MILTON WOLF SEMINAR
VIENNA, AUSTRIA
MARCH 30 – APRIL 1, 2014

THE THIRD MAN THEME REVISITED:
FOREIGN POLICIES OF THE INTERNET IN A TIME OF SURVEILLANCE AND DISCLOSURE

2014 MILTON WOLF SEMINAR COMPENDIUM

MAY 2014
Table of Contents

Introduction .............................................................................................................................................. 1

Panelist Essays .......................................................................................................................................... 3
“A Brief History of a Collaborative Law,” by Sergio Branco ................................................................. 4
“Reflections for the 2014 Milton Wolf Seminar,” by Alison Gillwald ...................................................... 6
“’Ist’ vs. ‘Soll’: the Dark Side of the Internet,” by Richard Hill .............................................................. 9
“Analyzing foreign policies of the Internet: Problems of Legitimacy and Knowledge in Collaborative Lawmaking,” by Wolfgang Schulz .............................................................. 12
“Between the Local and the Global: Notes towards thinking the nature of Internet Policy,” by Nishant Shah .......................................................................................................................................................... 14

About the Milton Wolf Emerging Scholars Program ........................................................................... 17

Emerging Scholar Essays .......................................................................................................................... 18
“To Tame the Digital Frontier,” by Woon (Anthony) Cho ....................................................................... 22
“Refusing to be the Price: Bringing Gender to the Center of the Internet Governance Stage,” by Rosemary Clark ...................................................................................................................................................... 26
“Am I Big Brother’s Keeper?,” by Lee McGuigan .................................................................................. 35
“Walking the Tightrope: Multinational Technology Corporations and Global Internet Governance in the Age of Government Surveillance,” by Ryan Spagnolo ................................................................. 44
“Internet Governance, Technical Standards and the "Tree" Antennas,” by Diego Vicentin ........ 48
“Making Access Visible: Representations of the Internet,” by Willow Williamson ................................. 52

About the Milton Wolf Seminar Series ................................................................................................. 56
Previous Milton Wolf Seminar Topics ..................................................................................................... 57

About the 2014 Milton Wolf Seminar ..................................................................................................... 58
Suggested Further Reading ....................................................................................................................... 59
Final Agenda ............................................................................................................................................. 61
Panelist Bios ........................................................................................................................................... 65
Student Bios ........................................................................................................................................... 78

About the Organizers ............................................................................................................................... 84
The Organizing Team ............................................................................................................................... 85

Acknowledgements ................................................................................................................................. 87
INTRODUCTION

By Amelia Arsenault

Launched in 2001, the Milton Wolf Seminar Series aims to deal with developing issues in diplomacy and journalism—both broadly defined. The 2014 seminar was jointly organized by the Center for Global Communication Studies (CGCS) at the University of Pennsylvania’s Annenberg School for Communication, The American Austrian Foundation (AAF), and the Diplomatic Academy of Vienna (DA). Guests included those working for state and multi-lateral organizations, journalists, activists, academics, and a select group of highly engaged graduate students interested in the seminar themes.

Drawing upon case studies such as Russia, Brazil, China, India, and the United States, participants and presenters explored: The Third Man Theme Revisited: Foreign Policies of the Internet in a Time of Surveillance and Disclosure.

Filmed on location in 1948 in the post-World War II rubble of Vienna, The Third Man highlighted the classic Cold War themes of espionage, surveillance and visibility. Vienna also provided the setting for the 2014 Milton Wolf Seminar, which examined the resurgence of these themes in contemporary international relations and journalism.

As highlighted by the Seminar discussions, the ongoing series of leaks by Edward Snowden provides a stark reminder that new communication technologies also pose new opportunities for surveillance and state power articulation. Conversely, these same technologies also afford old and new media organizations with unprecedented capacities for counter-surveillance and disclosure on a global scale. As states from around the world formulated responses to the American spying program, journalists conveyed these actions to their readers. International condemnation of the US spying program was sharp and swift ranging from calls for UN resolutions on privacy to reform of internet governance institutions. Much to the chagrin of many state actors, press revelations regarding similar surveillance programs by states around the world were equally sharp and swift.

This contemporary media coverage, diplomacy, and debate about the role of the internet are underscored by a series of tensions: between privacy and surveillance; between disclosure and secrecy; and between information sovereignty and global information flows. Rather than looking backward at these events, the 2014 Milton Wolf Seminar looked forward, exploring potential diplomatic, journalistic, and regulatory solutions to evolving issues of surveillance and disclosure,
or what we call foreign policies of the internet. Panelists and participants engaged in two and half days of intense consideration of the current and potential role of the media, diplomats, and activists in facilitating positive outcomes. Discussions focused on how non-Western and Western countries are developing their own internet foreign policy strategies, the role of media and diplomatic actors in translating those strategies, and the implications of these activities for the evolving global Internet.

The 2014 Milton Wolf Compendium aggregates the blog pieces authored by panelists as well as those written by our 2014 Emerging Scholars that reflect on this year’s Seminar themes. These reaction pieces highlight the major debates, conclusions, and lingering questions raised during the seminar.

The panelist essays reprinted in this compendium point toward the multiple challenges and opportunities underlying current and future foreign policies of the internet; Sergio Branco, Director of The Institute for Technology & Society explores the intersection of foreign and domestic internet policy by taking readers through the origin of Brazilian internet law, Marco Civil. Alison Gillwald, director of Research ICT Africa examines the under-representation of African countries in internet governance forums. While Richard Hill, a partner at Hill and Associates and former Secretary for the ITU-T Study Groups, underscores the reasons for US dominance. Wolfgang Schulz, professor at the University of Hamburg focuses on the legal problems that emerge for states involved in multi-stakeholder and participatory attempts at formulating international internet legislation. Nishant Shah, Co-founder and Director-Research at the Centre for Internet and Society, reminds readers that in the face of global cries for more and better internet networks, there are still several areas that need further research, including: the workings of global and local internet policy networks, how computer mediated networks respond to crises, and longitudinal studies of network evolutions.

Each year, the organizers select outstanding postdoctoral fellows, PhD students, and advanced MA candidates currently involved in academic studies related to the seminar themes who received full funding to attend the Seminar as Emerging Scholar delegates. Their essays explore a broad cross-
section of the themes explored during the Milton Wolf Seminar: Colin Agur highlights three dimensions of internet surveillance that warrant further attention: laws, physical design, and user practices. Anthony Cho draws parallels between contemporary problems on the internet and the American Wild Wild West. Rosemary Clark explores the intersection of gender and internet governance, pointing towards ongoing challenges and potential opportunities for empowering women in the information society. Lee McGuigan questions the implications of the evolution of internet of things for individual autonomy and corporate and state power. Robert Ralston focuses on the rhetoric of the internet, outlining how states utilize strategic framing to enhance their ontological security. Ryan Spagnolo investigates the role of corporations in debates about the future of the internet. While Diego Vicentin takes us behind the curtain, exploring the implication of how technical standards are formulated—a little known and understood process—for the future of the global internet. And last but not least, Willow Williamson reminds us that issues of race, class, gender, and religion play critical, if often forgotten, roles in lived experiences online.

We hope you enjoy reading these exciting pieces. More information about the seminar, speakers, agenda, and organizers is included at the close of this document.
A BRIEF HISTORY OF A COLLABORATIVE LAW

By Sergio Branco

I.

In September 2006, when Brazilian model Daniella Cicarelli was video recorded, having intimate moments with her boyfriend in a Spanish beach, she could never imagine she would help engender an unprecedented forum of discussion for Brazilian internet law.

The unauthorized video was a huge success online (and street vendors even sold copies of the video to people who did not have internet access). Soon after the video was uploaded, Cicarelli sued Google and several major Brazilian websites, demanding financial compensation for moral damages and the immediate removal of the video.

After the first decision (not favorable to the plaintiff), Cicarelli got a judicial order from the Court of Appeal in the State of São Paulo requiring the defendants to remove the video from their servers. However, the decision proved difficult to enforce; every time the video was removed someone else soon uploaded it again. For this reason, Cicarelli requested that the entire YouTube site be taken down; and the Court agreed.

For about two days, millions of Brazilians could not access YouTube. Under huge social pressure, the Court retracted its decision and YouTube returned to Brazil. In the wake of the takedown, it was evident that Brazil needed a new law to determine internet principles and to clearly define who was responsible for content uploaded to the net. Many criminal laws were being discussed in Brazil at the time; but it was evident that criminal responsibility should be the ultima ratio, the last resort. Before criminalizing social conduct, people should know their legal rights, obligations, and civil responsibilities. This was the genesis of Marco Civil (the Civil Law for Brazilian Internet).

Because Marco Civil aimed to establish rights and duties for internet users, nothing seemed more reasonable than to produce the text of such law in the internet domain. In 2009, a platform was launched for discussion about internet regulation. Between October 29 and December 17, 2009 any interested person could contribute comments on the following topics: privacy, freedom of expression, right to access, civil responsibility for third party content, net neutrality and governmental data. More than 800 contributions were posted during this period of public consultancy.

After this first phase, the Ministry of Justice drafted the initial version of the proposed law for discussion. After a period of public debate (April 8 – May 30, 2010), the final text was sent to the Brazilian Congress.

