Opinion of the European Data Protection Supervisor

on the Commission Communication on Internet Policy and Governance - Europe`s role in shaping the future of Internet Governance

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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,[1]

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 41 thereof,[2]

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. Consultation of the EDPS

1. On 12 February 2014 the European Commission published a Communication on Internet Policy and Governance ("the Communication").[3] The Communication was adopted in the aftermath of revelations about a large-scale surveillance scheme implemented by the US National Security Agency on (and through) the Internet, which affected trust in the Internet and its current governance model and called for immediate reform.

2. We regret that we were not consulted before the publication of the Communication. Nonetheless, as Internet Governance and the rights to privacy and data protection are closely related, we have decided to issue this Opinion on our own initiative, pursuant to Article 41(2) of Regulation 45/2001.

I.2. Content of the Communication

3. The Communication proposes a basis for a common European vision for Internet Governance. In particular, among other things, it purports to:

[1] OJ L281, 23.11.1995, p. 31.
[2] OJ L8, 12.1.2001, p. 1.
[3] COM(2014) 72 final.

- defend and promote fundamental rights and democratic values as well as multistakeholder governance structures based on clear rules and on the respect for those rights and values;

- promote a single, unfragmented network, subject to the same norms and laws that apply in other areas of our lives, where individuals may benefit from rights and judicial remedies, in case their rights are breached.[4]

4. In order to do so, the Communication focuses on the main policy areas relevant to the complex Internet Governance ecosystem, namely the development of Internet Governance principles, cooperative frameworks and core Internet functions. It also makes concrete proposals on how to strengthen the current multistakeholder model. Last, it looks ahead to some of the key issues that must be addressed in the context of Internet Governance in the future, namely the strong interplay between technical norms and Internet policy, the key challenges in rebuilding trust, and conflicts of jurisdictions and laws.

5. The underlying principles of the reform should - in the Commission´s view - consist of an increased transparency, accountability and inclusiveness of the way the Internet is managed.

6. At the core of the reform, the Commission places fundamental freedoms and human rights that "*are not negotiable*" and "*must be protected online*".[5]

I.3. Aim of the Opinion

7. Since the publication of the Communication, the discussion on the development of Internet Governance has carried on, notably at the ICANN meeting in Singapore in March 2014 and at the Global Multistakeholder Meeting on the Future of Internet Governance (NetMundial) in Brazil in April 2014. The discussion will continue at the ICANN meeting in London in June 2014.

8. With this opinion, we wish to contribute to the debate, as any reform of Internet Governance will likely have a significant impact on citizens and on their fundamental rights, not least the rights to privacy and data protection. While this Opinion addresses an issue of global nature and while it takes account of the developments at global level, it focuses on the actions that the European Union and its institutions can perform to influence the debate and the Internet Governance structures and processes themselves.

9. This Opinion consists of three sections. Section II draws upon the tight relationship existing between Internet Governance, on the one hand, and privacy and data protection on the other. Section III explores how the current system of EU law may help shaping the Internet, focusing on measures and rules ensuring that individual rights to privacy and data protection are properly fulfilled. Section IV touches upon further action which appears both desirable and necessary in order to achieve a satisfactory shaping of Internet Governance and aims at providing a timely response to the issues that the Internet poses on a daily basis.

[4] See Communication, p. 2.
[5] Commission Vice-President Neelie KROES, press release IP/14/142 of 12.02.2014.

II. PRIVACY AND DATA PROTECTION ARE STRONGLY RELATED TO GOOD INTERNET GOVERNANCE

II.1. The protection of privacy and data protection as internationally recognized fundamental values

10. The Communication clearly underlines the need to base the future development of Internet Governance on the respect of fundamental rights. We welcome this principle, but we stress the need to translate it into practical policy initiatives, which is not always sufficiently the case.

11. Privacy and data protection are recognized in several international instruments - such as Article 12 of the Universal Declaration of Human Rights[6], Article 17 of the International Covenant on Civil and Political Rights[7], the OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data[8] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[9]. These instruments provide a firm foundation for citizens' involvement in online interaction.

12. We emphasise that, in order to "*sustain and develop the Internet as an essential part of life*"[10] and to create a "*single, open, free, unfragmented network of networks*" with a "*safe, secure, sound and resilient architecture*"[11], Internet Governance should be built starting from commonly shared international rights and values. Consequently, privacy and data protection principles need to gain more weight within Internet Governance fora and mechanisms.

