Session 7: Internet Freedom and Global Information Society (Friday, 10:45 – 12;15 PM)
Roundtable: Ron Deibert (moderator), Adriane Lapointe, Michele Markoff, Rafal Rohozinski

1. To what extent will an international agreement on cyberspace weaken existing multi stakeholder frameworks that govern the internet? How will civil society's interests be include (or not) in a state-led process of cyberspace governance?
2. What is more important: securing the Internet to preserve public confidence (which extends to policing, commercial viability, and national security), or preservation of openness as a global public good that is in line with the norms of liberal democratic societies? How do we strike that balance appropriately?
3. What are some of the unintended consequences of the Internet Freedom promotion agenda?
   - Can we control the ways in which tools and techniques that are promoted as part of this agenda are used? Do we care?
   - What are the policy risks of funding/supporting Internet freedom NGOs? The Wikileaks/Tor example.
   - How can states promote Internet Freedom without it being seen as a vehicle for narrow national interests?
   - In what ways has the promotion of Internet Freedom caused blowback, or the development of more effective and elaborate Internet control methods and policies (e.g. in Iran and China?)
4. In those areas where there is broad agreement on appropriate infringements to speech online (e.g., Child Porn), what are the best mechanisms (filtering versus?) and processes (oversight?) to follow in order to restrict speech?
5. To what extent do Internet intermediaries and the private sector as a whole contribute to cyber norms?
6. How do the growing liabilities placed on Internet Intermediaries in democratic countries (e.g., on data and traffic retention; geolocation information; lawful access) set norms for acceptable practices that undermine Internet freedom worldwide? What type of oversight should there be on processes of intermediary liability?
7. It would be useful to distinguish between existing norms and the norms we'd like to advocate—we are of course not working in a vacuum. Particularly given the multi-stakeholder nature of the internet, we need clarity, too, about whom we expect to comply with these norms of behavior: citizens/consumers/individuals, and industry as well as governments, will be interested parties when it comes to norms development, and may all be encouraged to adhere to them in some fashion, though that may not be our primary consideration at this workshop. Norms—and their outcomes—will presumably differ at the individual vice national/industry levels (e.g., the consequences of anonymity/lack of authentication).
8. How do norms get promoted/socialized in a multi-stakeholder context?
9. To what extent might the norms characteristic of the open-source community be a useful starting place for discussion?
10. What kind of norm might allow nations to protect life and property from crime associated with social-networking-linked criminal events like flash rioting without compromising—and in addition, without allowing others to reasonably argue that they have compromised—norms associated with freedom of speech/association/access to

information? How does one frame a new norm on this situation so as to distinguish clearly between actions taken to inhibit violent or economic criminal activity and actions taken to inhibit what some other governments define as criminal disruptive speech activity?

11. Tolerance of internet content critical of the government varies from government to government consistent with tolerance for other, non-virtual forms of dissidence or free speech. The current norm is that government policy regarding virtual free speech/freedom of association is consistent with policy on human rights in the non-virtual world. How do we manage cyber norm development in this arena without changes in the underlying value systems of all parties? Does “cyber norm development” inherently equal social change?