II.

April 23rd, 2014 was a historical day for the Brazilian internet. The collaborative draft of a civil law for the internet was approved by both houses of parliament and signed by President Dilma Roussef, officially becoming law 12.965/14.
In general terms, Marco Civil (hereinafter we will refer to the approved law as "Marco Civil") works as a law of principles, outlining the fundamental rights of users and how they are ensured. The law gave importance to different guiding principles of Brazilian internet use (art. 3): guarantees to freedom of expression, communication and manifestation of thought under the Federal Constitution; protection of privacy; protection of personal data; preservation and guarantee of net neutrality; and freedom of internet business models, provided that do not conflict with other principles set out in this law. There were several points of contention.

Net neutrality was a controversial issue during Congressional debates, but it was finally incorporated into the final version of Marco Civil. According to Article 9, whoever is responsible for transmission, switching, or routing has the duty to treat data packets isonomically, irrespective of content, origin and destination, service, terminal, or application.

Civil responsibility was another sensitive subject. An initial suggestion was to adopt a notice and takedown system. Civil society, however, claimed that this would remove the judicial prerogative to decide when content represented a legal infringement and provide an open door to censorship. For this reason, the text was changed to provide that, as a general rule, only judicial commandments might force the removal of third party content from websites.

Finally, data protection became a central concern after Wikileaks and the Snowden case. Although Brazil does not have a specific law for data protection, Marco Civil (Article 3) refers to data protection as a principle to be pursued; the internet user has the inviolable right to transmit and store private internet communications, that can only be impinged upon by court order, as provided by law (Article 7).

Marco Civil will go into effect at the end of June 2014. Although some of its provisions need further legal clarification and expansion (the responsibility for copyright infringement is out of the scope of Marco Civil, for example), the approval of this collaboratively-developed law may represent a new form of public debate and direct democracy. Now that the internet is more than twenty-five years old, naïve times are over. Let’s use our expertise to promote and protect it.
**REFLECTIONS FOR THE 2014 MILTON WOLF SEMINAR**

**By Alison Gillwald, Executive Director, Research ICT Africa**

The work of Research ICT Africa in relation to Internet Governance has sought to understand why—despite the significant resources of multilateral and donor agencies thrown at such endeavors and opportunities created for participation through multistakeholder initiatives—with a few notable exceptions such as Kenya, few African countries participate actively in Internet governance debates. Fewer still are involved agenda setting, decision-making, or seek to engineer Internet governance outcomes to serve their interests, whatever those might be perceived to be. This is despite the rhetoric of dissatisfaction with current Internet governance systems.

From an African perspective, Internet governance requires not only an understanding of the unevenness in access to and use of the Internet, but also of the disparities between developed and developing countries’ abilities to effectively participate in global Internet governance debates. My own intermittent work in this area has sought to identify the political and economic assumptions underpinning the governance of the Internet and specifically behind efforts to make it more democratic, both representative and participatory, through multistakeholderism from an institutional perspective.

African countries appear to be far more comfortable in national sovereign state membership-based organizations, where active participation is restricted to member states—despite limited institutional reforms over the last decade, which have seen parts of civil society and industry able to advise and observe. While most African members remain equally inactive in agenda setting in such institutions they are able to determine outcomes through voting en bloc as the African caucus—often in support of regressive motions with severely negative outcomes for their citizens, particularly the poor.

Despite commitments by many African governments at various global forums to the principle of “an open and free Internet,” in practice, in global member state bodies such as the International telecommunications Unions (ITU) such principles generally are trumped by the interest of their state-owned incumbents or new dominant private players, with whom there is often formal ownership by political parties, national leadership, or straight kickbacks. Such was the case with the African caucus position at the World Conference on International Telecommunications (WCIT) 2012 in Dubai which supported the European operators (ETNA) motion to require over the top (OTT) service to pay network providers with the likely outcome of ending the “free Internet” as we know it and denying millions of Africans the potential offer it offers to free information.

Yet despite these negative outcomes, an African agenda on Internet governance is far from being defined. In a paper written together with Enrico Calandro and Niccolo Zingales we map the multistakeholderism in the system of Internet governance and draw out the largely negative outcomes for Africa. Some of the reasons for this include the absence or nascent nature of the Internet industry and civil society organizations in many African countries. Even where they exist, with the exception of Kenya in sub-Saharan Africa, their exclusion from the delegations of national governments to international meetings is the norm. Even where international meetings are open to non-governmental entities, and participation is permitted independently of formal state
delegations, they tend to take place in venues requiring resources for travel and accommodation, to which civil society organisation seldom have access. This is of course different for industry and large multinational operators particularly, do tend to have a presence in such forums and are often included in government delegations. As a result, civil society organizations are generally unable to advocate at national, regional and inter-governmental levels.

A political economy approach to Internet governance provides insights into why this is so and counters some of the treatment of Internet governance in the literature and practice as primarily a technical management issues as opposed to an issues of public policy. Internet governance organizations, and particularly through multistakeholder approaches adopted as part of reform initiatives to inform them, assumes democratic underpinnings in the national political systems of African member states that are often absent or fragile. By and large, they appear unable to tolerate non-state participation in what is regarded as a strategic resource that requires safeguarding, in the national interest, rather than the public interest. The kind of deliberative democratic engagement that civil society organizations are demanding in terms of reform is highly threatening to fragile states who see civil society as more aligned to international forces and social movements than to their own countries.

Economically, the assumptions of connectivity, not to mention technical expertise, unwitting undermine efforts of inclusion. The latest ICANN President’s Strategy Panel on Multistakeholder Innovation to redesign ICANN and its multistakeholder decision-making processes process is a case in point. Almost exclusively, the solutions proposed to making the ICANN a more transparent and accountable organisation were underpinned by such assumptions--from opening up procurement to crowd sourcing decisions – of affordable access to Internet and technical expertise to contribute to ICANN were assumed. There was one “human” solution that sought ways of getting those currently marginalized from participation to places were they could engage directly to influence outcomes. Despite efforts to broaden the discussion with the inclusion on the panel of Africans (Bitange Ndemo from Kenya and myself) this was primarily the connected world and those with a voice already within the ICANN community and web-based epistemic communities already talking among ourselves.

In the work going forward with the Internet Policy Observatory Project at the Center for Global Communication Studies at Annenberg, RIA intends to undertake a more systematic and comprehensive historical institutional analysis of Internet Governance in order to explain and understand some of these apparent contradictions. It will also attempt a demand side survey of individuals active in Internet governance at any level, to understand the constraints for participation and influence within the system of Internet governance and what opportunities exist to make the system more transparent, accountable and inclusive.

References

**Ist’ vs. “Soll”: the Dark Side of the Internet**

By Richard Hill, Partner, Hill & Associates

The Internet has become a vitally important social infrastructure that profoundly impacts our societies. It has transformed the way we do many things but the benefits promised for all have not been adequately realized. On the contrary, we have seen mass surveillance, abusive use of personal data and their use as a means of social and political control; the monopolization, commodification and monetization of information and knowledge; inequitable flows of finances between poor and rich countries; and erosion of cultural diversity. Many technical, and thus purportedly “neutral,” decisions have in reality led to social injustice as technology architectures, often developed to promote vested interests, increasingly determine social, economic, cultural and political relationships and processes.

Many of the issues outlined above are discussed in the context of what is called “Internet governance.” This is a minor industry, with something like 100 people working in it full-time, attending various meetings around the world.

Why? Why isn’t there a “GSM governance” (Global System for Mobile Communications) industry, even though GSM reaches more than twice as many people, is more economically significant, and is more significant even as a tool for fostering political change?

Because offline law applies online, and some people don’t like this with respect to “the Internet.” In particular, some people think that the meta-rules, that is, the rules for making rules, should be different with respect to the Internet. Some think that technologists should set the rules for Internet, others think that governments should set public policy, others think that all “stakeholders” should work together on an equal footing. This last view in effect gives veto power to private companies, thus protecting incumbents and the status quo.

It is axiomatic that private companies seek to maximize, or at least protect, their profits. Thus it is not surprising that those who favor the status quo are those who are at present profitable. These are primarily US-based companies, supported by some developed-country companies.

It is also axiomatic that states seek to maximize, or at least protect, their power and interests. Thus it is not surprising that the US seeks to maintain the status quo, which enables it to exercise pervasive surveillance and at least a nominal level of control over certain aspects of the Internet. The US is supported by Australia, Canada, Japan, Sweden, UK and several other European countries. It is challenged by the BRICS and most developing countries.

Supporters of the status quo rely on certain narratives to support their position. We will outline, and criticize, those narratives in section (3) below. But first we need to recall how we got to where we are now. It was for two reasons: (1) a design accident and (2) a unilateral assertion of power by the US government.

1. **Design accident**

The Internet was not designed as a public network. Its initial design was intended for a private, closed network. The initial design did not include security (security was supposed to be end-to-end) or billing.
End-to-end security has proven difficult to implement, so the Internet suffers from spam, cybercrime, and pervasive surveillance.

