SCRIPT-ed

The World Summit on the Information Society – Privacy not Found?

Ralf Bendrath and Rikke Frank Jørgensen[*]

Abstract

This article will explore how privacy was dealt with in the United Nations World Summit on the Information Society (WSIS) process. WSIS was the first time that information and communication technology was linked to human rights and development on the global policy agenda. The article will argue that though the WSIS documents ended up with a formal commitment to human rights, there was de facto no recognition of privacy as a human right which is fundamentally affected by the design and use of technology. On the contrary, privacy continues to be dealt with as a marginal issue attached to an overarching agenda of state security. We will conclude that the post WSIS phase is showing some momentum in favor of privacy, due to new emerging alliances between civil society and industry.

---

[*] Ralf Bendrath is a researcher at the Collaborative Research Center „Transformations of the State" at the University of Bremen, Germany, and co-coordinator of the WSIS Civil Society Privacy and Security Working Group. Rikke Frank Jørgensen is a senior advisor at the Danish Human Rights Institute, and co-chair of the WSIS Civil Society Human Rights Caucus.

1. Introduction

This article will explore how privacy was dealt with in the United Nations World Summit on the Information Society (WSIS) process. WSIS was the first time that information and communication technology was linked to human rights and development on the global policy agenda. The article will argue that though the WSIS documents ended up with a formal commitment to human rights, there was de facto no recognition of privacy as a human right which is fundamentally affected by the design and use of technology. On the contrary, privacy continues to be dealt with as a marginal issue attached to an overarching agenda of state security. We will conclude that the post WSIS phase is showing some momentum in favour of privacy, due to new emerging alliances between civil society and industry.

2. The World Summit on the Information Society

WSIS was the first in the series of United Nations (UN) summits arranged to deal with information society issues.[1] It took place in two meetings which are officially regarded one summit: The first WSIS in Geneva in December 2003, and the second one in Tunis in November 2005. The Summit process was initiated by the UN General Assembly in 2001. The task of the Summit was not a small one: to develop a "common vision of the information society." In the UN resolution which initiated the WSIS process, it is stressed that both governments, international organisations, the private sector and civil society are encouraged to effectively contribute to, and actively participate in, the preparatory process of the Summit.[2]

2.1 The First Summit: Trying to get privacy on the agenda

At the Geneva summit in December 2003, the governments adopted a Declaration of Principles[3] and a Plan of Action.[4] Civil society groups active at the summit lobbied to improve these documents and to centre them more around human rights and justice, but in the end issued two separate documents: "Shaping Information Societies for

---

[1] Official web site <*http://www.wsis.org*>
For an overview of WSIS, see: EPIC, *The public voice WSIS sourcebook: Perspectives on the World Summit on the Information Society* (2004); W Kleinwächter and D Stauffacher(eds), *The World Summit on the Information Society – moving from the past into the future* (2005); M Raboy and N Landry, *Civil society, communication and global governance: Issues from the World Summit on the Information Society* (2005). For comprehensive WSIS Civil Society news, analysis, and documents, see <*http://www.worldsummit2005.org*>

[2] UN General Assembly, fifty-sixth session: Res 56/183 of 31 Jan 2002 World Summit on the Information Society <*http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf*>

[3] WSIS-03/GENEVA/DOC/4-E of 12 December 2003 on World Summit on the Information Society: WSIS Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium. <*http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160*>

[4] WSIS-03/GENEVA/DOC/5-E of 12 December 2003 on World Summit on the Information Society: WSIS Plan of Action <*http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160*>

Human Needs: Civil Society Declaration to the World Summit on the Information Society,"[5] and "Civil Society Essential Benchmarks for WSIS."[6]

As the idea for the summit had developed first in the International Telecommunications Union (ITU), the telecommunications body of the UN, the initial focus was quite technology-centred. Mainly because of the efforts of civil society activists and academics, the discussion gradually moved from "information" (read: ICTs) to "society" over the course of the summit preparations. One outcome was that human rights gained a prominent place in the Geneva Summit Declaration and Plan of Action. The Universal Declaration of Human Rights is underlined in the first paragraph of the summit declaration, and its article 19 on freedom of expression is quoted as "central to the Information Society."[7]

The summit preparations took place in the context of the global "war on terrorism," and one of the highlighted topics was security.[8] This was a key issue for the United States and the Russian Federation, and was already on the agenda in international organizations like the Council of Europe,[9] the OECD[10] and the UN General Assembly,[11] where Cyber-Security or similar topics have moved up the agenda in recent years. The relevant paragraph of the WSIS summit declaration ends with an explicit reference to the war on terrorism: "It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights."