13. We note some positive developments at international level in recognising privacy and data protection as essential values for the internet. At the Net Mundial, a general consensus was reached on the need to protect privacy on the Internet, by pointing out that "*The right to privacy must be protected. This includes not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data. The right to the protection of the law against such interference should be ensured*".[12]

14. We therefore urge that privacy and data protection should be core elements of any Internet Governance model, and recommend that the European Union put its full weight behind initiatives ensuring that such integration process is undertaken at a global level.

II.2. Data protection as a cornerstone for shaping Internet Governance

15. The Communication emphasizes that the Internet has become a key infrastructure with global dimensions and that, as a consequence, greater international balance within the existing structures would increase the probability of issuing legitimate outcomes.[13]

---

[6] UN Universal Declaration of Human Rights. Available at http://www.un.org/en/documents/udhr/index.shtml#a12.
[7] UNHCR International Covenant on Civil and Political Rights. Available at http://www2.ohchr.org/english/law/ccpr.htm#art17.
[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Revised (2013) version available at http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines.
[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe's Convention 108). Available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[10] See the Communication, p. 1.
[11] See the Communication, p. 10.
[12] The final statement adopted at the end of the summit is available at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.
[13] See the Communication, p. 5.

16. When discussing Internet Governance, it should be kept in mind that the governance of the Internet's infrastructure and global resources such as names and addresses is not the only source for privacy risks, but that the services provided on the Internet often create even greater risks for the privacy of their users and of third parties. In order to develop a comprehensive policy for the protection of privacy on the Internet, the Union must not only look at the global processes, but also at other relevant rules and mechanisms. An example of a data protection issue which has to be addressed by the Internet governance bodies is the current WHOIS system with the authentication and data retention requirements.[14] On the other hand, examples of activities performed on the Internet with significant data protection implications include eCommerce, eGovernment, eHealth, eMoney, ePayments. We would like to emphasise that, in each of the above cases, privacy and data protection principles must be at the core of policy considerations at global level, so as to ensure protection for every Internet user.

17. In this context, it should be recalled that ICANN (*Internet Corporation for Assigned Names and Numbers*) remains a national organization essentially regulated by domestic –Californian– private law. This makes it difficult to ensure proper fulfilment of data protection rights of non-US internet users. In this respect, the European Parliament has indicated the need to end the control over Internet governance bodies by a single country.[15] Since 2009, ICANN has taken steps in this direction, but its own status, based on a contractual relationship within a single country, has not changed.

18. Other stakeholders have also addressed the pressing need for globalisation of Internet Governance bodies and rules and for ensuring the respect of the right to privacy online as well as compliance with the data protection laws enacted in numerous jurisdictions. In response, the NTIA (US National Telecommunications and Information Administration)[16] announced on 14 March 2014 the intention to transfer the role it currently plays in the implementation of the policies of IANA (Internet Assigned Numbers Authority, a department of ICANN) to the global multistakeholder community by September 2015, by asking ICANN to provide a proposal for a multistakeholder body to take this role. Consequently, in its role as a facilitator, during the Singapore public meeting, ICANN initiated the discussion regarding the process for performing such transition. At the same time, ICANN has recently identified privacy and data protection as a new key area for its institutional activities.[17] Moreover, in April 2014, the Net Mundial provided additional opportunities to address the globalisation of ICANN and the IANA functions.

19. As the Communication rightly states, it has become crucial that Internet Governance be based on a shared and truly global model which would better ensure the fulfilment of privacy and data protection rights on the Internet. We suggest that the European Union, in particular

[14] See below on the gTLD EWG report for ICANN 50.

[15] The Moraes Report voted by the Parliament "[c]*alls on the Commission and the EEAS to take action at the international level, with the UN in particular, and in cooperation with interested partners to implement an EU strategy for democratic governance of the internet in order to prevent undue influence over ICANN's and IANA's activities by any individual entity, company or country by ensuring appropriate representation of all interested parties in these bodies, while avoiding the facilitation of state control or censorship or the balkanisation and fragmentation of the internet*". See Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 21.2.2014, 2013/2188(INI), para 105.

[16] NTIA is the Executive Branch agency that advises the President of the United States on telecommunications and information policy.

[17] See ICANN´s President opening address at ICANN meeting in Singapore on 24 March.

the Commission, takes a leading role in developing an Internet Governance model based on global partnership and full respect of data protection and other fundamental human rights.