Since there is no detailed billing, the receiver-pays model predominates: users pay flat rate charges. Those who offer services (such as search engines) must derive revenue through indirect means, in particular targeted advertising. Capacity management can be an issue, and entities that have significant market power try to pass their costs along to other entities, leading to calls for network neutrality regulation. (But the real debate should be about whether infrastructure is a natural monopoly and, if so, how it should be provided, with functional separation being perhaps the best solution.)

2. Unilateral assertion of US power

During the early years, management of Internet names and addresses was provided by an individual funded by the US government. As the network grew, it became apparent that a single person could not handle the central coordination function, and that rather more sophisticated procedures and processes would probably have to be developed and implemented to ensure proper coordination.

Consequently, the Internet Society, and other organizations, facilitated a process that resulted in certain recommendations. However, the US government unilaterally rejected those recommendations and proposed instead a different approach, which led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN).

In the approach initially proposed by the United States, its role, as a government, would have been phased out relatively rapidly. But that did not happen and the US, as a government, retained a privileged role. Not surprisingly, this led to criticism from other governments, with explicit discussions of the matter taking place at the World Summit on the Information Society (WSIS) in 2005, and ever since.

3. Narratives that defend the status quo

The first and foremost narrative used to defend the status quo is that it is all about preserving freedom of speech. But it is widely accepted that offline rights apply equally online, so the restrictions on offline freedom of speech allowed under international human rights law apply equally well to online speech. And indeed all countries restrict freedom of speech to some extent, even if the US does restrict it less than most other countries.

If one really wished to promote online freedom of speech, then one would seek to reduce the offline speech restrictions provided for by national and international law. Or, at a minimum, seek to introduce a new international legal provision reducing restrictions at least for online speech. And indeed we have proposed such a provision.1

Another narrative is that it is important to protect “the unique multi-stakeholder model” that has been so successful to date. But the Internet has grown more slowly than has the mobile network, it is becoming increasingly centralized and dominated by powerful quasi-monopolies, and it has been

---

plagued by the same issues for the past 20 years: asymmetric role of the US government compared to other governments, complaints about the financial flows (in particular the relatively higher cost in developing countries), and lack of security (leading to spam, etc.). The multi-stakeholder model has not successful addressed those issues.  

Yet another narrative is that in the “multi-stakeholder model” all players should have equal rights, in particular private companies should participate in decision-making on an “equal footing” with governments. This in effect gives veto power to private companies. How could network neutrality regulations ever be agreed in such a setup?  

A persistent narrative used by the US government is that there should be “freedom to connect.” Note that this is not a “right to connect,” the distinction being that if you cannot afford to connect, then that is not necessarily our problem. So the real goal is to allow more and more people to provide more and more data. That data can then be used, on the one hand, to generate more and more target advertising and thus more and more profit for the dominant players. And it can be used, on the other hand, to conduct more and more pervasive surveillance.  

So, in reality, those narratives are about maintaining the geo-political and geo-economic dominance of the present incumbents, that is, of the US and its powerful private companies.  

For a more detailed exposition and justification of these thoughts, see the cited references.

---


ANALYZING FOREIGN POLICIES OF THE INTERNET: PROBLEMS OF LEGITIMACY AND KNOWLEDGE IN COLLABORATIVE LAWMAKING

By Wolfgang Schulz, Professor, University Professor in Media Law and Public Law including Theoretical Foundations, Faculty of Law at the University of Hamburg

During my latest research on Internet policies and governance I have become more and more interested in problems of lawmaking in times of "multistakeholderism" concerning legitimacy and knowledge. The Brazilian "Marco Civil" project is for two reasons a perfect case of lawmaking to shortly illustrate those problems to you: It attempts to create a comprehensive framework for the Internet as the basic information infrastructure of the knowledge society. And the process of drafting the law has been highly participatory.  

In this regard the Marco Civil process is significant as to how it reconstructs and seeks to change elements of legitimacy at first hand. Legitimacy is key to the acceptance of laws and regulations by those affected including citizens, NGOs, governments, and corporations. Lawmaking and the question of legitimacy is, of course, first and foremost a political matter. In a democracy, the definition of what might be considered a social problem and which regulatory means should be applied to solve it, should be designed as a process of "public reasoning." That challenge can also be tackled by participatory means: Well-designed participatory processes have the ability to provide fora for public deliberation and collaboration. On the other hand, the parliament remains the main actor in the process of lawmaking on national level in my opinion. From the normative perspective of the institutional setting it is the main task of the parliament to convey democratic legitimacy in representative democracies. Notwithstanding the importance of new participatory instruments for citizens, multi-stakeholder forums and other means of preparing legislation in representative democracies, the procedures on national level are still designed in such a way that the decision of the parliament constitutes the transfer of legitimacy.

Secondly the Marco Civil process is remarkable with regards to the production of knowledge. In drafting this kind of internet laws the lawmaker has to anticipate the effects different solutions for a regulatory problem can have in different fields of society, in this case especially as regards free speech or economic innovation. In fact, many of the contributions to the Marco Civil draft law focus on the potential effects that the enactment of the bill might have and therefore provided the cognitive basis for lawmaking. Will a specific form of liability be likely to create chilling effects? What means of circumvention are available? What are the most likely reactions of multi national providers facing regulation? To answers these questions one needs complex Internet specific knowledge.


There is in fact a group of knowledge brokers ready to fill the informational gaps the institutionalized lawmaker - consisting of the parliament and the actors participating in the new processes - may have, and those are lobbyists. Lobbyism is an important factor in the knowledge ecology of modern democracies. However, since not all interests that are present in a society have the same resources to lobby their interests there is an inherent tension with democratic principles where the process of lawmaking would be cognitively dominated by lobbyists (Lessig, 2011; Abeles, 2008). The Marco Civil process also demonstrated that the risk of participatory procedures being “high jacked” by interest groups is not a mere phantasm. There have been hints that many individual remarks on the draft had been made using the IP address space used by an organization thus there is the suspicion of political astroturfing.8

Both insights lead me to the conclusion that the knowledge-eco-system of lawmaking especially in international, multi-stakeholder governance processes has to be further scientifically analyzed both on theoretical as well as on empirical level.

BETWEEN THE LOCAL AND THE GLOBAL: NOTES TOWARDS THINKING THE NATURE OF INTERNET POLICY

By Nishant Shah, Co-founder and Director-Research at the Centre for Internet and Society, Bangalore, India

There is an imagined and perceived gap between the global and the local that informs transnational politics and policy of the Internet. The global relates to the local as simultaneously the site upon which the global can be made manifest as well as the microcosm that supports and strengthens the global visions by providing mutations, adaptations and reengineering of the governance practices. The local is encouraged to connect with the global through a series of outward facing practices and policies, thus producing two separate domains of preservation and change. On the one hand, the local, the organic and the traditional needs to be preserved and made the exotic other of the transnational and the global. On the other hand, the local also needs to be in a state of aspiration, transforming itself in order to belong to the global networks of polity and policy that are deemed as desirable, especially for a development and rights based vision of societies.

While these negotiations and transactions are often fruitful and local, national, and transnational structures and mechanics have been developed to facilitate this flow, this relationship is precarious. There is an implicit recognition that the local and the transnational, dialectically produced, are often opaque categories and empty signifiers. They sustain themselves through unquestioned presumptions of particular attributes that are taken for granted in these interactions. There have been many different metaphors that have been used to understand and explain these complex transfers of knowledge and information, resources and capital, bodies and ideologies. Vectors, flows, disjunctures, and intersections are some of the examples. However, with the rise of the digital technologies (and vocabularies) and especially the internet, the metaphor of the Network, with its distributed nodes, has become one of the most potent explanations of contemporary politics. So seductive and “common-sense” is this idea of living in networked worlds, that it has become an everyday practice to think of the global as a robust, never-ending, all-inclusive network where the local becomes an important node because it enables both connectivity within but also an expansion of the edges, in order to connect to that which is outside the traffic capacities of the network.

Within the “Network Society” paradigm—distinct, for instance, from earlier rubrics of information and open society that have informed existing information and communication policies—we have the opportunity of revisiting and remapping the ways in which local governments and populations function and how they produce the locals which can feed into the discourse of the transnational and the global. The network facilitates some knowledge that is valuable. Networks allow us to map inequity and mal-distribution of resources by offering comparisons between the different nodes. Networks force our attention to the edges, the no-person’s-zone, which is porous but still serves as an osmotic filter that often keeps the underprivileged and the unintelligible outside its fold. Networks as metaphors are valuable because they produce a cartographic vision of the world with multiple boundaries and layers, dealing with big data sets to create patterns that might otherwise be invisible. Networks enable the replication of models that can be further localized and adapted to fit the needs of the context. Networks make the world legible—we write it through the lens of the network, intelligible—we understand it through the language and vocabulary of the network, and accessible—it allows for knowledge and practices to transfer across geographies and times.

At the same time, networks are a vicious form of organisation because they work through the logic of resource maximization, efficiency and optimization, often disallowing voices of dissent that
threaten the consensus making mechanisms of the network. Networks have a self-referential relationship with reality because they produce accounts of reality that can easily stand in for the material and the real. Networks are the new narratives that can operate with existing data sets and produce such rich insights for analysis that we forget to account for that which cannot be captured in the database structures of these data streams. Networks work through a principle of homogeneity and records, thus precluding forms of operation that cannot be easily quantified.