In contrast, the protection of privacy was not a prioritised issue and the first drafts of the summit declaration had no reference to privacy. Civil society groups active in Geneva were concerned about the strong focus on security and argued that it was a vague political goal that could be higher or lower on the agenda depending on day-to-day politics, and which may be misused for political purposes to restrict fundamental freedoms. Further, the notion of security has different meanings whether it refers to public security (e.g. protection against war or crimes), technical security (e.g. security of networks), data security (e.g. protection against data theft) or the security of the

---

[5] Civil Society Declaration to the World Summit on the Information Society of 8 Dec 2003 on Shaping Information Societies for Human Needs <*http://www.worldsummit2003.de/download_en/WSIS-CS-Decl-08Dec2003-en.pdf*>

[6] Civil Society Essential Benchmarks for WSIS of 3 Nov 2003 <*http://www.worldsummit2003.de/download_en/CS-Essential-Benchmarks-for-WSIS-14-11-03-final.rtf*>

[7] For an analysis of human rights in the WSIS process, see R Frank Jørgensen (ed), *Human Rights in the Global Information Society* (2006).

[8] For a more comprehensive analysis of the security and privacy discussions before the summit, see R Bendrath, "National Security or Civil Liberties? WSIS debate on security issues in deadlock" in Olga Drossou (ed), *Visions in process. World Summit on the Information Society Geneva 2003 - Tunis 2005* (2003) <*http://www.worldsummit2003.de/download_de/Vision_in_process.pdf*>

[9] Council of Europe of 23 Nov 2001on Convention on Cybercrime <*http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm*>

[10] Organization for Economic Cooperation and Development (OECD) of 25 July 2002 on Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security <*http://www.oecd.org/dataoecd/16/22/15582260.pdf*>

[11] UN General Assembly, fifty-seventh session: Res 57/239 of 31 January 2003 on Creation of a global culture of cyber security <*http://ods-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf*>

individual (e.g. protection against misuse of power or surveillance from state or private parties). Privacy and other civil liberties, on the other hand, are constitutional fundamentals of every democracy and must be protected as such.

The civil society groups active in the WSIS process, mainly the Privacy and Security Working Group (PSWG) and the Human Rights Caucus, advocated the insertion of a new paragraph specifically devoted to privacy, placed at the beginning of the "security" section of the summit declaration.[12] However, the whole debate in the intergovernmental drafting group on security was focused on the security language, and no delegation wanted to insist strongly on privacy. Privacy was later mentioned in the summit declaration only due to some efforts of the European Union, Switzerland, Brazil, Australia and a few other countries.
The 2003 Geneva Declaration of Principles calls for a "global culture of cyber-security," in particular for strengthening a "trust framework, including information security and network security, authentication, privacy and consumer protection." Here, privacy and security as well as authentication and consumer protection are seen as parts of a common strategy. Only "within this global culture of cyber-security, is [it] important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade," the summit declaration reads. Both civil society groups and the private sector suggested more specific privacy language in the summit declaration. The Coordinating Committee of Business Interlocutors set up for the WSIS by the International Chamber of Commerce, for example had asked for "*effective* privacy protection of personal data."[13] In sum, privacy gained very limited formal recognition in the Geneva summit documents compared to other civil liberties such as e.g. freedom of expression.

The Plan of Action, which was also adopted by the 2003 Geneva summit is generally vague. It was intended to facilitate the implementation of the principles espoused in the Declaration and provide concrete measures of progress for the development of the Information Society. However, besides some initiatives like connecting every school and library in the world to the Internet by 2015, there are no concrete benchmarks or indicators for implementation. The second phase of the summit that ended in Tunis in November 2005 was supposed to bring more substance and define processes for the follow-up and implementation.

The paragraph of the Geneva Plan of Action that deals with security and privacy does not mention the "war on terrorism," but is mainly focused on security and makes an implicit reference to the Council of Europe's Cybercrime Convention.[14] Of the ten initiatives suggested by the action plan in the context of security and privacy, only one specifically mentions privacy. It calls for "user education and awareness,"

---

[12] The paragraph would have read "The right to privacy is a human right and is essential for self-determined human development in regard to civic, political, social, economic, and cultural activities. It must be protected online, offline, in public spaces, at home and in the workplace. Every person must have the right to decide freely whether and in what manner he or she wants to receive information and communicate with others. The possibility of communicating anonymously must be ensured for everyone. 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." *Crucial Issues for Privacy and Security Working Group* of Geneva, 22 Sept 2003.