II.3. A representative multistakeholder model

20. In setting forth guidelines for shaping the new Internet Governance framework, the Communication refers to the need for a multistakeholder discussion model, in order to ensure that the rules adopted are truly inclusive of all interests and instances at stake.

21. However - as the Commission rightly mentions - the fact that a process is claimed to be multistakeholder, does not *per se* guarantee outcomes that are legitimate and in line with fundamental principles.[18]

22. The multistakeholder method must be shaped adequately in order to gather the opinions of all concerned stakeholders, and be flexible enough to allow the involvement of new categories of stakeholders. The Communication observes the need to make "*efforts to counter the significant differences in the ability to participate across the various stakeholder groups to better ensure representativeness"*.[19] The Communication mentions remote participation at meetings as one such effort. We believe that remote participation alone cannot be sufficient to overcome the considerable asymmetry between internet giants and civil society organisations depending on volunteers and individual donations. The Commission should investigate the possibility of using the various programmes under its control to support efforts to ensure greater representativeness.

23. This is particular important with respect to inclusiveness and accessibility. Respect for fundamental rights must be ensured for all users regardless of their means and capabilities.

24. In this respect, we welcome that the Commission will implement a Global Internet Policy Observatory which could become an important resource for all groups of stakeholders to participate in internet governance processes.

25. In particular, due to their expertise and practical experience with the implementation of data protection and privacy principles, data protection and privacy authorities can make a unique contribution to the development of appropriate policies, structures and procedures at global level. They should be able to participate in the multistakeholder discussions and submit their views in order to ensure that, in shaping the future Internet governance model, due account is taken of individuals' rights to privacy and data protection. This responsibility should be taken into account in their legal mandates and the resources provided to them.

26. We welcome that ICANN has undertaken the establishment of an expert working group on directory services for generic top level domains[20] with a view to replacing the current WHOIS system with a solution taking account, inter alia, of privacy concerns. We also welcome the Commission's participation in this group. We take note that the EWG has so far failed to reach a full consensus in particular on privacy related issues. We urge the ICANN bodies and stakeholders to take proper account of the report and the related arguments[21] in the forthcoming stages of its governance process which may lead eventually to a replacement

[18] See Communication, p. 6.
[19] See Communication, p. 5
[20] Expert Working Group on gTLD Directory Services; https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf.
[21] http://www.internetgovernance.org/2014/06/07/icann-suppresses-a-privacy-advocates-dissent/.

of the current WHOIS system. In this context, we fully share the position of the Article 29 Working Party which has urged ICANN at numerous occasions to change practices which are in conflict with EU data protection law.[22]

III. HOW CAN THE EU HELP SHAPING THE INTERNET?

27. Currently the rules applicable on the Internet as regards privacy and data protection are fragmented, as each country applies its own set of rules to the Internet. The European Union has adopted a set of harmonised rules on data protection as well as rules that impact how the Internet is governed in the EU, which must respect privacy and data protection requirements. With this experience of integrating privacy and data protection requirements in its legislation, the EU should take the lead in promoting at international level the respect of fundamental rights in the policy and governance of the Internet.

III.1. Promoting better protection of privacy and data protection online

28. Privacy and data protection are enshrined in the primary sources of European Union law. Article 16 TFEU provides that "[e]*veryone has the right to the protection of personal data concerning them*". The Charter of Fundamental Rights of the European Union ("Charter") identifies and explains the fundamental rights to privacy (Article 7) and to data protection (Article 8). These rights are elaborated in secondary legislation, in particular Directive 95/46/EC and Regulation 45/2001, which lay down the general legal framework for data protection. Other legislation complements this general framework, in particular, Directive 2002/58/EC governing the processing of personal data in electronic communications ("the ePrivacy Directive").

Updating the EU legal framework applicable to privacy and data protection to the Internet and technological progress

29. In the Communication, the Commission commits itself to work to achieve rapid adoption and implementation of key legislation (including the proposed General Data Protection Regulation or GDPR) and, thus, strengthen trust online.

30. We welcome this commitment, especially since the recent surveillance scandal has revealed the extent of undue interference with individuals' rights to privacy and data protection and has shaken users´ confidence and trust in the Internet as a tool for engaging in social interaction and participating in the public debate.