Given this complex nature of networks and the fact that they are emerging as the de facto explanations of not only social and cultural relationships but also economic and political transactions, it might be fruitful to approach the world of policy and politics, the local and the transnational, through the lens of the network. Building a critique of the network while also deploying the network as a way to account for the governmental practices might produce key insights into how the world operates. What does it mean to imagine the world in the image of the internet as a gigantic network? What are the ways in which a networked visualization of policy and governmental processes can help us analyze and understand contemporary politics? What tools can we develop to expose the limitations of a network paradigm and look at more inclusive and sensitive models for public discourse and participation? How do we document events, people and drivers of political change that often get missed out in the networked imagination of transnational politics? These are the kind of questions that the IPO could initiate, building empirical, qualitative and historical research to understand the complex state of policy making and its relationship with enforcement, operationalization and localization.

Given the scope and scale of these questions, there are a few specific directions that can be followed in order to ensure that the research is focused and concentrated rather than vague and generalized:

1. **Bird’s eye views:** The big picture understanding of transnational political and policy networks is still missing from our accounts of contemporary discourse. While global representative networks of multi-stakeholder dialogues have been established, there isn’t enough understanding of how they generate traffic (information, knowledge, data, people, policies) within the network through the different nodes. Producing an annotated and visual network map that looks at the different structural and organizational endeavors and presences, based on available open public data, bolstered by qualitative interviews would be very useful both as a research resource but also an analytic prototype to understand the complex relationships between the various stakeholders involved in processes of political change.

2. **Crisis Mapping:** One of the most important things within Network studies is how the network identifies and resolves crises. Crises are the moment when the internal flaws, the structural weaknesses and the fragile infrastructure become visible. The digital network (like the internet) has specific mechanisms of protecting itself against crises. However, the appearance of a crisis becomes an exciting time to look at the discrepancy between the ambition of the network and its usage. A crisis is generally a symptom that shows the potentials for radical subversion, overthrowing, questioning and the abuse of network designs and visions. Locating ICT related crises through historically and geographically contained focus could similarly reveal the discrepancies of the processes of making policy and orchestrating politics.

3. **Longitudinal Studies:** The network remains strong because it works through a prototype principle. Consequently, no matter how large the network is, it is possible to splice, slice, and separate a small component of the network for deep dive studies. This microcosm offers rich data sets, which can then be applied across the network to yield different results.
Further, working with a different kind of actor—from individual to the collective, from the informal to the institutional—but giving them all equal valency provides a more equal view of the roles, responsibilities and aspirations of the different actors involved in the processes. This kind of a longitudinal study, working on very small case-studies and then applying them to analyze the larger social and political conditions help in understanding the transnational and global processes in a new way.

These research-based inquiries could result in many different outputs based on the key users that they are working with and for. The methods could be hybrid, using existing local and experimental structures, with predefined criteria for rigor and robustness. The research, given its nature, would necessitate in working with existing networks and expanding them, thus building strong and sustainable knowledge networks that can be diverted towards intervention through capacity building and pedagogy directed at the different actors identified within these nodes.
ABOUT THE MILTON WOLF EMERGING SCHOLARS PROGRAM

The Milton Wolf Seminar represents a unique opportunity for distinguished diplomats, academics, and media practitioners to interact with graduate students and other emerging scholars in an intimate and intellectually engaging setting. In order to maximize opportunities for students and emerging scholars and to enrich the discussions, each year, the seminar organizers select eight outstanding PhD students, advanced MA Candidates, emerging scholars or equivalents that are working in areas related to the seminar themes. These delegates were chosen from an elite pool of applicants nominated by their home institutions. With support from the American Austrian Foundation, selected student and emerging scholar delegates received full funding to attend the Seminar.

These distinguished delegates not only participated in the seminar discussions but also served as the seminar blog team. Each delegate authored a reaction piece to the seminar, which was originally published on the CGCS website blog shortly following the seminar.

The 2014 Delegates

The eight distinguished delegates are:

1. Colin Agur, PhD Candidate, Columbia University
2. Woon Anthony Cho, MA Student, The Fletcher School of Law and Diplomacy, Tufts University
3. Rosemary Clark, PhD Candidate, Annenberg School for Communication, University of Pennsylvania
4. Lee McGuigan, PhD Candidate, Annenberg School for Communication, University of Pennsylvania
5. Robert Ralston, MA Student, Virginia Polytechnic Institute and State University
6. Ryan Spagnolo, MA Student, The Fletcher School of Law and Diplomacy, Tufts University
7. Diego Vicentin, PhD Candidate, University of Campinas, UNICAMP, Campinas, Brazil
8. Willow Williamson, PhD Candidate, School of International Service, American University
DISCLOSURE AND ITS DISCONTENTS: PROTECTING PRIVACY IN A TIME OF SURVEILLANCE

By Collin Agur

In the 1825 farce play *Paul Pry*, the title character spies on his neighbors by asking third parties for details of their lives and leaving objects (often umbrellas) behind so he has an excuse to return unannounced. His catch-phrase, “I hope I don’t intrude,” is as contrived as his reasons for monitoring his neighbors. In the years following *Paul Pry*, government efforts to read letters in the post and telegrams sent over the wires eclipsed the threat of a bumbling snoop. Today, in the wake of the Snowden disclosures, these concerns seem quaint. With powerful agencies monitoring our electronic communication, ours is a world of frequent and deep intrusions. Nosy neighbors are the least of our worries.

Surveillance was a recurring theme at this year’s Milton Wolf Seminar, held at the Diplomatic Academy in Vienna. In formal sessions and social events spread over three days, the participants — an international mix of scholars and practitioners — explored how, in a time of increasing concerns about privacy and surveillance, diplomats, international organizations, the private sector, civil society, and the press can influence internet governance. The surveillance disclosures of Edward Snowden figured prominently in discussions about the capacities and intentions of national governments, and about the degree of privacy enjoyed by ordinary citizens.

For the growing number of people whose lives depend on the internet and global telecommunications infrastructure, the Snowden disclosures raise troubling questions about what sort of “reasonable expectation” citizens can have to privacy when government agencies are willing and able to monitor electronic communication and aggregate that information with other personal data. The uncomfortable truths that Snowden exposed force us to rethink what is and is not private. As Monroe E. Price has written, society is a mix of open and closed terrains of speech. In open terrains, discussion is free and uninhibited. In closed terrains, there are limits on speech. Surveillance means that these closed terrains are more open than we expected. This has prompted attention from scholars and activists who want clear limits on government surveillance.

One particularly illuminating presentation at the Milton Wolf Seminar focused on the evolution of “privacy panics” from the 19th century — when citizens worried that British authorities were reading their mail and telegrams — to the present day. The historical lessons are worrying: consumers want convenience above all else, and many are willing to accept surveillance so long as it does not interfere with the ease of communication. In the 19th century, despite revelations of postal mail surveillance, more people sent more letters through the post. Today, polls show that many people are concerned about surveillance of telephone and Internet usage. At the same time, these tools offer enormous convenience and few users are willing to invest the time and effort necessary to encrypt their communications. If history is a guide, current outrage about mass surveillance will wane and many users will accept a loss of privacy in exchange for convenience.

---


10 See the extensive set of articles at the Electronic Frontier Foundation. Available at: [https://www.eff.org/nsa-spying](https://www.eff.org/nsa-spying). Also see *The Guardian*’s collection of articles. Available at: [http://www.theguardian.com/world/the-nsa-files](http://www.theguardian.com/world/the-nsa-files).
Given the aggregating power of current and emerging surveillance technology, we should be worried. When we give up aspects of our privacy, we rarely get that privacy back. Of course, it is not just governments who have access to our data. When we sign up for a Gmail account, we allow Google to read messages we send as well as messages sent to us by others. Google is able to read those messages, regardless of whether those message senders provide their consent. For those concerned about Google storing and studying their email contents in conjunction with other user information (for example, web searches performed while the user is signed into a Gmail account), the answer is straightforward: use another email service. But we do not always have that choice. Many institutions have outsourced their email to Google, meaning that the internal correspondence of many universities, including the one where I am pursuing my PhD, is stored on servers in Mountain View, California. When an outsider emails a faculty member or student at Columbia, s/he may be unaware that the university's email and all messages (incoming or outgoing) are subject to Google terms of use. Here we see the challenge of web-based services that offer us benefits in exchange for using our data. As one Milton Wolf Seminar participant stated: "We want the convenience of these services, but we also want to put the genie back in the bottle. How do we do both?"

This year's seminar made a point of focusing on the future, on solutions for better governance of global communication networks. I see three aspects of surveillance that deserve our attention: laws, design, and practices.

