espionage (section 202a of the Criminal code), phishing (section 202b of the Criminal Code) as well as acts preparatory to data espionage and phishing (section 202c [of the Criminal Code]); moreover, data tampering (section 303a of the Criminal Code) and computer sabotage (section 303b of the Criminal Code) are likewise liable to punishment under criminal law.

Furthermore, the provisions of civil law allow for claims to compensation of damages to be filed, and to demand that an action be ceased and desisted from. The inviolability of human dignity guaranteed by Article 1 para. 1 of the Basic Law and the right to free development of an individual’s personality warranted by Article 2 para. 1 of the Basic Law has served as the basis for case law to derive the general right of personality (*Allgemeines Persönlichkeitsrecht*) and has qualified it, in the context of section 823 (1) of the Civil Code (*Bürgerliches Gesetzbuch*, BGB), as another right. Said general right of personality is to be understood as a uniform, comprehensive subjective right to respect and the free development of an individual’s personality, which protects the social and private sphere as well as the privacy of every individual. It is an omnibus definition that will give precedence to any more specific law conclusively providing for the rights given in the event of violations of the general personal right. The general personal right has a very broad scope of protection

and has been given a relatively indeterminate definition. Where the elements of a norm are left undefined to the extent given here, the unlawful nature of an act must always be established as a positive determination; in other words, only an unlawful impairment of the general personal right will be deemed a legally relevant violation. In determining unlawfulness in this way, the objects of legal protection and the interests must be comprehensively balanced out. In addition to a fault-based claim to compensation of damages pursuant to section 823 (1) of the Civil Code, a violation of the general personal right will grant an entitlement to defend against claims in analogy to the stipulations of section 1004 of the Civil Code, which is targeted at the acts of infringement being ceased and desisted from and is not based on any fault. With a view to the aspect of "surveillance of communications," it should be emphasised that the unauthorised opening of mail is to be deemed a violation of privacy. The same criterion is to be applied to digital mail.

In negotiations at EU level about a General Data Protection Regulation, Germany actively supports the adoption of pan-European data protection rules which are enforceable throughout Europe. These rules should meet the challenges of the digital age and must not fall short of the high data protection standard in Germany.

Secure IT systems in German infrastructure, the use of reliable and trustworthy information technology, and improving IT security in public administration are among the priorities of the German cyber security strategy and at the same time essential for ensuring the right to privacy.

Question 2:
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?

Measures to prevent violations: See above – answer to question 1.

Ensuring compliance of national legislation: On the federal level there are four institutions that are responsible for examining draft legislation for the conformity with international law including human rights:

- the Ministry with overall responsibility for the particular draft – before that Ministry submits it to the other Ministries for approval,

- the Federal Ministry of Justice and Consumer Protection, to which every draft bill has to be submitted – before adoption by the federal cabinet – so that it can be checked, in the so-called "scrutiny procedure", to see whether it fulfils all legal requirements, including compliance with human rights, for eventual entry into force,
- the Legal Affairs Committee of the Federal Parliament (Bundestag) and
- the Legal Affairs Committee of the Federal Council (Bundesrat).

In the case of draft ordinances there will be an examination for conformity with all legal requirements including human rights obligations by the Ministry with overall responsibility for the draft as well as by the Federal Ministry of Justice and Consumer Protection in the scrutiny procedure.

The *Länder* have corresponding control mechanisms.

The independent data protection supervisory authorities of the federation and of the *Länder* control the implementation of the data protection laws.

Question 3:
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?

In promulgating legislation regarding the surveillance of telecommunications, it is painstakingly ensured from the outset that the provisions to be adopted will conform to the national and international obligations existing in the sphere of basic rights and human rights that take prior rank (see the answer to Question 2).