31. We consider, in addition, that once the GDPR has been adopted, it will provide the Commission with a solid basis to promote EU data protection rules as standards to be adopted at international level, including Internet Governance.

32. The GDPR, in fact, introduces a number of provisions with significant effects on the regulation of data protection online and addresses a number of issues which are crucial for Internet Governance.

Consistent application and enforcement

[22] E.g. Letter by Article 29 Chair to ICANN General Counsel of 8 January 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140108_letter_icann.pdf.

33. The GDPR will introduce a mechanism for ensuring consistency in the application of data protection legislation across the entire Union, thus ensuring, inter alia, legal certainty for data subjects and controllers for transnational transactions on the internet. The mechanisms developed between EU Member States for this objective, including the one-stop-shop principle, provide a model for other cross-jurisdictional issues related to internet governance and other world regions.

Improved data subject´s rights

34. The GDPR brings about substantial improvements of the rights of the data subject, particularly in situations where interference with their right to privacy might be magnified by online interaction. Examples include Article 11 (obligation on controllers to provide transparent and easily accessible and understandable information), Article 12 (obligation on controllers to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests), and Article 14 (controller's information obligations towards the data subject, additional information to be provided on storage period, right to lodge a complaint, international data transfers and source from which the data are originating). The strengthening of data subjects' rights online is an important element of the EU data protection reform, which could be promoted by the Commission on a global scale so as to benefit all individuals interacting online.

Right to be forgotten

35. Article 17 of the GDPR provides for the right to be forgotten and erasure, which is particularly important in the Internet era. Interestingly -regardless of whether Article 17 is ultimately adopted in the initial version of the proposal- the Court of Justice has defined the scope and conditions of application of the existing right of erasure, as laid down in Article 12(b) of Directive 95/46/EC, on the Internet. In *Google v AEPD*[23], the Court decided on the applicant`s request to erase links to information in a newspaper about his bankruptcy which, although obsolete, was still indexed by Google in its search engine. In balancing the right to erasure against the freedom of information, the Court concluded that the former overrides the general public's right to be informed, unless the data subject plays a role in public life that justifies interference with his/her right to privacy.[24]

36. The consequences of the ruling for the Internet at a global scale remain to be seen. While it is most welcome that individuals should have the right to rectify or delete, under certain conditions, data processed over the Internet about them, the EU certainly has a role to play in guiding other jurisdictions on how to achieve a proper balance of all interests and rights over the Internet.

III.2. Internet policies must reconcile security requirements and fundamental rights

37. The Communication argues that confidence in the Internet and its governance is a prerequisite for the realisation of the Internet's potential as an engine for economic growth and innovation. The safety, security, stability and resilience of the Internet are crucial to preserve and foster the economic and societal benefits of the digital ecosystem.[25]

[23] Case C-131/12, *Google Spain and Google v AEPD*, judgment of 13 May 2014.
[24] *Google v AEPD*, para 97.
[25] See Communication, p. 9.

38. We agree that -especially after the recent revelations about mass surveillance- there is a need to restore users´ confidence in the Internet and in the use of personal data on the Internet. As indicated in our previous opinion on the Cyber Security Strategy,[26] we believe that, due to the ever growing use of Information and Communication Technologies, measures aimed at ensuring a high level of security on the Internet should help improve the security of all the information processed therein, including personal data. In particular, we consider that security of data processing has always been a crucial element of data protection as security requirements are included in a number of data protection provisions.[27] Therefore, improving the security standards of the Internet will increase the protection of users` personal data and prevent undue interference to occur. We consider that improved standardisation of network and information security requirements at international level will also help address more efficiently the needs for trust and security.

39. In this respect, we welcome the clarification that security is not opposed to privacy and data protection. We recall the explicit recognition of privacy and data protection in the Cyber Security Strategy and the fact that they are considered as core values which should guide cyber security policy in the EU and internationally.

40. A Cyber Security system should complement, rather than overlap or contradict existing (and forthcoming) data protection provisions. To this end, we invite the Commission to take action to facilitate coordination of security policies at global level, as any conflict of such policies would jeopardise both security and data protection.