The first is law. At the domestic level, there are major technical challenges. Surveillance technology is inescapably global; and the United States plays an outsize role. When surveillance activities cross borders, there is only so much that law enforcement can do. Another challenge is judicial. There are prior cases that touch on metadata. In the United States, for example, *Smith v. Maryland* (1979) set the precedent that telephone users cannot expect that the numbers they dial will remain private. Judges, however, have interpreted that case in different ways; and it is unclear how the Supreme Court would rule in a case on telephone metadata. While the NSA has sought to portray its actions as targeted efforts that isolate specific users, experts have suggested that the collection of “metadata” is a form of mass surveillance. In the US, there is a long history of government agencies finding ways around privacy laws and attempting to downplay the scale and significance of the data being collected. Internationally, the challenges are even greater than at the domestic

---


level. Given the power disparity between the surveillance-haves and have-nots and the different attitudes national governments have toward binding treaties, it will be difficult to craft a meaningful and enforceable set of laws governing surveillance technology.

A second aspect of surveillance is design. It is important to promote laws that clarify what surveillance agencies can and cannot do with data and clearly outline the relationship between these agencies and internet and telecommunications firms. Good laws, however, are not enough. If communication networks are designed in such a way that it is possible for law enforcement and spy agencies to collect, store and use data-- they will do so. In recent years, advocates of “Privacy by Design” have developed a core set of seven foundational principles for prioritizing privacy in the design of large technical systems:

1. Make design proactive not reactive and preventative not remedial;
2. Make privacy the default setting;
3. Embed privacy into design;
4. Avoid zero-sum dichotomies such as “privacy vs. security;
5. Emphasize end-to-end security;
6. Provide transparency on the design process; and
7. Keep design user-centric.14

While these principles are laudable, they often exist in tension with the business models of network enterprises, whose profitability stems from their ability to aggregate users, services, and data. Privacy-by-design thus faces a central challenge—many of the institutions we would most like to see implement these principles have a financial disincentive to do so.

While law and design are important, a third aspect of surveillance—practices—ultimately determine the degree of privacy enjoyed by users. At several points during the Milton Wolf Seminar sessions, participants highlighted the ability of major players (especially internet and telephone service providers) to pursue practices that privilege users over mass surveillance. To be fair, major players face a delicate balancing act. Their business model depends on the trust of millions of users and support from government officials. In the months since the Snowden disclosures, big tech firms have struggled to answer criticisms regarding their complicity with surveillance programs.15 The question for internet and telephone service providers and social media giants is: How can they develop practices that strike a balance between national security and individual privacy? A large part of the answer involves empowering users to understand how their data is used and how to encrypt their communications.


In all three of these aspects of surveillance—law, design and practice—the mobile telephone should receive the greatest attention. The telephone has a long history as a tool of surveillance. Today, it is a more important tool than ever. A telephone is no longer just a fixed-line medium of communication. For a large and growing number of users, it is a mobile device that conveniently aggregates several different (and previously separate) forms of data. This data aggregation function—which users find so convenient—also allows institutions to track users’ location, monitor their phone usage, and access content on devices. As we think about the changing physics of search and seizure, the behavior of government institutions at home and abroad, and the evolving set of “reasonable expectations” that pertain to contemporary privacy, the telephone should have a significant place in our thinking.

In each of these aspects of privacy, good journalistic reporting is crucial. As more than one participant in Vienna pointed out, news organizations should not be intimidated by government requests to circumscribe coverage of surveillance issues. The existence of “honorable secrecy” between government officials and journalists does a disservice to democracy and to the rights of citizens. In the face of government pressure, news organizations need to develop and encourage best practices in the protection of data and sources.

As we think about surveillance in a changing technological context, informed and vigilant users are perhaps the actors who can make the greatest difference. In our communications laws and treaties, there is an implicit social contract: we accede power to the state and large corporations in exchange for the implicit promise that these institutions will respect our private lives. The surveillance we are learning about today is extensive, sophisticated, and unclear in its legality. By understanding terms of service and taking steps to protect correspondence and other data, we can have some control over how this information is used.

About the Author

Colin Agur is a PhD candidate in Communications at Columbia University’s Graduate School of Journalism. His dissertation focuses on cultural and sociological aspects of mobile phone use in India. His research involves examination of policy documents (1991-present), interviews of policymakers, telecom executives and users, and observation of mobile phone use across India.

At Columbia, he developed and taught a course (“Mobile Revolutions: Markets, Politics, Journalism”) that explored contemporary issues related to the mobile phone.

Since 2011, he has been a Visiting Fellow at Yale Law School’s Information Society Project. His work there has focused on telephone surveillance and the Fourth Amendment. Twitter: @colinagur
TO TAME THE DIGITAL FRONTIER

By Woon (Anthony) Cho

Due to the generous support of the American Austrian Foundation; the Diplomatic Academy, Vienna; and the Annenberg School of Communication at the University of Pennsylvania, scholars from all over the world gathered in Vienna for the 2014 Milton Wolf Seminar. Between schnitzels and Stephansplatz, the seminar theme, Foreign Policies of the Internet in a Time of Surveillance and Disclosure, took center stage. Though we were physically in Vienna, our discussions passed through various sectors and around the world ranging from national cybersecurity threats, China’s growth in internet search, and the way that the internet is changing Africa as we know it. As for me, I am interested in foreign policy and cyberspace; my research examines the cyber-offensive of North Korea. However, I realized that in order to keep up with the breadth and scope of the seminar, I had to take a step back and zoom out from my academic microcosm. From afar, all the wires, devices, and users formed a hazy picture. As the dust settled from our passionate discussions, this picture became clearer.

We now understand WWW to mean World Wide Web. About a century ago, it meant something completely different: the Wild Wild West. The taming of the American frontier encapsulates many of the issues that the internet faces today. Historically, the movement westward represented a new opportunity for many people. They left the urbanizing East for an alternative lifestyle earned through their own sweat and tears. The West was more than a place—it was an ideal. However, beneath the rhetoric, westward expansion was largely profit-driven. Major corporations and governments subsidized and encouraged western migration to fill a market need, whether it was for furs and food, gold, or oil. Because of its profit-driven nature, abuse of power was also quite common. Not only did the corporations and governments control the westward movement, the profiteers that turned west and entrenched themselves became the de facto authorities. Law enforcement and formal governance were geographically distant and behind the times. As new power structures were formed in the absence of a clearly defined civil-legal space, more and more abuses followed, such as the birth of American opium dens. How then, did justice come to the West? Enter the vigilante cowboy heroes like Wyatt Earp: a hero for the common man. Chaos was the only law in the West and those who sought justice had to find it themselves.

Now, replace the western plains with the cyber-plane and we have a digital frontier on our hands. As I will argue below, the internet is also profit-driven, characterized by abuses of power and efforts at vigilante justice for the common man.

The internet is revolutionary. With more and more people and things connecting to the web, the internet is bringing about whole scale societal change. It has been so beneficial to society that
significant parts of the UN consider access to the internet to be a human right. In education, open source course materials have made tertiary education material available for anyone with a connection. In commerce, data can be shared between firms and their clients with unprecedented ease. The entertainment factor of the internet hardly requires explanation. According to a 2014 Pew research study, 90% of internet users said that the internet has been good for them personally, and 76% of internet users say the internet is good for society as a whole. For me personally, I enjoy the news, last night's TV shows, and amazon's recommended readings lists. Unequivocally, the internet has changed the way we live. Much like the West, the internet is not only a place, but also an ideal. An ideal we all seem to embrace.

However, we cannot ignore the fact that the majority of the internet is profit driven. Both Google and Facebook, the two most trafficked websites on the internet, are private for-profit firms, with a market cap worth of $233 billion and $58 billion respectively. In China, Baidu and Alibaba are also experiencing unprecedented profits, with Baidu CEO Robin Li now worth over $12 billion and Alibaba soon to make one of the largest Wall Street IPO debuts in history. Even in the altruistic realm of education, for profit degree mills have latched on to open source education. The Apollo Group, which runs 4 online, for-profit universities, is worth $3.6 billion. In comparison, my own school (Tufts University) has an endowment of $2 billion. Not only are these web platforms generating a tidy sum; they are also investing in their vision for the future of the internet. The companies that control our connectivity—the telecom and cable companies—have also generated profits in excess of hundreds of billions of dollars. Just as westward migration was shaped by the pursuit of money and profits, so too is our journey to and on the net.

These major companies are taking steps to ensure that their profits and revenues increase. Indeed, we must ask if we could call them good free-market companies if they didn’t seek to enhance their competitive advantage. Unfortunately, this competitive advantage is currently costing consumers their privacy and intellectual property rights. Smaller corporations have not been spared, as acquisitions and patent wars abound. Two major issues regarding public power dynamics seem to be:

1. The failure of multi-stakeholder governance, and
2. Citizen surveillance.

The myth of multi-stakeholder governance was a big topic at the Milton Wolf Seminar. There seemed to be a consensus that multi-stakeholder internet governance is failing because internet “stakeholders” do not accurately represent internet users. Those participating under the umbrella of multi-stakeholder governance do not reflect the public interest, and therefore have no civil accountability. The current system of internet governance is shaped by systemic abuses of power by governments and corporations seeking to further their own interests. The Edward Snowden leaks were perhaps the most discussed example of these power dynamics. Government surveillance is not only an issue in the United States, but also notably in China and Russia. There have also been cases of corporate surveillance. Governments and watchdogs have accused Google of having a monopoly on consumer data all across the world. In accusation and counter-accusation, the fight between Google and the NSA is at a stage where the common user is not involved; they are bystanders. These examples of corporate and government surveillance represent an inherent abuse of citizen data and the pursuit of financial or strategic gains.
With seemingly no one on the side of public good, private individuals and organizations have risen up against these perceived injustices. Echoing the vigilante heroes of American Westerns, online watchdog communities and active technocrats have mobilized for the public good. Even bigger companies such as Netflix and Amazon have also joined the cause. Aside from the high profile cases of Edward Snowden and Bradley Manning, vigilante groups have grown in number and force. Against financial injustices and regulations, the hacker collective Anonymous mobilized Operation Payback to make their presence known to financial elites. Even in China, the netizen population is fighting corruption to a certain degree of effectiveness. The common theme in countries around the world is the dispensing of cyber vigilante justice. Unfortunately, these movements alone have not galvanized major changes to the status quo. In fact, many corporations have started to push back. However, what is important here is that there is a widely held desire for justice, order, and civil governance on the internet. Though these vigilantes may be heroes to the common user, they cannot effect change themselves. The actual establishment of representative and accountable justice, order, and civil governance on the internet is needed.