In an individual case, the data subjects have means of obtaining legal protection in order to review the measures taken against them (on this, see also the answers provided to Questions 1 and 4). In Article 19 para. 4, the Basic Law guarantees the right to legal protection. This warrants effective protection by the courts against violations of an individual's legal sphere by intrusions caused by the German public authority implementing such measures. In cases involving the surveillance of telecommunications under the laws governing criminal procedure, rules concerning the notification of data subjects ensure that these can effectively safeguard their rights (see the answer to Question 4 below).

Under certain circumstances, data subjects may lodge a constitutional complaint with the Federal Constitutional Court in the event of an alleged violation of their basic right to informational self-determination by a public authority. However, inasmuch as decisions taken by authorities and courts are being challenged, all remedies must first have been fully exhausted. Accordingly, a constitutional complaint (as a general rule) will be admissible only once a ruling has been handed down by the court of last instance. An exception from this principle of legal remedies needing to be exhausted applies to constitutional complaints lodged directly against a law, as no regular legal remedies are available in this case.

Question 4:

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

As far as the activities of the intelligence services (BfV, BND, MAD) are concerned, the Federal Government is subject to the supervision of the Parliamentary Control Panel in accordance with the Parliamentary Control Panel Act (PKGrG). At the beginning of each electoral term, the panel members are elected from among the members of the German Bundestag. The panel has numerous supervisory powers which are laid down by law. For example, it can request the Federal Government or the intelligence services to provide records or documents which are in official custody. The Parliamentary Control Panel can also request access to stored data and to the premises where the data are stored. It may also interview staff members of the intelligence services and members of the Federal Government or make written inquiries. Generally, the Federal Government is obligated to provide the Parliamentary Control Panel with comprehensive information about the general activities of the intelligence services and on incidents of special significance. The Federal Government may withhold information or reject to provide documents only in very exceptional cases evidently requiring secrecy.

The offices for the protection of the constitution at federal and state level, the Federal Intelligence Service (BND) and the Military Counterintelligence Service (MAD) are authorized to carry out measures restricting the privacy of letters, posts and telecommunication (Art. 10 of the Basic Law). Details are laid down in a specialist act known as the G10 Act. Such restrictive measures are subject to monitoring by a special commission, the G10 Commission of the German Bundestag. The members of the Commission serve in an official honorary

position and are appointed by the German Bundestag for one legislative period. The Commission's statutory mandate is to decide ex-officio or on the basis of complaints whether restrictive measures are permissible and necessary. Within the Federal Government, the Federal Ministry of the Interior is responsible for ordering restrictive measures which are then subject to monitoring by the Commission. The Federal Ministry of the Interior submits the relevant cases to the Commission and informs the Commission about restrictive measures ordered by the ministry and their enforcement. If a federal state makes an application for restrictive measures, it is up to the competent superior state authority to instruct the relevant agencies to take such measures. Restrictive measures pursuant to the G10 Act are ordered only upon application. Only the Federal Office for the Protection of the Constitution (BfV), the Federal Intelligence Service (BND) and the Military Counterintelligence Service (MAD) are eligible to apply for restrictive measures.

In a decision of June 2006 (54934/00), the European Court of Human Rights decided that the G10 Act provides adequate and effective guarantees against misuse of surveillance measures. According to that decision, taking into consideration the fairly wide margin of appreciation of the contracting state, the interferences with the secrecy of telecommunications can be considered as necessary in a democratic society in the interests of national security and for the prevention of crime.

As regards the laws governing criminal procedure, the surveillance of telecommunications is subject to controls both by the courts and by public authorities. Any measure serving the surveillance of a suspect’s telecommunications will be possible only within the narrow limits imposed by sections 100a and 100b of the Code of Criminal Procedure (*Strafprozessordnung*, StPO). Only if certain circumstances give rise to the suspicion that one of the serious criminal offences individually listed in section 100a (2) of the Code of Criminal Procedure has been committed, and the offence is one of particular gravity in the individual case as well, the court may order, upon a corresponding petition by the public prosecutor’s office, that surveillance measures be pursued. Only in exigent circumstances may the public prosecution office also issue an order for such measures; however, this will require a confirmation to be issued by a judge within three (3) days. A measure that is expected to provide no more than information concerning the core area of the private conduct of life is impermissible. The order concerning the surveillance of telecommunications pursuant to sections 100a and 100b of the Code of Criminal Procedure shall be limited to a maximum duration of three (3) months. Extensions by no more than three (3) months in each case are possible. Pursuant to section 101 (4) no. 3 of the Code of Criminal Procedure, the persons affected by the surveillance of their telecommunications are to be notified thereafter, unless this is contravened by overriding interests worthy of protection that a data subject