[13] Paragraph for the Declaration of Principles suggested by the Coordinating Committee of Business Interlocutors, 27 Aug 2003. Italics added.

[14] See note 9 above

specifically about "online privacy and the means of protecting privacy."[15] There is no reference to specific measures or initiatives that governments or private companies should take to ensure protection of the large amounts of personal information, which they handle.

2.2 In between the summits: Progress in the Working Group on Internet Governance

The second summit phase mainly discussed implementation and follow-up, financing, and the contested issue of Internet governance. UN secretary-general Kofi Annan in November 2004 set up an independent "Working Group on Internet Governance" (WGIG),[16] following a mandate from the Geneva WSIS Summit. Its task was to define "Internet governance", identify public policy issues related to it, and develop a common understanding of the respective roles and responsibilities of the different stakeholders. The WGIG was seen as a model for new international diplomacy processes, since it had a balanced membership from governments, the private sector, civil society, and international organizations. The group conducted regular open online and offline consultations and produced a number of "issue papers". One of these dealt with "consumer protection and privacy", but the content was mixed and included language like "while privacy is recognized as a human right, it is a right that balances the competing and legitimate interests of government and business to intrude upon privacy under law."[17]

The PSWG suggested including privacy as a key element of the WGIG deliberations, because "in an 'Information Society', where almost all attributes of an individual can be known, interactions mapped, and intentions assumed based on records, the need for protection of privacy is more crucial than ever."[18] Like many other stakeholders, the International Working Group on Data Protection in Telecommunications[19] also submitted input to the WGIG and e.g. referred to its "Ten Commandments to protect Privacy in the Internet World".[20]

---

[15] "Governments, and other stakeholders, should actively promote user education and awareness about online privacy and the means of protecting privacy," WSIS Plan of Action 2003 (12 c).

[16] See <*http://www.wgig.org*>

[17] Working Group on Internet Governance (WGIG) of February 2005 on Draft Issues Paper on Consumer, User Protection and Privacy <*http://www.wgig.org/docs/WP-Consumer.pdf*>

[18] Statement of the Civil Society Privacy and Security Working Group (PSWG) of 24 Feb 2005 at PrepCom2 <*http://www.itu.int/wsis/docs2/pc2/plenary/24feb-privacy.doc*>. It should be noted that this was the first ever civil society intervention in the WSIS process that was read in Arabic. See also the PSWG comment to the WGIG issue paper on Cybersecurity and Cybercrime at <*http://www.wgig.org/docs/CommentWSIS-CS3.doc*> and the two PSWG comments on Consumer Protection and Privacy <*http://www.wgig.org/docs/CommentWSIS-CS1.doc*> and <*http://www.wgig.org/docs/CommentWSIS-CS2.doc*>. All comments to the WGIG are available at <*http://www.wgig.org*>

[19] The IWGDPT, also called the "Berlin Group", mainly consists of national data protection commissioners. See <*http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm*>

[20] International Working Group on Data Protection in Telecommunications of 12 April 2005 on Comments on WGIG Draft Issues Paper on Consumer, User Protection and Privacy <*http://www.wgig.org/docs/Letter-IWGDPT.pdf*>

The WGIG report was published on 15 July 2005.[21] While the centre of discussions had been around the unilateral control of core Internet resources by the U.S. government, the report also dealt with other Internet governance issues like interconnection costs, multilingual domain names, spam, and intellectual property rights. It also contained a paragraph on data protection and privacy rights. The WGIG stated that there was "a lack of national legislation and enforceable global standards for privacy and data-protection rights over the Internet" and recommended to the Tunis summit to "encourage countries that lack privacy and/or personal data-protection legislation to develop clear rules and legal frameworks, with the participation of all stakeholders, to protect citizens against the misuse of personal data, particularly countries with no legal tradition in these fields".

The WGIG also suggested a revision of the privacy policies for the WHOIS databases according to data protection law in the country of the registrar and the registrand, and the development of open technical proposals for privacy requirements for global electronic authentication systems. The WGIG recommended that "arrangements and procedures between national law enforcement agencies" should be "consistent with the appropriate protection of privacy, personal data and other human rights", and as a general rule asked to "ensure that all measures taken in relation to the Internet, in particular those on grounds of security or to fight crime, do not lead to violations of human rights principles". The WGIG background report includes a lengthy paragraph on privacy that begins by stating that privacy "becomes even more important over the Internet, where the intrinsic nature of the Internet makes it possible to effectively track an individual in cyberspace and use information about him/her illegally or without authorization. Threats to personal privacy increase the mistrust towards the Internet."[22]

