WSIS Civil Society Privacy and Security Working Group
WSIS Civil Society Human Rights Caucus

Language proposals on Internet Governance
here: Paragraphs 49-54 of the Chair's paper
Final version for submission, 26 September 2005, 14:30 CEST
Comments are in italics.

Chair's Paper (Document WSIS-II/PC-3/DT/10-E	**Language proposed by Civil Society**
49. We seek to counter the growing threats to the stability and security of the Internet. **We reaffirm** that a global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.	***Note:*** *This is agreed language from paragraph 35 of the Geneva Declaration of Principles, but the first part on "consumer protection" and "user confidence" is missing.*
50. We underline the need to develop effective instruments and efficient mechanisms for the prosecution of crimes using technological means, that are committed in one jurisdiction but have effects in another. **We call upon governments**, in cooperation with other stakeholders, to continue to develop appropriate instruments and mechanisms, including treaties and enhanced cooperation, to allow for effective criminal investigation and prosecution of crimes committed in cyberspace as well as against networks and technological resources. This should address the problem of cross-border jurisdiction, regardless of the territory from which the crime was committed and/or the location of the technological means used, while respecting sovereignty.	**50. We underline the need to develop** effective instruments and efficient mechanisms for the prosecution of crimes using technological means, that are committed in one jurisdiction but have effects in another. **We call upon governments**, in cooperation with other stakeholders, to continue to develop appropriate instruments and mechanisms, including treaties and enhanced cooperation, to allow for effective criminal investigation and prosecution of crimes committed in cyberspace as well as against networks and technological resources. This should address the problem of cross-border jurisdiction, regardless of the territory from which the crime was committed and/or the location of the technological means used, while respecting <u>human rights,</u> sovereignty, <u>openness, accountability, and civil liberties</u>. <u>All efforts in this regard must be consistent with the rights to freedom of expression and privacy, and they must comply with the principles of due legal process</u>.

51. We resolve to deal effectively with the significant and growing problem posed by spam. **We call upon governments**, in cooperation with other stakeholders, to adopt a multi-pronged approach to counter spam. This would entail: a) appropriate legislation and enforcement; b) development of technical measures; c) establishment of multi-stakeholder partnerships; d) awareness raising and user education of anti-spam measures; e) development of a global and coordinated approach to the problem.	**51. We resolve to deal effectively** with the significant and growing problems of privacy invasion, identity-theft and spam. **We call upon governments**, in cooperation with other stakeholders, to adopt a multi-pronged approach to counter these problems. This would entail: a) appropriate legislation and enforcement; b) privacy impact assessments and the development of technical measures; c) establishment of multi-stakeholder partnerships; d) awareness raising and education of policy makers, data controllers, end-users and producers about privacy-enhancing measures; e) development of a global and coordinated approach to the problems; f) mainstreaming of measures to ensure privacy protection in internet governance capacity-building programs.
52. We reaffirm our commitment to the freedom to seek, receive, impart and use information for the creation, accumulation and dissemination of knowledge. **We urge** that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam do not violate the provisions for freedom of expression as contained in the Universal Declaration of Human Rights and the WSIS Declaration of Principles.	**52. We reaffirm our commitment** to the freedom to seek, receive, impart and use information for the creation, accumulation and dissemination of knowledge. **We will ensure** that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam protect and promote ~~do not violate~~ the provisions for privacy and freedom of expression as contained in the Universal Declaration of Human Rights and the WSIS Declaration of Principles.

	New 53a. The right to privacy is a human right and is essential, especially on the Internet where all social interaction takes place through technology. The collection, retention, use and disclosure of personal data, no matter by whom, should remain under the control of and determined by the individual concerned.
53. **We encourage** those governments that have adopted legislation on privacy and/or data protection to coordinate these measures, and their enforcement, with other countries and **we call upon** those governments that have not yet developed such measures to consider doing so, with the participation of all stakeholders.	**53b.** *(revised old 53)* **We encourage** those governments that have adopted legislation on privacy and/or data protection to coordinate these measures, and their enforcement, with other countries and stakeholders, and **we ~~call upon~~ urge** those governments that have not yet developed such measures to ~~consider doing~~ do so, with the participation of all stakeholders. The broad set of privacy issues related to Internet governance should be discussed in a multi-stakeholder setting. **We agree** on the establishment of a global Privacy Forum.
	New 53c. International, national and local measures must ensure open and transparent voting processes that fully and completely guarantee the privacy and integrity of the vote if and when electronic voting technologies are implemented.
54. **We call for** the policy and privacy requirements of global electronic authentication systems to be developed through a multi-stakeholder process.	**54.** **We call for** the policy and privacy requirements of global electronic authentication systems to be developed through a multi-stakeholder process. The possibility of communicating and using the Internet anonymously must be ensured for everyone.