III.3. Encouraging the design and development of privacy friendly solutions for the Internet

41. The principles of *data protection-by-design* and *by-default* could serve as significant enablers of trust on the Internet. While the Communication does not refer to these principles, it points out that "*design can impact on human rights such as users' data protection rights and security*..." and that "[a]n *effective multistakeholder approach to specification setting on the internet will be based on efficient mutual interactions between technical and public policy considerations so that technical specifications more systematically take into account public policy concerns*".[28]

42. We welcome that the Communication takes account of the importance of technical design, recognizing that standardisation and specification are crucial phases in which attention must be given to individual rights and public policy needs. *Data protection-by-design* ensures that important public policy concerns, such as privacy and data protection, are taken into account at the right time, where relevant.

---

[26] See the EDPS Opinion of 14 June 2013 on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf.

[27] Security requirements are contained in Articles 22 and 35 of Regulation (EC) No 45/2001, Articles 16 and 17 of Directive 95/46/EC and Articles 4 and 5 of Directive 2002/58/EC, as well as in Article 7 of the Convention 108 of the Council of Europe on Data Protection, adopted in 1981 and by now ratified by all EU Member States.

[28] See Communication, pp. 8-9.

43. We particularly welcome the reference to RFC 6973, which aims to provide guidance on applying the data protection-by-design principle in the design of internet protocols. This is a promising starting point which needs to be put in practice not only in the technical design process but also in the structure and processes of the organisations promoting the technical design of the internet, such as IETF, W3C etc.

44. The Commission should promote structures and mechanisms supporting the application of both *data protection-by-design* and *by-default* as guiding principles in the shaping of a new governance model. It should therefore ensure that data protection mechanisms and safeguards are included, from the outset, in the design of normative and technical governance tools.

45. The Commission should also use its policy and financial instruments to support the development of technical solutions for the internet that demonstrate how privacy can be respected in internet protocols, services and applications.[29]

III.4. Guaranteeing net neutrality to Internet users

46. Another challenge that should be addressed in discussing a new Internet Governance model is net neutrality. The Communication refers in various instances to the fact that the Internet infrastructure should remain "*one single unfragmented space*"[30] without elaborating further on the topic of net neutrality. An extensive debate is currently going on in relation to net neutrality in different forms and shapes and the arguments in support of the various positions are well known.

47. We have released a specific Opinion on the topic, addressing the impact of net neutrality on privacy and data protection and pointing out the dangers to privacy from the technology.[31] Our major concern is that, in a non-neutral network environment, in order to ensure paying content providers the priority they are subscribing for, ISPs engage in *deep packet inspections*, scanning extensively the data uploaded by Internet users, accessing the content of their communications and filtering out data that should not have priority.[32]

48. In its proposal for a new regulation for a European single market of electronic communications,[33] the Commission referred in Article 23 to the "*Freedom to provide and avail of open internet access, and reasonable traffic management*". We commented on the proposal in a specific Opinion,[34] expressing, *inter alia*, the concern that the proposal provides a number of grounds for traffic management measures that scan and discriminate among

[29] The EDPS has launched together with other DPAs an initiative for privacy-aware design of internet services, the Internet Privacy Engineering Network, IPEN.
[30] See Communication, p. 3.
[31] Opinion of 7 October 2011 on net neutrality, traffic management and the protection of privacy and personal data, OJ C 34/01, 08.02.2012, p. 1.
[32] Deep packet inspection enables the ISP to access information addressed to the recipient of the communication only. Taking the usual postal service as an example, this approach is equivalent to opening the envelope and reading the letter inside to perform an analysis of the content of the communication (encapsulated inside the IP packets) in order to apply a specific network policy.
[33] COM (2013)627 final.
[34] Opinion of 14 November 2013 on the Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-11-14_Single_Market_Electronic_Communications_EN.pdf.

various types of content, thus leaving the door open to the interferences with data protection we have mentioned above.

49. We strongly recommend, therefore, that, without any prejudice to a healthy public debate on network neutrality, any solution ultimately adopted on this delicate topic both at EU and international level gathers widespread consensus on the need to provide for adequate safeguards for users and their rights. We call on the Commission to defend this position in the debate on net neutrality.

IV. PROPOSALS FOR FURTHER ACTION AT INTERNATIONAL LEVEL

IV.1. Solving conflicts of jurisdiction and law

50. In recalling the importance of the Internet as a single unfragmented infrastructure, the Communication also points to the important issue of jurisdiction over the Internet and conflicts of laws.

51. In particular, it takes the view that a more thorough reflection on how existing rules apply on the Internet is needed, even more so as "*extraterritorial application of national law, often based on the geographies of the Domain Name System, has led to a number of contradictory legal decisions*".[35] In addition, the complexity and, in some cases, the opaqueness of contractual arrangements between providers and users add uncertainty to the application of the correct jurisdiction and law.