2.3 The second summit: Improvements and setbacks for privacy

The emphasis on privacy protection in the WGIG report was an improvement compared to the Geneva Summit documents from 2003. This was mainly possible because the members of the WGIG were acting in personal capacity and as peers, which gave civil society members more influence on the outcome than during the intergovernmental negotiations for the summit documents. However, the WGIG report only contained recommendations, as it provided a basis for negotiations among governments before the second summit in Tunis November 2005. The underlying conflicts resurfaced at the 3rd preparatory committee (PrepCom) meeting in September 2005. Its task was to finalize drafts of two summit documents – the "Tunis Agenda" with detailed follow-up on Internet governance, financing and other issues, and the "Tunis Commitment", a shorter document re-emphasizing the Geneva Principles.

There was some momentum building up in favor of stronger privacy protection in the run-up to that meeting. Just a week before, the international network of Data Protection Commissioners had convened at its annual conference in Montreux. In the

---

[21] Report of the Working Group on Internet Governance, Château de Bossey of June 2005 *<http://www.wgig.org/docs/WGIGREPORT.pdf>*. Translations into all UN working languages are available at *<http://www.wgig.org>*.

[22] Working Group on Internet Governance of June 2005 on Background Report (141) *<http://www.wgig.org/docs/Background-Report.htm>*

Montreux Declaration, the commissioners appealed "to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights."[23] This also echoed commitments taken by the Iberoamerican summit of Santa Cruz in 2003, [24] the Francophonie Summit of Ouagadougou in 2004,[25] and the "Declaration on Human Rights and the Rule of Law in the Information Society"[26] adopted by the Council of Europe in 2005. The International Working Group on Data Protection in Telecommunications also sent a letter to the chairman of the Internet governance negotiations in Geneva, Pakistan Ambassador Masood Khan, urging him to "should not be neglected or become part of a trade-off when the main political issues of Internet governance such as the future structure of ICANN are being discussed".[27] There was therefore a slight momentum for privacy in the months leading up to the Tunis Summit.

In line with the Montreux declaration, the PSWG encouraged the governments to adopt a commitment for developing a global legal framework that ensured the rights to privacy and data protection to all citizens within the Information Society. They proposed, as did the International Working Group on Data Protection in Telecommunications, to install a global Privacy Forum to prepare multilateral negotiations for a privacy agreement.

The first draft by chairman Khan actually contained an explicit reference to these proposals, by stressing the need for the *legal* protection of privacy, and encouraging countries that lack such legislation to adopt it:

> *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.[28]*

In the end, this proposal was watered down, mainly because the U.S. government and the private sector were not in favour of legal privacy regulation. However, the final

---

[23] 27th International Conference of Data Protection and Privacy Commissioners: Montreux Declaration. "The protection of personal data and privacy in a globalised world: a universal right respecting diversities" of 16 Sept 2005
<http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>

[24] Thirteenth Ibero-American Sumit Meeting of Heads of State and Heads of Government of 14-15 Nov 2003 on Declaration of Santa Cruz De La Sierra" (45): "Social Inclusion, the Driving Force Behind the Development of the Ibero-American Community".

[25] Xe Conférence des chefs d'Etat et de gouvernement des pays ayant le français en partage of 26-27 November 2004 on Déclaration de Ouagadougou *<http://www.francophonie.org/doc/txt-reference/decl-ouagadougou-2004.pdf>*

[26] Council of Europe CM(2005)56 final of 13 May 2005 on Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society
<https://wcd.coe.int/ViewDoc.jsp?id=849061>

[27] International Working Group on Data Protection in Telecommunications of 10 August 2005 on Comments to the Report of the WGIG *<http://www.itu.int/wsis/docs2/pc3/contributions/misc/iwg-data-protection.pdf>*

[28] WSIS PrepCom3, WSIS-II/PC-3/DT/10-E of 23 September 2005 on Masood Khan, Chair of the Sub-Committee A (Internet Governance): Chapter Three: Internet Governance. Chair's paper
<http://www.itu.int/wsis/docs2/pc3/working/dt-10.pdf>

"Tunis Agenda" from the summit still contains a whole paragraph on the importance of privacy protection:

> *We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users.*

Further attempts by the PSWG to insert more specific language, especially on the importance of being able to use the Internet anonymously, were not successful (the word "privacy" even dropped out of the "Tunis Commitment", the shorter political summit document). Instead, the civil society groups fought against an unexpected development. On 29 September, close to the end of the summit preparations, the Israeli delegation proposed a new paragraph that dealt with terrorist uses of the Internet:

