International Working Group
on Data Protection
in Telecommunications

675.47.12 3 September 2013

Working Paper
on
the Human Right to Telecommunications Secrecy

54th meeting 2 – 3 September 2013, Berlin (Germany)

In view of recent reports on the activities by intelligence services the Working Group recalls that it has on several occasions stressed the importance of telecommunications secrecy as a human right[1]. Most telecommunications today is taking place across borders therefore the distinction between national and international telecommunications has become obsolete.Telecommunications and in particular the Internet are essential technologies for individuals and societies in the 21st century. Both depend on the legitimate expectation of users that communications *in principle* are free from surveillance and interception. This applies to contents as well as metadata and other digital traces. If this confidentiality by default is threatened the very fabric of free societies is at risk. Interception of communications by government agencies in general[2] and intelligence services in particular can be necessary for legitimate reasons but it must be the *exception*, not the rule. To comply with principles of openness, transparency and accountability, there should be mechanisms to re-assure the public that interception powers are being used lawfully, appropriately and proportionally.

[1] Common Statement on Cryptography (12.09.1997) – http://www.datenschutz-berlin.de/attachments/172/crypt_en.pdf ; Common Position on Public Accountability in relation to Interception of Private Communications, 23rd meeting, 15 April 1998, Hong Kong – http://www.datenschutz-berlin.de/attachments/904/inter_en.pdf; Ten Commandments to protect Privacy in the Internet World – Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements, 28th meeting, 14 September 2000, Berlin – http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf ; Working Paper on Telecommunications Surveillance, 31st meeting, 27 March 2002, Auckland – http://www.datenschutz-berlin.de/attachments/912/wptel_en.pdf; The Granada Charter of Privacy in a Digital World, 47th meeting, 15./16 April 2010, Granada – http://www.datenschutz-berlin.de/attachments/794/675.40.11_Endfassung.pdf. The European Court of Human Rights in its jurisprudence has interpreted Art. 8 of the European Human Rights Convention along similar lines, see Case of Weber and Saravia v. Germany, Decision of 29 June 2006, with further references.

[2] For the diverse legal situation globally cf. International Data Privacy Law, Vol. 2 No.4 (2012), Special issue on Systematic Government Access to Private Sector Data.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media

The Working Group therefore urges governments:

1. To recognize telecommunications secrecy as an essential part of the globally acknowledged human right to privacy;[3]

2. To strengthen telecommunications secrecy as a human right in an international convention. Restrictions should be limited to what is strictly necessary in a democratic society;

3. To agree on international rules limiting government access to data stored by Internet service providers and signals intelligence on the Internet;

4. To provide for greater transparency and public accountability of government agencies as to the results of lawful interceptions[4]; this includes transparent rules on classification and de-classification[5];

5. To ensure that every data subject regardless of nationality has the right to be notified *ex post*, to have his data deleted and corrected and of access to justice;

6. To allow and encourage citizens to freely research, create, distribute and use tools for secure communications; no citizen should be monitored simply on the ground that he or she is using such tools;

7. To ensure effective and independent oversight with regard to surveillance activities carried out by police and intelligence agencies or on their behalf by private processors[6].

[3] The right to private correspondence is specifically mentioned in Article 12 of the UN Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 8 of the European Convention on Human Rights (ECHR).
[4] The European Court of Human Rights in the case of Youth Initiative for Human Rights v. Serbia, Judgment of 25 June 2013 has clarified that intelligence agencies are within the scope of freedom of information legislation.
[5] See Principles 11-17 of the Tshwane Global Principles on National Security and the Right to Information of 12 June 2013.
[6] See Principle 6 of the Tshwane Global Principles.