If this comparative diagnosis of the Wild Wild West to the World Wide Web is to be effective, there must be a common prescription, a common solution that can be gleaned from this comparison. To that end, it is important now to analyze how the West was won and if any comparable methods exist for winning the web.

There are many claims to how the West was tamed. I believe the most transformative revolution was in the deployment of transit and communication systems—think the Pony Express and the transcontinental railways. More critically, the accessibility, reliability, and speed of transit and communication brought governance and accountability westwards. People and information moved quicker and there was no longer a sharp divide between the East and the West. With an increased flow of people and information, civil governance in the West increased, supported by a more mobile enforcement structure based in Washington D.C. So, what can improve the accessibility, reliability, and speed of the internet? And how can it improve civil governance? The following are my humble suggestions:

**Accessibility – Connecting more users to the internet**

By decreasing the cost of connectivity, the number of internet users will increase. In turn, more users will inevitably lead to an increase in the number of responsible stakeholders. I believe that the internet is still missing a critical mass of users, especially residents of the global south, who can and should be incorporated into and represented within systems of internet governance. By increasing the overall number of users, especially among older and disenfranchised populations, the number of stakeholders will rise. The issue of law and order in the internet will come to the forefront of societal discussions in a non-sensationalized manner if a broader base of people is invested in the internet.

**Reliability – Ensuring connectivity for users**

By increasing the number of stakeholders online, the number of services and service providers can increase. Opening up to international competition can be helpful in regulating domestic monopolies as well. There is a reason why many countries have their own version of Facebook and Google. Moreover, considering the right to connect as an international human right may give people confidence to see the internet as more than a strictly informational and commercial space. By
increasing the appeal of the internet and its reliability as a medium, a broader base of stakeholders can be achieved.

**Speed – Deregulate bandwidth restrictions for users and corporations**

Expanding consumer access to reliable and affordable broadband connections allows users to connect more often and to participate in a broader array of online activities. This is also a neutral technological goal that is based on collaborations between the government, the private sector, and individuals. Having a common goal in sight can foster teamwork. Also, ISP meters and artificial limitations on data, especially abroad, should be eliminated. Citizens cannot become stakeholders if they are limited to 200 megabytes a month. This can help create an international standard for internet usage and subject ISPs to globalized competition when a select few companies dominate a domestic market.

In conclusion, increasing users (and thereby stakeholders) via increased and more reliable connectivity holds the potential to improve internet governance. In a sense, the Wild Wild West both suggests reasons for hope and a cautionary tale for our digital frontier. Even after the American frontier was tamed, huge problems—including monopolies over natural resources like oil and poor qualities of life—remained. However, expanding governance institutions to the West was no small achievement. It made the West a safer and more prosperous environment for settlers. Likewise, this analytical framework only sheds light on the current issues at hand. The issues of the future will be different and our solutions must adapt accordingly. For me personally, this macro-level view of the web serves as a jumping off point for further academic research. Now, back in my microcosm, I can connect the dots that were outside of my vision before. At the 2014 Milton Wolf Seminar, everything is connected if you look at the broader picture: Don’t only consider what you can see.

**About the Author**

**Anthony (Woon) Cho** is a M.A. student at The Fletcher School of Law and Diplomacy with a focus on international negotiation and conflict resolution in the East Asia region and current serves as a staff editor for The Fletcher Forum. His academic interests include public and private security, cyberspace relations, and U.S.-East Asia Relations. His recent research analyzed the cyber-attack strategies of North Korea and its implications for future negotiations. Prior to coming to The Fletcher School, Anthony received a Fulbright Grant to South Korea where he stayed for two years. He received his B.A. in International Studies at the University of North Carolina – Chapel Hill.
REFUSING TO BE THE PRICE: BRINGING GENDER TO THE CENTER OF THE INTERNET GOVERNANCE STAGE

By Rosemary Clark

MARTINS
Oh, Anna, why do we always have to...

CLOSE SHOT - ANNA
Looking ahead of her. She tears her passport in two. Martins enters from CR and leans on bar in b.g.

MARTINS
...quarrel?

ANNA
If you want to sell your service, I'm not willing to be the price...

- The Third Man screenplay, Graham Greene (1949)

Anna Schmidt, played by Alida Valli, is one of two credited female roles and the only major female character in Carol Reed’s and Graham Greene’s 1949 film noir, The Third Man. This made the film an especially poignant frame of reference for myself and for fellow feminists contemplating internet governance (IG) at the 2014 Milton Wolf Seminar in Vienna, organized under the film-inspired title, “The Third Man Theme Revisited: Foreign Policies of the Internet in a Time of Surveillance and Disclosure.”

The film takes place in post-World War II Vienna and tells the story of Holly Martins, an out-of-work, pulp Western, writer who travels from America to Austria, where his friend, Harry Lime, has promised him employment. Upon arriving in Vienna, however, Martins discovers that Lime was killed after being struck by a car, leaving behind his grieving girlfriend, Anna, along with a cast of suspicious associates, who soon become suspects in Martins’ unofficial investigation into what he believes to be Lime’s murder. Anna is quickly ensnared in the male-dominated web of characters spiraling outward from the center of Lime’s illicit and shadowy life on the Viennese black market. Only, unlike Lime’s coconspirators, Anna is left wholly in the dark, unaware of his exploits, his true whereabouts, and his colleagues’ intentions and involvement in his sudden death. Anna’s blind ignorance leaves her as little more than a pawn surrounded and manipulated by men who play powerful roles in official and unofficial careers, spaces, and marketplaces. Her apartment becomes a crime scene; the international police confiscates her fake Austrian passport (which Lime forged for her); her legal status hangs in the balance as she is threatened with deportation; and her wellbeing becomes a bargaining chip between Martins, who claims to love her, and the international police, who are aware of only her striking beauty and counterfeit papers. In other words, following Lime’s
death, which we ultimately discover was not murder but a staged disappearance, this network of dubious men, largely unknown to Anna, strip whatever agency she once possessed and appropriate her citizenship and personhood as tools for their own purposes. Not once do these men, even those who care for her, stop to ask Anna what she wants or how she views the complexities surrounding Lime’s disappearance, despite the fact that she played a key role in his life. Instead, they each assume that their vision of how to handle Anna and her involvement in the case is best; they unconsciously universalize their perspective, and assume without a thought that they can speak for her. Nowhere is this practice of the men's privilege over Anna more clearly demonstrated than toward the end of the film, when, unbeknownst to her, Martins agrees to help the international police find Lime on the condition that they return Anna’s passport and release her. Anna, sitting on a train that would bring her to freedom, spies Martins near the platform, realizes that he must have struck a deal with the police, and confronts him, never having wanted to aid in Lime’s capture. It is here that Anna begins to reclaim control. “If you want to sell your service, I’m not willing to be the price,” she retorts, as she rips her passport in half and the train leaves the station with all of her belongings. She will no longer allow herself to be sacrificed or spoken for so that the men acting as puppeteers looming over her personal life might more easily get what they want.

In the final scene, suspense builds as Anna slowly walks toward Martins, and, effectively, the viewer, who wait for her at the end of a tree-lined road. Every romantic film convention would have Anna finish her walk in Martins’ arms, happy to be relieved of the wicked ways of her former beau. Only, after approximately 40 seconds of silently closing the distance between them, she continues to walk past Martins, to the edge of the frame, off screen, and out of sight. She has torn up her official ties to the state, renounced most of her material possessions, defied our and likely Martins’ conventional understanding of how women behave, and, at last, removed herself from the tangles of Lime’s nefarious web. But what happens now for Anna? Can she ever actually escape the official and unofficial structures of power that have ruled her life up until this point? Is there power for Anna in renouncing structures of control, or is her refusal to play her part within those structures also an abdication of formal agency? Can her defiance be one method of changing the male-dominated system from within, or does her empowerment depend upon the creation of a different system altogether?