> *We underline the importance of countering the manifestations of terrorism at all its forms in the Internet. In particular, we condemn the use of the internet for purposes of financing of terrorist acts, radicalization towards terrorist acts, recruitment for terrorist acts, and glorification of terrorist acts that may incite further terrorist acts.[29]*

The PSWG and the civil society Human Rights Caucus members present in Geneva issued a response, stressing that "civil society is impressed by the fact that it is possible to use the word 'terrorist' not less than six times in one single sentence."[30] The groups were concerned about the proposal for several reasons. First, there still is no internationally agreed definition of terrorism. Secondly, it was unclear what "manifestations" and "glorification" of terrorism on the Internet would mean. The language therefore could open a door to censorship and infringements on freedom of expression. To make clear how imprecise the paragraph was, the PSWG read it to the governments with a minor change, thus exchanging "Internet" with another public infrastructure:

> *We underline the importance of countering the manifestations of terrorism at all its forms in the streets. In particular, we condemn the use of the streets for purposes of financing of terrorist acts, radicalization towards terrorist acts, recruitment for terrorist acts, and glorification of terrorist acts that may incite further terrorist acts." - Would you really want a paragraph like that in a UN summit declaration on traffic and public transport?[31]*

---

[29] Government of Israel (53bis) of 28 September 2005, Paper distributed at PrepCom3 drafting group on cyber-security <*http://www.itu.int/wsis/docs2/pc3/contributions/sca/Israel-28.doc*>

[30] WSIS Civil Society Privacy and Security Working Group & WSIS Civil Society Human Rights Caucus of 29 September 2005 on Statement in Subcommittee A, morning session, WSIS PrepCom3, Geneva <*http://www.itu.int/wsis/docs2/pc3/contributions/sca/hbf-29.doc*>

[31] Id.

This intervention produced results. The paragraph stayed in the draft document, but was cut down to less than half its length and included references to human rights and other international law:

> *We (…) underline the importance of countering terrorism in all its forms and manifestations on the Internet, while respecting human rights and in compliance with other obligations under international law (…).*

In sum, privacy gained more prominence in the second phase of the summit, though there still is no internationally agreed commitment to protect privacy and personal data by legislation. Furthermore, privacy is still framed within the security and anti-terrorism discourse, thus trumped by the interest of law enforcement.

The civil society groups active at the summit in Tunis once again dissociated themselves from the official summit outcomes and developed a joint document "Much more could have been achieved".[32] The evaluation from the introduction - "minor achievements in the outcomes from WSIS were offset by major shortcomings, with much remaining to be done"[33] - is also valid with regard to privacy:

> *The right to privacy, which is the basis of autonomous personal development and thus at the root of the exertion of many other fundamental human rights, is only mentioned in the Geneva Declaration as part of 'a global culture of cyber-security'. In the Tunis Commitment, it has disappeared, to make room for extensive underlining of security needs, as if privacy were a threat to security, whereas the opposite is true: privacy is an essential requirement for security.[34]*

3. Implementation: The ITU and the "Culture of Cybersecurity"

One of the main issues of the WSIS second phase, follow up and implementation, resulted in establishment of a UN group on the Information Society within the UN's Chief Executives Board for coordination, and a mechanism for stocktaking and implementation under ECOSOC's Commission on Science and Technology for Development.

The Tunis Agenda for the Information Society states that the WSIS implementation mechanism at the international level should be organised taking into account the themes and action lines in the Geneva Plan of Action, and moderated or facilitated by UN agencies when appropriate. It also states that ITU, UNESCO and UNDP should play a leading facilitating role in the implementation of the Geneva Plan of Action and organise meetings for moderators/facilitators of action lines. As for privacy, this

---

[32] "Much more could have been achieved". Civil Society Statement on the World Summit on the Information Society of 18 Dec 2005 <*http://www.worldsummit2005.de/download_en/WSIS-CS-summit-statement-rev1-23-12-2005-en.pdf*>

[33] ibid., 3

[34] ibid., 5

is mentioned under action line *C5: Building confidence and security in the use of ICTs*, with ITU as the responsible UN facilitator.[35]

In line with this, ITU organized a facilitation meeting on WSIS Action Line C5 on 15-16 May 2006.[36] The purpose of the meeting was to discuss the WSIS multi-stakeholder implementation process for the action line. The agenda of the meeting was cybersecurity with limited focus on privacy. The PSWG spoke on one of the panels during the meeting, highlighting the issue of digital privacy and identity management. The presentation argued that with the move towards the so-called "Web 2.0", there is a need for "Privacy and Identity 2.0".[37] Up to now the issue, which is related to the notion of "digital citizenship", has mainly been dealt with in the technical community, without larger public debates or user participation. The presentation met some interest, but as the main subject of the meeting was security, it did not generate much debate nor follow up activity.