52. In this respect, the Communication notes that, at international level, conflict rules are insufficiently developed, leading to unsolved conflicts of laws beyond the Union. The Commission, therefore commits itself to addressing the tension between a global Internet and national jurisdictions.[36]

53. In doing so, the Commission will launch an in-depth review of the risks, at international level, of conflicts of laws and jurisdictions arising on the Internet and assess all mechanisms, processes and tools available and necessary to solve such conflicts.[37]

54. We very much welcome these efforts, as legal uncertainty and multiplicity of legal provisions are certainly harmful to users and should be timely and effectively addressed.

55. In particular, we note that, given the global and cross-border nature of the Internet, personal data are often transferred to and processed in jurisdictions other than those in which users have submitted their data, exposing them to the risk of lower or no data protection. In addition, controllers processing personal data on the Internet may be faced with conflicting laws and obligations and must choose between violating foreign obligations or EU data protection law. They may be obliged to disclose data of users regardless of EU data protection safeguards (*e.g.* access requests by surveillance bodies in foreign jurisdictions), which in consequence undermines the data protection safeguards afforded to users under EU law.

[35] See Communication, p. 10.
[36] See Communication, p. 11.
[37] See Communication, p. 11.

56. In this respect, valuable guidance on the applicable law in connection with data processing taking place on the Internet is provided by the recent judgment of the Court of Justice in the *Google v AEPD* case.[38] In that judgment, the Court has taken into account a number of elements, such as the presence of an establishment on the territory of an EU Member State and the relationship between the activities of that establishment and the data processing at issue, to decide on the applicability of EU data protection law to a processing carried out online.

57. None the less, conflicts of jurisdiction remain possible and difficult to resolve in other cases, in particular as regards legal obligations imposed on controllers based in foreign jurisdictions (such as requests for access for surveillance purposes, financial reporting obligations to foreign authorities, etc).

58. From a European perspective, we would encourage controllers processing the personal data of EU individuals on the Internet to increase the transparency and the amount of information they provide to users in relation to the law(s) they are subject to and the data protection rules they are bound to apply, including laws on access to data by governmental bodies, jurisdictions where data may be processed, what safeguards have been implemented to protect users' data (*e.g.* in respect of international transfers of data). As a result, users would be better aware of their rights and possible restrictions thereof.

59. We welcome the work to be done by the Commission in assessing all mechanisms, processes and tools available and necessary to solve such conflicts. This will necessarily involve closer cooperation of states at the international level in order to find ways to resolve conflicts (such as by defining common standards and developing better cooperation mechanisms between competent authorities).

IV.2. Need for improved international standards and cooperation

60. In discussing conflicts of jurisdiction, the Commission makes it clear that its work aimed at finding an effective solution will build on existing policies.[39] Also, at the beginning of the Communication, the Commission emphasizes that it does not call for any new international legal instrument to address the issues of Internet Governance.[40]

61. We do not support the view that the legal tools to address the challenges of a new Internet Governance model are already in place and will cater for all policy needs, once policy is clearly defined. We believe, on the contrary, that significant efforts need to be deployed in order to build a governance framework which is at the same time comprehensive and responsive to issues posed by the fast-changing reality of the Internet. In addition, much work will be needed in order to cause all international stakeholders to adhere to the same governance standards, whether they are already existing legal tools or minimum common rules and principles yet to be adopted.

62. In this respect, there are many interesting initiatives at international level which provide excellent opportunities for discussing, seeking agreement and building consensus on the

[38] See footnote 23, above**Error! Bookmark not defined.**.
[39] See Communication, p. 11.
[40] See Communication, p. 3.

measures most needed. For example, we have already cited the Net Mundial meeting in Brazil, which called for greater privacy safeguards.[41]

63. Other existing legal tools which may facilitate the convergence of different interests on common data protection standards include the Madrid International Standards on the Protection of Personal Data and Privacy[42] and the international instruments mentioned above (paragraph 11), including Convention 108 of the Council of Europe - which provides workable standards of data protection to which all countries may subscribe - and the OECD revised Guidelines of 2013.[43] Finally, on the topic of security and data protection, it is important to refer to the Budapest Convention[44] which provides standard rules in the field of the fight against cybercrime.