A Feminist Revisits The Third Man theme

I indulge in this female-centric synopsis of The Third Man because I see a powerful metaphor in the film and its choice as a unifying theme at this year’s Milton Wolf Seminar for the intersection of internet governance and gender. I believe the questions Anna leaves for viewers to contemplate can also be asked of women’s involvement in internet governance. As my fellow Emerging Scholar and colleague, Lee McGuigan, eloquently demonstrated during the seminar’s concluding session, the film’s questionable yet powerful cast of characters and their wildly diverse walks of life parallel the variety of stakeholders and motivations at play in the complicated world of internet governance. Yet, as we realized in our discussion on possible improvements to the seminar, a whole group of key players is often overlooked by stakeholders at the IG table and by people like us at the seminar, who attempt to turn a critical eye on the table and those sitting at it, and this neglected group just so happens to constitute half the world’s population—women.

Like Anna, women are positioned at the periphery of male-dominated information society networks. Female underrepresentation in science and technology, politics, and government leads to their underrepresentation in both IG groups and discourse. Women are consistently outnumbered
by large margins and stifled at IG-related meetings, where panelists and moderators are typically male and, consequently, not attuned to the ways in which the big headline issues of internet governance—access, security, content, traceability, privacy, and representation—intersect with gender.

For current and future female users, the internet is a crucial resource because it offers a space for assembling around and accessing information about women’s rights. However, in many developing nations, women’s access is limited not just by infrastructural weaknesses, but also by cultural norms regarding appropriate behavior for women. The internet can also pose significant dangers for female users. Violence against women has gone digital; abusers can stalk and harass their victims through social media and even post compromising photos or videos of their victims without their consent, raising questions about the permanency and traceability of harmful internet content, as seen in the recent “revenge porn” surge. Female journalists, bloggers, and activists whose writing challenges the status quo of male privilege or demands the expansion of women’s rights often face death and rape threats, mediated through social networking platforms like Twitter. While these issues certainly echo the core questions surrounding internet governance, they are, at the same time, unique to women’s gendered experiences online. As long as women and the topic of gender equality are not adequately represented in IG fora, the very specific concerns born out of the intersection between internet governance and gender are left off the table, out of the discourse, and, consequently, out of policy.

Here, I would like to trace a brief history of how various organizations have integrated the topic of gender equality into the discourse surrounding internet governance. As will soon become clear, no proposed strategy for incorporating gender analyses into discussion frameworks or for increasing women’s participation has been completely successful. Nonetheless, stakeholders and organizers can learn from past efforts, if only to ensure that women’s voices will not be the price paid for streamlining approaches to internet governance moving forward.

**Tracing a Gendered History of Internet Governance**

The recorded history of the struggle for gender equality at various internet governance fora, much like the representation of women at these meetings, is spotty, scattered, and lacking uniformity. A Google search yields a handful of relevant organizational websites and female bloggers reflecting on their experience of being one of the few women participants to shoulder the responsibility of representing their gender at IG meetings. Most academic writing on gender and internet governance has not been taken up by scholars focused on internet governance models. Understanding the successes and failures of past efforts, however, is a necessary first step in effectively integrating gender into internet governance discourse. The gendered history that I trace here is likely incomplete and cursory. For me, this represents the very beginning stages of my own gender analysis of internet governance, and I look forward to suggestions that might fill the gaps in

---


17 The following organizations’ websites offer great resources for researchers interested in the relationship between gender and internet governance: GenderIT.org, APC.org, EROTICS.APC.org, Diplomacy.edu, ISISwomen.org, Digital Divide.net.
Regardless, what follows is hopefully a helpful preliminary etching of the trajectory of feminist activism in the playing field of internet governance.

Gender intersected with internet governance for the first time on the international stage at the United Nations’ 1995 Fourth World Conference on Women in Beijing. Over the course of the 11-day conference, women’s rights and media activists successfully fought for the inclusion of a provision concerning women’s access to ICTs in the Beijing Platform for Action (BPfA), the conference’s major outcome. The fact that activists had to rally together to evidence the need for a gendered analysis of ICTs exposed a twofold issue: 1) digital media and communication issues were, as they largely remain today, at the margins of feminist agendas around the globe; and 2) ICTs and related policies were, as again, they often are today, viewed through a gender-blind lens. The activists gathered in Beijing argued that women’s lack of access to ICTs was both a symptom and a cause of gender inequality, especially as contemporary life became increasingly dependent on communication technologies. Their remarkably forward-looking provision, known as “Section J,” called on all governments and media organizations to “increase the participation and access of women to expression and decision-making in and through media and new technologies of communication.” In 1995, only 3% of online users had ever signed on to the World Wide Web; yet, Section J prophetically highlighted two issues now central to any internet governance debate: access and decision-making.

In 2000, the UN General Assembly conducted a five-year review of the BPfA (Beijing+5), and identified ICTs as one major new issue that needed to be addressed in relation to gender equality. The World Summit on the Information Society (WSIS), to be convened in two phases in 2003 (Geneva) and 2005 (Tunis), offered an opportunity to create policies concerning gender equality and twenty-first century communication technologies, policies that reaffirmed women’s rights as framed in the BPfA. In July 2002, during the Africa regional WSIS preparatory committee meeting, 12 gender-focused organizations joined forces to form the WSIS Gender Caucus. This multi-stakeholder group comprised of women and men from the private sector, government agencies, non-governmental organizations (NGOs), and civil society was charged with ensuring that gender equality was included in the WSIS process and outcome documents. A second gender-focused working group was created at the first WSIS preparatory meeting one year later in Geneva, when NGOs working in the area of gender and ICTs voiced a need for a separate but parallel committee to better represent non-governmental and civil society organizations in the WSIS process. The WSIS NGO Gender Strategies Working Group (GSWG) was thus formed as part of the Civil Society Coordinating Group (CSCG). Together with the Gender Caucus, the GSWG worked under nearly impossible deadlines to ensure the mainstreaming of gender issues into the CSCG’s lobbying attempts and formal feedback reports to the official summit. Their advocacy was consensus-driven and included input from organizations and individuals who could not be physically present in Geneva, but could contribute via email listservs and websites.

---

18 My hope is that this blog post will be the first iteration of a much more in-depth look at the intersection of gender and internet governance. Please do not hesitate to contact me with questions and suggestions at rclark@asc.upenn.edu.

By the second preparatory meeting in February 2003, this network of gender activists had conducted several outreach campaigns to educate relevant organizations and activists about the WSIS process so that women might more easily access IG discourse. Most significantly, they had created a core document of gendered recommendations entitled, "7 Musts: Priority Issues for Gender Equality in the WSIS Process." The "7 musts" contextualized the WSIS Preparatory Committees’ recommendations within the gender-focused Beijing Platform for Action and argued for the need to incorporate a consideration for gender equality in the WSIS Declaration of Principles. Importantly, the language used to present the “7 musts” was constructed with non-technical audiences in mind, true to the feminist value of universal access. However, by the third and final Preparatory Committee Meeting, the Gender Caucus and the GSWG found that their demands had fallen on deaf ears. The draft of the Declaration of Principles excluded the topic of gender equality in its consideration of ICTS. In July 2003, Canadian representatives had, with apparent success, proposed that a paragraph on gender equality be included in the Declaration; but by the final preparatory meeting in September, the paragraph had disappeared. The conventions structuring the WSIS process failed gender activists working with the CSCG. While the WSIS claims to be a multi-stakeholder forum, it, like many such fora, privileges governments and corporations (which are dominated by men) over civil society representatives.

The Gender Caucus and GSWG spent months on the periphery reacting to drafted principles from the more central government and corporate interests with little opportunity for proactive efforts. Consequently, their priorities were viewed as tangential and cast aside. Stifled and frustrated by the WSIS process, GSWG members chose to resort to traditional feminist protest tactics and disrupt the official space of the summit.

GSWG members entered one of the final negotiating sessions wearing black t-shirts, on the front of which was printed, “Draft WSIS Declaration has a missing paragraph,” and, on the back, surprised WSIS delegates found missing paragraph 11a:

A focus on the gender dimensions of ICTs is essential not only for preventing an adverse impact of the digital revolution on gender equality or the perpetuation of existing inequalities and discrimination, but also for enhancing women’s equitable access to the benefits of ICTs and to ensure that they can become a central tool for the empowerment of women and the promotion of gender equality. Policies, programs, and projects need to ensure that gender differences and inequality in the access to and use of ICTs are identified and fully addressed so that such technologies actively promote gender equality and ensure that gender-based disadvantages are not created or perpetuated.

A paragraph on gender equality was eventually adopted into the WSIS Declaration, but, unfortunately, with weaker language than that used in the Canadian proposal. The adopted paragraph 12, one of three mentions of gender or women in the document’s 67 principles, states:
We affirm that development of ICTs provides enormous opportunities for women, who should be an integral part of, and key actors, in the Information Society. We are committed to ensuring that the Information Society enables women's empowerment and their full participation on the basis on equality in all spheres of society and in all decision-making processes. To this end, we should mainstream a gender equality perspective and use ICTs as a tool to that end.

Following the first phase of WSIS, gender issues entered the discourse and key outcome documents only in passing, often in long lists punctuated with commas lumping various types of cultural diversity together into a single sentence. The Tunis Agenda, which was the final outcome of the second WSIS phase, includes the words “gender” and “women” three times in its 122 points, and only in subsections, never in the main body. The WSIS process and its outcomes failed to fully integrate gender equality as a crosscutting theme central to the governance of a just information society and, as a result, failed to expand the BPfA in light of ICT advancements.