ITUs general emphasis on cybersecurity has been underlined several times in the WSIS process. In June 2005, ITU held a high-level WSIS "Thematic Meeting" on cybersecurity, while a similar high-level conference on Privacy and Data Protection never took place in the Summit process. On 17 May 2006, in celebration of the World Telecommunication Day, ITU published the results from a global online opinion survey to assess trust in online transactions and awareness of cybersecurity measures. The theme of the survey - "Promoting Global Cybersecurity - aimed to highlight the serious challenges of ensuring the safety and security of networked information and communication systems.[38] In addition to the announcement of the survey, ITU also launched a new "Cybersecurity Gateway" web portal.[39]

The opinion poll of the survey made it clear that privacy is not an esoteric concern of some human rights fundamentalists. According to the survey, 76 per cent of respondents considered privacy to be an important consideration in the context of the Internet. As to whether privacy was respected, 56 per cent of the respondents said that it was respected to some degree, while 44 per cent felt it was poorly respected.[40] Whether the opinion poll will lead to a stronger focus on privacy by the ITU remains to be seen.

---

[35] ITU: Action Line C5: Building confidence and security in the use of ICTs <*http://www.itu.int/wsis/c5/index.html*>

[36] See the documentation at <*http://www.itu.int/osg/spu/cybersecurity/2006/index.phtml*>.

[37] B de La Chapelle *Digital ientity and pivacy. A user-centric approach for the Trust Framework* (16 May 2006) <*http://www.itu.int/osg/spu/cybersecurity/2006/presentations/de-la-chapelle-digital-identity-16-may-2006.pdf*>

[38] International Telecommunication Union of 17 May 2006 on Promoting Global Cybersecurity. ITU announces results of global survey and launches cybersecurity gateway on World Telecommunication Day 2006 (Press Release) <*http://www.itu.int/newsroom/press_releases/2006/09.html*>.

[39] <*http://www.itu.int/cybersecurity*>

[40] International Telecommunication Union of 17 May 2006 on World Telecommunication Day 2006 : Promoting Global Cybersecurity On-line Survey Results, <*http://www.itu.int/newsroom/wtd/2006/survey/charts/index.asp*>

4. New policy spaces and emerging alliances: The Internet Governance Forum

At the Tunis summit, the governmental delegates had difficulty agreeing on what had become the core issue of the second WSIS phase: Internet Governance; mainly the allocation of domain names and the control of the Internet's core technical resources like the DNS root zone file. In the end, they adopted a proposal that originated from civil society and which mandated the UN secretary-general to convene an Internet Governance Forum (IGF) to further discuss Internet Governance and related matters in a "multilateral, multi-stakeholder, democratic and transparent" way.[41] At the time of writing, the IGF process seems to encourage relatively open modalities compared to previous UN meetings. After two rounds of consultations in Geneva in the first half of 2006, the secretary-general has nominated a Multistakeholder Advisory Committee that served as a program committee. It conducted the first IGF meeting in Athens from 30 October to 2 November 2006.

In the process of IGF consultations, the PSWG submitted two proposals. The first one proposed a "Global Privacy Forum" to be formed as part of the IGF, with the mandate to develop a global legal privacy protection framework:

> *A global privacy framework is a natural consequence of the global Internet. This also echoes paragraph 3 of the Tunis Commitment that aims at strengthening "respect for the rule of law in international as in national affairs". (…) We therefore encourage the conveners of the Internet Governance Forum to work for an international legal framework that ensures the rights to privacy and data protection for all citizens within the Information Society.*

This proposal was supported by several international NGOs, by the International Working Group on Data Protection in Telecommunications (Berlin Group), the Swiss Federal Data Protection Commissioner, and got tabled at an APEC privacy workshop. A supportive proposal was also submitted by the Kuwait Information Technology Society.[42] The PSWG submitted the proposal in an attempt to keep the discussion around legal instruments for privacy protection on the table. As the need for *legal* privacy protection had already been taken off the Tunis summit agenda, this proposal was however dropped off the official IGF agenda as well.

