Internet Freedom, Snowden, and Dubai

Richard Hill

30 September 2013

Congress on Privacy & Surveillance
EPFL
Lausanne, Switzerland

Parts of this presentation are based on Richard Hill, “WCIT: failure or success, impasse or way forward?” International Journal of Law and Information Technology, vol. 21 no 3, p. 313; and on Richard Hill and Shawn Powers, “Cybersecurity and spam: WCIT and the future”, submitted to the 2013 World Cyberspace Cooperation Summit
“In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy.”

Dilma Rousseff, President of Brazil, 24 September 2013 speech at the UN
“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” (emphasis added)

Art. 12, The Universal Declaration of Human Rights
“In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.” (emphasis added)

Art. 29.2, The Universal Declaration of Human Rights
“We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, ...” (emphasis added)

US Declaration of Independence (1776)
“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Amd. 4, US Constitution (art. 4 of Bill of Rights), drafted 1789 approved 1791
“4. Liberty consists of the power to do whatever is not injurious to others; thus the enjoyment of the natural rights of every man has for its limits only those that assure other members of society the enjoyment of those same rights; such limits may be determined only by law.

5. The law has the right to forbid only actions which are injurious to society. Whatever is not forbidden by law may not be prevented, and no one may be constrained to do what it does not prescribe.

6. Law is the expression of the general will; all citizens have the right to concur personally, or through their representatives in its formation; it must be the same for all, whether it protects or punishes. All citizens being equal before it, are equally admissible to all public offices, positions, and employments, according to their capacity, and without other distinction than that of virtues and talents.” (emphasis added)

French Declaration of the Rights of Man and Citizen (1789)
“In the absence of the respect for sovereignty, there is no basis for the relationship among Nations.”

Dilma Rousseff, President of Brazil, 24 September 2013 speech at the UN
Outline

• Basic principles
• Snowden’s allegations
• What happened in Dubai
• A way forward
Snowden’s allegations

• US security agencies conduct widespread surveillance
  – Judicial supervision for US persons
  – No judicial supervision for surveillance abroad
  – Various methods used to defeat encryption
  – US-based companies must cooperate and cannot always disclose the cooperation

• Other nations’ security agencies also conduct widespread surveillance

• Knowledgeable people knew about this, but not all ordinary Internet users knew
Voluntary waiver of data privacy (1/2)

One example (contract agreed by click)

• We use the information that we receive for the services that we offer to you, and to other users such as your friends, our partners, advertisers who purchase publicity on the site, and developers of games, applications and web sites (emphasis added)

➢ So you are the product that they sell
Voluntary waiver of privacy (2/2)

Your information is the product:

• It can be used to target political campaigns
• State security agencies may be able to access it (and build profiles by cross-referencing)
• It can be a very profitable business

Dubai: WCIT-12, revision of the ITRs

The International Telecommunication Regulations (ITRs):

- Establish general principles on the provision and operation of international telecommunication services offered to the public
- Facilitate global interconnection and interoperability
- Underpin harmonious development and efficient operation of technical facilities
- Promote efficiency, usefulness, and availability of international telecommunication services
- Treaty-level provisions are required for international networks and services

The ITRs underpin how we communicate with each other by phone or computer, with voice, video or data, and across the globe.
Some statements about WCIT (1/3)

• [There are proposals related to] regulating peering, termination charges for data traffic, and other internet-related rate issues to, among other things, potentially lower certain internet backbone costs and to capture for domestic coffers some of the value of international VoIP services entering their countries (Gross and Lucarelli, Nov. 2011, Who’sWhoLegal)

• Proposals by [certain states] ... could serve as a justification for countries to engage in Internet censorship in the name of national security (background memo for US Congressional Hearing, May 2012)

• The United Nations is also looking at possible amendments to a telecommunications treaty that could amount to worldwide Internet censorship (Kerr, June 2012, Cnet)
Some statements about WCIT (2/3)

• Ideas that have been floated include ... content-related proposals focused not only on spam and fraud, but also “information security”and online child protection issues, which could lead to increased content control mandates (Center for Democracy and Technology, Mar. 2012, Policy Post)

• Perhaps the most troubling proposals submitted for consideration at WCIT are those which aim to limit the openness of the internet and give national governments greater control over internet content (Hays, Nov. 2012, Digital Liberties)

• Without question, the new treaty did nudge the text further in the direction of impacting privacy and free expression (Llansó, Dec. 2012, blog post, Center for Democracy and Technology)
Some statements about WCIT (3/3)

• Proposals related to security and spam could not hinder the free flow of information, because the ITRs cannot contradict the ITU Constitution

• In Article 33 of ITU’s Constitution, Member States recognize the right of the public to correspond through international telecommunications
  – Most countries already have measures to e.g. protect copyright owners, prevent defamation, etc. Such measures are permitted by Article 34 of the ITU’s Constitution

The provisions in the ITU Constitution are essentially the same as those in the Universal Declaration of Human Rights and in art. 19 of the Covenant on Civil and Political Rights
What is in the 2012 ITRs (1/2)

- **Preamble** *(human rights, right to access)*
- **Article 1:** Purpose and scope *(not content-related, AOA)*
- **Article 2:** Definitions
- **Article 3:** Right to communicate at good technical quality; countries to coordinate their infrastructure *(misuse, CLI, traffic exchange points)*
- **Article 4:** International telecom services to be made available to the public *(roaming transparency, quality and competition)*
- **Article 5:** Priority to be given to emergency communications *(emergency number notification)*
- **Article 6:** Network security
- **Article 7:** Combating spam