enjoys. The notification shall take place as soon as it can be effected without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another, or any significant assets. Pursuant to section 101 (7) of the Code of Criminal Procedure, a person affected by the surveillance measures may have a court review their lawfulness, as well as the manner and means of their implementation. Additionally, the *Länder* and the Federal Public Prosecutor General are obligated by section 100b (5) of the Code of Criminal Procedure to report to the Federal Office of Justice (*Bundesamt für Justiz*) every year on the measures ordered within their area of competence. The Federal Office of Justice produces a summary of these reports for publication on the Internet.

Similar provisions apply to the collection of telecommunications traffic data. Pursuant to section 100g of the Code of Criminal Procedure, such data may be collected only in the event of criminal offences that are of substantial significance also in the individual case, or in the event of criminal offences committed by means of telecommunication; in each case, their collection requires an order to have been issued by a judge. Pursuant to section 100g (4) and section 100b (5) of the Code of Criminal Procedure, reports are to be prepared and published annually also on the measures taken in this regard.

Any enquiry may be made for customer inventory data stored by telecommunications companies (name, address, telephone number et cetera) pursuant to section 100j of the Code of Criminal Procedure in the case of a criminal offence for purposes of establishing the facts or determining an accused's whereabouts. Inasmuch as these are data that serve to protect against access to terminal devices or storage facilities (such as PINs and PUKs), section 100j (3) stipulates that this will require an order from the court as a matter of principle.

In addition to the authority granted under the laws governing criminal procedure for the surveillance of telecommunications, the Police Acts of the federation and of the *Länder* authorise the police forces to perform such surveillance for purposes of preventing threats. The procedures serving to order, control, and provide notification of such surveillance of telecommunications measures are similar to those stipulated by the laws governing criminal procedure. Inasmuch, reference is made to the above remarks.

Additionally, we refer to the answers given to Questions 1 and 2.

Question 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.

For numerous years, the Federal Ministry of Justice and Consumer Protection has been promoting projects serving to inform consumers on measures serving the protection of their privacy on the internet and in the digital world, particularly on topics such as surfing safely and protecting personal data in social networks. These campaigns, targeted at informing and educating the public, are intended to increase awareness among consumers for the protection of their privacy and to enhance their media competence. The intention is to give consumers the wherewithal to themselves take measures serving to protect their privacy and to decide, consciously and at their own discretion, which information and data they wish to disclose.

Additionally, the Federal Government promotes innovative projects that have made it their objective to develop special technologies, tools, and programmes serving to protect privacy in the digital world.

The Federal Ministry for Family Affairs, Senior Citizen, Women and Youth particularly focusses on the protection and promotion of the right to privacy for children and young people. On behalf of the ministry, the Online Child Protection Centre has been launched, inviting industry, politics and youth protection in order to develop an intelligent risk management that particularly addresses the issue of personal data.