The PSWG also submitted a second proposal, titled "Strengthening the Trust Framework through People-Centred Digital Privacy and Identity".[43] The proposal picked up the WSIS phrases "people-centred [information society]" and "trust framework", and connected them with a reference to current technological

---

[41] World Summit on the Information Society WSIS-05/TUNIS/DOC/6 (rev. 1) of 18 Nov 2005 on Tunis Agenda for the Information Society <*http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf*>

[42] Kuwait Information Technology Society (KITS) of 16-17 February 2006 on Input to the Internet Governance Forum, Geneva, <*http://www.intgovforum.org/contributions/KITS_statement_IGF_-__English.pdf*>

[43] WSIS Civil Society Privacy and Security Working Group: Internet Governance Forum - Theme Proposal, "Strengthening the Trust Framework through People-Centred Digital Privacy and Identity" <*http://www.intgovforum.org/contributions/IGF-Theme-Proposal-People_Centred_Privacy_and_Identity.rtf*>

developments around identity management infrastructures, which are emerging in the context of new social networking software – "Web 2.0".

> *The issue of how participation in an online world changes our personal need to control the expression of personal identity is at the heart of comprehending Internet Governance in the context of a transition to an Information Society. As the online world moves towards "Web 2.0," the concept of digital identity ("Identity 2.0") is evolving and existing identity systems are faltering. New systems are emerging that centre identity around the user, while strengthening privacy. This is an issue that has so far largely been without public participation. We need public deliberation around it precisely because the issue clarifies the benefits as well as the dangers of an online life in a particular way. Citizens and users will trust that the structures of an Information society are fair, just, and democratic only when it is clear in right, in law, and in code that individuals are the owners of all of the forms for the digital expression of themselves.*

The framing was chosen in order to push the issue on the agenda while not arguing for a specific policy to be implemented. It also helped avoid entrenched arguments that for long had dominated discussions between the privacy and the security policy community. Instead, civil society now focused on "emerging issues" of internet governance in a less controversial and more collaborative and open manner. This reflected a general feeling among many WSIS participants. Compared to the summit process from 2003-2005, privacy was now increasingly being mentioned in the IGF process. In the official "synthesis of written contributions and discussions"[44] prepared by the Internet Governance Forum's secretariat in May 2006, privacy was ranked 5th of the top ten suggestions, and it is the first one dealing with human rights aspects, the top four being spam, multilingualism, cybercrime, and cyber-security. In the official summary of the discussions and contributions, the privacy aspects were summarized as follows:

> *On the issue of privacy and data protection several contributions discussed the evolving concept of digital identity. It is predicted that these new technologies will allow a greater degree of public trust once policy deliberation has clarified the benefits and risks of on-line life. Another issue discussed under this category concerned protection of the privacy rights of Internet users and website owners. Several of the contributions brought out the linkage between privacy and data protection and governance and human rights.[45]*

In the summer of 2006, members of the PSWG from the London School of Economics and the University of Bremen submitted two multi-stakeholder workshop

---

[44] Internet Governance Forum Secretariat of May 2006 on Short synthesis of written contributions and discussions *<http://www.intgovforum.org/brief.htm>*

[45] Internet Governance Forum Secretariat: The substantive agenda of the first meeting of the Internet Governance Forum Summary of the discussions and contributions (May 2006) @: *<http://www.intgovforum.org/Summary%20of%20discussions.htm>*

proposals. They in the end were accepted by the IGF advisory group, they took place at the IGF in Athens, and they have had quite an impact on the privacy agenda post WSIS.[46]

One workshop was a follow-up around "Privacy and Identity" in cooperation with the private sector.[47] A number of technology leaders from the private sector have been working on identity management systems in the past few years,[48] and are increasingly implementing privacy-enhancing features in their technical solutions, arguing that it is a key component in the development of trust and the maintenance of consumer relationships. Over the past five years, the number of privacy organizations in the business sector has more than doubled, and corporations are increasingly calling for legal regulation of privacy. In November 2005, Microsoft called for a US privacy law to govern personal information held by the private sector.[49] The same call was repeated in June 2006 by the "Consumer Privacy Legislative Forum", an industry consortium including Microsoft, Oracle, Intel, Hewlett-Packard, Google and others.[50]

The second workshop held at the IGF in Athens was on "Privacy and Development", picking up on the overall "development" theme of the Forum. It tried to address the challenges developing countries face when dealing with the several global instruments of privacy regulation, from the EU directive to binding corporate rules or the NAFTA agreement. It was one of the first attempts at the United Nations policy level to link privacy protection with economic development and the perspective of the poor and the global South.