Note: these are not the actual titles of the articles.
Items in red and underlined are new compared to the 1988 version
What is in the 2012 ITRs (2/2)

• **Article 8**: Charging and accounting (commercial agreements, encourage investments, competitive wholesale pricing)

• **Article 9**: Suspension of services

• **Article 10**: Dissemination of information (Member States to communicate information to ITU)

• **Article 11**: Energy efficiency, E-waste

• **Article 12**: Accessibility

• **Article 13**: Special arrangements

• **Article 14**: Entry into force; reservations

• **Appendix 1**: Accounting rate system

• **Appendix 2**: Maritime telecommunications

• Some provisions of the old Appendix 3 on service telecommunications were moved to Article 8

Note: these are not the actual titles of the articles. Article 8 was previously art. 6, and so forth. Items in red and underlined are new compared to the 1988 version.
WCIT-12 Resolutions

1. Special measures for landlocked developing countries
2. Globally harmonized national emergency number
3. Fostering an enabling environment for the greater growth of the Internet (controversial)
4. Periodic review of the ITRs
5. International telecommunication service traffic termination and exchange

Note: these are not the actual titles of the Resolutions.

All are new. All old Resolutions, Recommendations, and the Opinion were suppressed.
Article 6 (1/2)
Security and robustness of networks

• Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.
Article 6 (2/2)

• Is subject to:
  – Human rights obligations: “Member States affirm their commitment to implement these Regulations in a manner that respects and upholds their human rights obligations”
  – Article 1: “These Regulations do not address the content-related aspects of telecommunications.”

• Cannot be seen as addressing content
  – It is about measures that do not relate to content
  – Should lead to cooperation to implement best practices that are already prevalent
  – Should make it less likely that some country would (perhaps unwittingly) adopt inappropriate security legislation
WCIT-12 outcome (1/2)

- Did not achieve desired goal, which was full consensus
- Split amongst the membership, resulting in a vote
- Media coverage was partly inaccurate, influenced by misinformation campaign

- Broad agreement: 90% of the treaty is not controversial, 10% was agreed by 62% of Member States present and accredited to sign
- Human rights concerns cited by 55 non-signatories (mostly developed countries)
WCIT Outcome (2/2)

• Hard to predict consequences of split
• Worst case: non-harmonized practices lead to fragmentation
  – Continued unilateral actions, in particular regarding surveillance

Historical note: US surveillance did not start with 9/11, it can be traced back to the occupation of the Philippines in 1898 and various other wartime measures, see Alfred McCoy, “Surveillance Blowback: The Making of the US Surveillance State, 1898-2020” (15 July 2012) http://www.popularresistance.org/surveillance-blowback-the-making-of-the-us-surveillance-state-1898-2020/
“The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. ... differing national and regional laws and practices—such as laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.” (emphasis added)

“The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues ... [see previous slide] Addressing these issues requires the United States to work with all countries— including those in the developing world who face these issues as they build their digital economies and infrastructures— plus international bodies, military allies, and intelligence partners.” (emphasis added)

Way Forward (3/7)

“The United States is leading the way in an international dialogue to achieve greater cooperation among nations to defend against cyber threats. In partnership with like-minded nations and allies across the world, the United States has taken a lead role in international institutions, such as the United Nations, to make cybersecurity an international priority. ... In the U.N. Group of Governmental Experts (GGE) on cybersecurity, the United States is working to build understanding around the applicability of international law to conflict in cyberspace.” (emphasis added)

Cybersecurity Progress after President Obama’s Address (14 July 2010)
“Our pursuit of cybersecurity will not -- I repeat, will not include -- monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans.”

Barack Obama, President of the USA, Remarks by the President on Securing Our Nation’s Cyber Infrastructure (29 May 2009)

Note: Prism started in 2007
Way Forward (5/7)

• All countries agree to implement the ITRs in a non-controversial manner
  – Recognize that the security provision does not relate to content, cannot facilitate censorship, and should favor best practices

• Best practices based on existing human rights obligations
  – Consider also the 13 principles put forward by a large number of civil society organizations at: https://en.necessaryandproportionate.org/text
Way Forward (6/7)

Rough summary of the “necessary and proportionate” principles

• Any limitation to the right to privacy must be prescribed by law.
• Laws should only permit surveillance to achieve an aim that is legitimate in a democratic society
• Surveillance must be limited to what is strictly and demonstrably necessary
• Proportionality must be enforced by an independent judicial authority
Way Forward (7/7)

Rough summary of the “necessary and proportionate” principles

• There should be limited exceptions to user notification of surveillance

• States should be transparent about surveillance

• There should be public oversight
Call for Action

• Those here, and the Swiss government and parliament can lead the way:
  – Revisit the ITRs and accede to them
  – Consider the Necessary and Proportionate Principles
    ➢ In national legislation
    ➢ In international instruments, e.g. new Resolutions
For more information

- [http://www.itu.int/en/wcit-12/Pages/default.aspx](http://www.itu.int/en/wcit-12/Pages/default.aspx)
- [http://www.itu.int/osg/wcit-12/highlights/dec13-14.html](http://www.itu.int/osg/wcit-12/highlights/dec13-14.html)
- [http://ijlit.oxfordjournals.org/content/early/2013/06/10/ijlit.eat008.abstract?keytype=ref&ijkey=otqkCXVOAelJUPy](http://ijlit.oxfordjournals.org/content/early/2013/06/10/ijlit.eat008.abstract?keytype=ref&ijkey=otqkCXVOAelJUPy)
- [https://en.necessaryandproportionate.org/text](https://en.necessaryandproportionate.org/text)
- [http://www.hill-a.ch/wcit](http://www.hill-a.ch/wcit)