64. We support the view that, in order to promote privacy standards internationally, third countries should accede to Convention 108, which is open to countries which are not members of the Council of Europe (as was the case of Uruguay in 2012). We also support the improvement of cooperation among data protection authorities and privacy enforcement authorities around the world, as this would facilitate the enforcement of national, regional and international privacy and data protection laws in cross-border situations.

65. The initiatives listed above are remarkable efforts to address the open policy issues concerning the Internet. However, in shaping a new Internet Governance framework, it is crucial to ensure that EU standards are not undermined (by adopting legislation and/or committing to agreements and initiatives which do not respect the fundamental rights enshrined in the Charter[45]) and that more sets of common rules and principles are adopted on specific issues - for instance, on access to data for surveillance and/or law enforcement purposes.

66. In this respect, and in the light of the commitments made in the Communication, we expect the Commission to take the lead of, and act as a catalyst in, the discussions on the new Internet Governance model. In particular, we encourage the Commission as Guardian of the Treaties to internationally promote EU rules on the protection of personal data as well as to encourage the accession by third countries to relevant international data protection standards. Furthermore, we support the adoption of an international instrument requiring the respect of common data protection standards by intelligence and law enforcement bodies.

V. CONCLUSION

67. We welcome the Commission's efforts in the Communication to identify the main policy areas in need of reform, in the aftermath of the surveillance scandals that have shaken the confidence of Internet users as a tool for participating in democratic debate.

---

[41] See footnote **Error! Bookmark not defined.**, above.
[42] Available at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/index-iden-idweb.html .
[43] Available at http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines.
[44] Council of Europe Convention no. 185 on Cybercrime, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=22/05/2014&CL=ENG
[45] In Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, judgment of 8 April 2014, para 47, the Court of Justice has ruled that "*where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference*".

68. The Commission has recognised the need for a shared and truly global model of Internet Governance and, as a consequence, has committed itself to a number of initiatives aiming at making the reform process as inclusive and transparent as possible.

69. Building on the Commission proposals and efforts we have formulated a number of suggestions in this Opinion designed to address effectively the critical issues concerning the tight relationship between privacy and data protection and the Internet.

70. In particular, our remarks focus on the following points:

- Internet policy discussions should take into account the nature of fundamental rights of privacy and data protection. Such rights are at the basis of users` online interactions and should be protected online as well as offline.

- Discussions over Internet Governance should include privacy and data protection as a priority.

- In the framework of a multistakeholder approach to Internet Governance, we support measures to ensure broad stakeholder representation, including the recognition of the role of data protection authorities in improving the consistency of enforcement of data protection rules at global level.

- We welcome that the Commission is committed to promoting the swift adoption of key legislation, in particular the proposed General Data Protection Regulation. The strengthening of data subjects' rights and the right to erasure should become part of the Internet Governance reform.

- The Commission should promote a comprehensive approach to Internet Governance, and ensure security of personal data processing. We invite the Commission to take action in order to facilitate coordination of security policies at global level, as any conflict of such policies would jeopardise both security and data protection.

- We welcome the Commission's reference to the close relationship between technological design and data protection. We encourage the Commission to work towards the inclusion of optimal data protection standards in the technology at the early design phase (*data protection-by-design* and *data protection-by-default*).

- In relation to network neutrality, we strongly recommend, that, without prejudice to the current debate on network neutrality, any solution ultimately adopted should gather widespread consensus as to the principles to be applied and on the need to provide for adequate safeguards for users and their rights.

- We support the Commission`s efforts in finding a rapid solution to conflicts of law that often arise in connection with the Internet and jeopardise users´ rights to privacy and data protection. We also propose that, in cases involving conflicting jurisdictions, users are provided with additional and more accurate information as to the data protection laws and safeguards applied to the processing of their personal data.

- We call for greater efforts, by the Commission and other private and public stakeholders, in order to reinforce international cooperation in the field of data protection as well as the

convergence of international stakeholders on common technical and data protection standards.

- We expect the Commission to show leadership and act as a catalyst in the discussions on the new Internet Governance model. In particular, we encourage the Commission to promote EU standards on data protection as well as to encourage the accession by third countries to relevant international data protection standards. Furthermore, we support the adoption of an international instrument requiring the respect of data protection standards by intelligence and law enforcement bodies.

Done in Brussels, 23 June 2014

(signed)

Giovanni BUTTARELLI