After both workshops, the participants from international organizations, the corporate sector, and civil society felt the need to continue the discussion. These ideas met with a surprisingly welcome surge of interest, and within 36 hours, the idea for a "dynamic coalition on privacy" to become part of the IGF process gained support from more than forty entities, including Amnesty International, Privacy International, Microsoft, SAP, the Council of Europe, the privacy commissioners of Canada and Greece, and the Government of France. The coalition plans to develop more detailed documents

---

[46] Workshop presentations are available @: <*http://identityproject.lse.ac.uk/igf.htm*>. Audio webcast archives will be made available <*http://www.intgovforum.org*>.

[47] Following a workshop in London in July 2006, Microsoft's National Technology Officer for the UK even suggested a "UN charter for digital identity", see J Fishenden, *A UN charter for digital identity …?* (4 July 2006) <*http://ntouk.com/?view=plink&id=161*>.

[48] Examples are Microsoft's work on an "identity meta-system", the open-source ID-system "Higgins", standards like SAML (Simple Authentication Markup Language), the work of the Liberty Alliance, and recent developments of identity micro-formats like OpenID and MicroID. Much of this work is coordinated through a loose network called "the Identity Gang", see <*http://identitygang.org*>. The EU is funding a network of excellence called "Future of Identity in the Information Society" (FIDIS), see <*http://www.fidis.net*> and a project on "Privacy and Identity in Europe" (PRIME), <*www.prime-project.eu*>.

[49] B Smith, *Protecting consumers and the marketplace: The need for federal privacy legislation* (2005). The author is Senior Vice President, General Counsel and Corporate Secretary of Microsoft.

[50] Consumer Privacy Legislative Forum, *Statement of Support in Principle for Comprehensive Consumer Privacy Legislation* of 20 June 2006 <*http://www.cdt.org/privacy/20060620cplstatement.pdf*>

and some consensus recommendations on internet privacy for the next Internet Governance Forum in the fall of 2007.[51]

These experiences reiterate the need for privacy advocates to be flexible and maneuver through different policy spaces with different proposals and different alliances at the appropriate times. Even though the direct call for global *legal* protection of privacy at WSIS was not immediately heard and was subsequently dropped from the agenda, the issue still has the opportunity to resurface now through the anticipated more specific and technology-centered discussions in the "dynamic coalition". It would not be the first example of this kind of regime-building in global governance; there are prior examples outside the world of IT and privacy of rainbow coalitions, driven by civil society, supported by interested business actors, and with initial support from only a few governments, after some years of intensive work managing to get agreement on a global treaty. The convention for the ban on landmines is probably the most well-known example, but there are more instances that work with a mix of "soft law" and "hard law" instruments.

5. Conclusion

In sum, "privacy" has become a more recognised issue in the global diplomacy around the information society and Internet governance over the last four years. A network of advocacy groups has developed over the years of the summit process, and there is a growing amount of links and issue-based alliances with the official data protection commissioners, the private sector, and some governments and international organizations. As the WSIS example has shown, privacy advocacy groups are much more successful if they work towards roughly the same goals as the private sector, even if coming from different angles. This has repeatedly been the case in the past, e.g. in the U.S. "crypto wars" against the Clinton administrations' plan to install a backdoor in encryption systems.[52]

However, as those past privacy lobbying efforts which were lost have also shown, the notion of privacy still has to struggle with the "security" agenda.[53] Privacy also has still some way to go before it becomes a value that is supported and taken serious by a broad majority of players. To the majority of WSIS governmental delegates, or even civil society groups, privacy remained a marginal issue, abstract in content, and much harder to grasp and advocate than for instance freedom of expression. Privacy as a fundamental human right, deeply affected by the use of technology, is still barely recognized. This was illustrated by the fact that the IGF advisory group chose "cyber-security", and not "privacy", as one of the major themes for the Internet Governance Forum. The challenge remains to make accessible and understandable the fundamental societal values which privacy guards, and to raise this awareness beyond the relatively small community of human rights and privacy advocates. It is a task

---

[51] The "Dynamic Coalition on Privacy" has set up a preliminary online presence at *<http://igf2006.intgovforum.org/wiki/Privacy>*.

[52] S Levy, *Crypto. Secrecy and privacy in the new code war* (2001); W Madsen and D Banisar, *Cryptography and liberty 2000: An international survey of encryption policy* (2000).

[53] A recent example is the 2006 EU directive on mandatory retention of telecommunications traffic data for all EU residents, which was opposed by both industry and civil society, but pushed through by a determined coalition of security and law enforcement interests in the governments. See the article by Judith Rauhofer in this issue.

which might be the most pressing and fundamental challenge for protecting and promoting privacy in the information society.