Furthermore, awareness and empowerment actions are regarded as important as a safe online environment for children beginning to use the internet. Awareness and empowerment actions enable children to develop strategies in order to protect personal data and to cope in case of data abuse. As children start using the internet at very young ages, it is necessary for online safety education to start in early childhood, supported by family and school. Therefore, awareness and empowerment actions address not only children but parents, carers and teachers. The Federal Ministry for Family Affairs, Senior Citizen, Women and Youth has launched several initiatives for parental information, such as online information on media education in general frequently covering issues of data protection (www.schau-hin.info) and online information specifically on children's internet use (www.surfen-ohne-risiko.net). In September 2013, material on data protection has been issued particularly to be used at schools. In addition to information, the Federal Ministry for Family Affairs, Senior Citizen, Women and Youth has launched initiatives to stimulate the production and visibility of quality

content for children, such as a child friendly browsers, search engines and – in cooperation with the Federal Government Commissioner for Culture and Media – the initiative “Ein Netz für Kinder” to stimulate innovation in quality online content for children. It should be noted that the German Bundesländer hold a major share in media education. Germany actively contributes to the EU safer internet programme.

Studying new approaches to privacy protection is an important priority for the German Federal Ministry of Education and Research (BMBF). Since 2011, the BMBF has been supporting three centres of excellence in the field of IT security research, which are strongly engaged in exploring new solutions for privacy protection:

- CISPA (Center for IT-Security, Privacy and Accountability) in Saarbrücken
- EC SPRIDE (European Center for Security and Privacy by Design) in Darmstadt
- KASTEL (Center of Excellence for Applied Security Technology) in Karlsruhe

The centres pool the expertise of leading universities and non-university research institutions in order to address and solve key issues of privacy protection in the digital world. The main focus is on technological solutions which ensure that privacy requirements are taken into account in the design of new products wherever possible.

In addition to the technological research of these centres, the BMBF is also supporting the interdisciplinary study of major, socially relevant issues of privacy protection. The aim of the funding activity is to develop sustainable proposals in an interdisciplinary dialogue, describing how informational self-determination can be guaranteed and implemented in future.

In the field of vocational education and training (VET), the Federal Ministry of Education and Research (BMBF) is funding a project on data protection learning under its "Digital Media in Vocational Training" funding programme. The aim is to make employees of companies aware of issues in the fields of basic data protection, social media and communication, customer data, staff data and health data. Moreover, the BMBF is supporting various projects addressing different aspects of privacy protection on the Web under its funding call in the field of media education in VET.

From the perspective of the Federal Government, the right to privacy in digital communications must be observed also in connection with measures serving to enforce intellectual property rights. In this regard, the interests need to be balanced out against those of the right holders.

Accordingly, German law provides for the reservation of a court order where a right holder demands information from an enterprise that can only be provided using telecommunications traffic data. To cite some examples, telecommunications traffic data include the time, duration, and recipient of a call, or the IP addresses used by the participants of internet communications.

In actual practice, a frequent occurrence will be that a copyright holder will wish to obtain information from an internet access provider about the subscriber to whom a certain IP address was assigned at a certain point in time. In this case, the copyright holder will have to file a petition with the court for an order stating that providing the information using the traffic datum “IP address” is permissible. The court will review, *inter alia*, whether the pre-requisites for such information (obvious violation of copyright) have been met. In this way, the traffic data that are sensitive with a view to the privacy of the subscriber – who will often be a private individual – are granted special protection. In parallel, it is ensured that the right holder receives the information necessary for effectively safeguarding his or her rights, provided that the statutory pre-requisites therefor have been met.

The procedure described applies with a view to all intellectual property rights and has been provided for in the laws governing the respective rights (such as the Trade Mark Act, Copyright Act, Patents Act). As an example, we refer to section 101 (9) of the Copyright Act (*Urheberrechtsgesetz*, UrhG). An English translation of this law is available at http://www.gesetze-im-internet.de/englisch_urhg/index.html .

From the perspective of the Federal Government, the right to privacy must also be observed if right holders and internet service providers collaborate on a voluntary basis in order to combat the violation of intellectual property rights. Such agreements must fully comply with the framework of applicable law and must observe data protection rules. Where internet service providers enter into obligation to intercept data traffic, or to store and transfer data in a manner extending beyond legal requirements, this will impair the privacy of their users – be they private individuals or corporations. Accordingly, such measures would not be acceptable.