Moving Forward: Best Practices?

Since the second phase of WSIS ended in Tunis in 2005, international considerations of gender and internet governance have largely played out at annual meetings of the Internet Governance Forum (IGF), born out of the WSIS Working Group on Internet Governance in 2006. It is unsurprising, given the underrepresentation of gender in the WSIS outcome documents, that women have not been well represented at these meetings. The Gender Dynamic Coalition has repeatedly criticized the gender imbalance in participants, speakers, and topics. In 2011, the Women's Networking Support Programme of the Association for Progressive Communication (APC WNSP), a key player in Beijing, developed a “gender report card” in time for the sixth annual IGF meeting in Nairobi. The report card, which APC makes available for all IGF participants to complete online, asks participants to keep track of how many speakers at a given session are women, the stakeholder group(s) women speakers represent, the extent to which a session incorporates a gendered analysis, and the approximate number of women in attendance at the session. Following the 2012 IGF meeting, APC found that, according to the gender report card data, more than half of the 89 sessions failed to mention gender at all and was the main theme in only 4 sessions. Internet Governance for Development (IG4D) sessions, where women made up the majority of participants, were more likely to mention gender. This lead the APC to conclude that women’s attendance correlates with increased focus on gender. Diplo's project on the language of internet diplomacy demonstrates that the gender balance is becoming more equitable at IGF, as far as women’s physical attendance and verbal participation is concerned. Taken together with APC’s conclusions, this paints a sunnier picture for the future of women's representation and internet governance; but questions remain about how to move forward. Given the history of women’s involvement in IG, what are some best practices for crafting a just model of internet governance that ensures gender equality?

The foremost issue is women’s participation. IGF and similar organizations should strive to include greater numbers of women at their meetings. It is important to note, however, that gender should not be conflated with women. The presence of women in an IGF session may increase the odds that gender equality will be addressed; many female participants will likely be members of government and corporate core-stakeholder groups. Addressing gender equality requires more than just female participation; it requires participation by civic society representatives actively working to address gender inequality and ICTs. While the WSIS process failed representatives working toward gender equality, the network of activists formed by the Gender Caucus and GSWG did remarkable work in
shedding light on the gender-IG problem and empowering women through educational outreach efforts focused on the complicated field of internet governance. Further, while the presence of women and of gender equality activists is critical, they must also participate on panels, as session leaders, and as moderators. This, of course, is part of a larger problem concerning civil society’s role in internet governance fora.

Following participation, the integration of gender as a topic remains problematic. This question was raised during the closing session at the Milton Wolf Seminar—should we have devoted a single panel to gender equality and internet governance? The answer espoused by others and myself was a resounding “no.” As seen in the efforts of the Gender Caucus and GSWG, the IG feminist ideal is one that mainstreams gender as a crosscutting theme rather than ghettoizing gender to a single session where it is addressed and left behind before moving on to the next session. In practice, this first requires overcoming gender-blindness by exposing: 1) the male-dominated nature of the factions competing for attention as IG stakeholders, 2) the social and cultural privilege and power granted to males in all arenas, especially politics and technology, and 3) the tendency to address an abstract citizen-subject rather than addressing the ways in which gender, as one axis of identity intersecting with other social, cultural, and economic categories, affects individuals’ access to and experience with ICTs.

Bringing these three feminist principles, with special emphasis on the latter, into awareness should, ideally, enable the integration of gender into all IG discussions and consideration of gender as important in itself, not lumped together with other types of “diversity” or marginalized groups. As one could imagine, however, this is easier said than done; and, from where I am standing, it seems like it would require an international feminist revolution. Gender mainstreaming also runs the risk of erroneously universalizing women’s experiences from privileged perspectives. Still, mainstreaming gender as a crosscutting theme is a worthwhile ideal, even if seemingly unattainable, as it throws the current gender-blindness and gender biases into sharp relief.

Mainstreaming also requires lifting the restriction of gender to certain areas. As the APC gender report card discovered, discussions of women in IG is typically relegated to IG4D/ICT4D contexts. Margaret Gallagher, in her entry in the 2011 Handbook of Global Media and Communication Policy, points out that this is because ICT4D positions women as a vulnerable group that could benefit from traditionally valued development efforts, such as education and ICT training; this is in contrast to more controversial, progressive frameworks that see women as key players and gender as a central issue to every aspect of IG. Whereas the latter is the road less traveled by, IG4D/ICT4D grants easier entry onto the internet governance stage for gender equality activists because its motivations have more obvious ties to the existing IG discourse. Further, as Heike Jensen wrote in the 2013 edition of Global Information Society Watch, feminists have critiqued IG4D/ICT4D initiatives that run the risk of training girls and women in developing nations for exploitation by global capitalist economies. Meanwhile, lobbying efforts concerning women-friendly infrastructure development have largely failed, as they do not appeal to the more longstanding, gender-blind values embedded in IG discourse. Pushing the limits of the IG-gender conversation could lead to better IG and ICT policies for women and girls. Gender mainstreaming, as Jensen argued, does not mean inserting an awareness of gender into existing hierarchies, but using a feminist platform to transform and combat these hierarchies.

Lastly, I would like to consider best practices for the content of IG-gender discourse. Feminist activists and scholars must continue to demand the collection of gender-disaggregated data,
without which we cannot hope to combat the gender-blindness of the existing IG discourse. Following Jensen and with respect for the heroic work that punctuates the gendered history of IG, discourse concerning gender equality and internet governance must also demand normative commitments through reaffirmations of past interventions, such as the BPfA. In order to make progress, we must point to what has already been done and promised, so that we might build upon rather than forget the accomplishments of feminist activists. As with any other IG-related issue, normative commitments must also be paired with concrete action plans, so that discourse might be implemented in policy. Finally, the content of IG-gender discourse needs to be accessible. The Gender Caucus and the GSWG did admirable work in drafting principles that avoided jargon and making assumptions about readers' technical knowledge. Given that women's barriers to entering the IG conversation are related to women's barriers to entering the science and technology fields, feminists working in IG should be mindful of their language and should strive to educate other feminists about IG and its relevance to the struggle for gender equality.

Refusing to be the Price

The small but determined group of feminist media activists who joined forces in Beijing nearly 20 years ago may have been disheartened to find us still grappling with gender and internet governance at the 2014 Milton Wolf Seminar. Moving forward, we would do well to remember their tenacity, the J Section, the disruptive t-shirt campaign their legacy inspired, and the unjust quickness with which their efforts for gender equality were brushed aside during the WSIS process. Tracing a gendered history of internet governance does more than shed light on good and bad strategies for better inclusivity and representation of women; it also exposes the international community's tendency to brush gender equality to the side of ICT-related issues, or at best, to confine it to “development” or lump it together with other types of diversity in passing. Like Anna in The Third Man, women and gender equality activists must not acquiesce to having their concerns overlooked in the male-dominated network that constitutes the information society. Women must refuse to be the price paid in exchange for more streamlined internet governance discourse uncomplicated by the exposure of gendered power hierarchies. As the first point of the J Section reminded delegates gathered in Beijing in 1995, “Everywhere, the potential exists for the media to make a far greater contribution to the advancement of women.” Those whose work revolves around internet governance should endeavor to highlight, not eclipse, this potential.

About the Author

Clark, Rosemary

Rosemary Clark is a doctoral student at the Annenberg School for Communication and a 2013 graduate of Ursinus College, where she earned her Bachelor of Arts in Media & Communication Studies and English. Her research can be summarized as a twofold feminist approach to media activism. As an undergraduate student of feminist media studies, much of her research revolved around deconstructing mass media representations of women and girls using critical feminist frameworks. As an Annenberg student, her research has turned toward understanding how and why contemporary American feminists use digital space to mobilize direct action against disempowering media representations and to delineate the boundaries of their feminist activist identities. Rosemary's
work pairs traditional and new media studies with feminist and social movement theories and employs a range of methodologies, including textual and content analysis, discourse analysis, network analysis, and ethnography.
“Am I Big Brother’s Keeper?”

By Lee McGuigan

I

Post-war Vienna, as portrayed in the film *The Third Man*, could be interpreted as a metaphor for the internet: A handful of competitively positioned actors are vying to assert authority over a jurisdiction and its strategic resources. While the edges are balkanized to a certain extent according to the controls, values, and norms imposed and enforced by sovereign powers, the central space is an ostensibly international zone in which claims to ownership and authority are contentious and without an obvious natural basis. In many ways, the development of the internet is impaired by an inability to resolve competing narratives of closure. In other words, the actors are staking not only geographical but ideological claims about what the digital space means, how it should be used, and who will oversee its assembly and maintenance. Closure is thus both a matter of architecture and a matter of vision—of consensus about the values embedded in the design of the internet (and its intended functions) and the norms underpinning the legitimacy of an actor’s claim to authority. Absent this closure, the global internet, like post-war Vienna, is a liminal zone wherein strategic actors enforce their preferred agendas, which correspond to different “social imaginaries” (cf. Mansell, 2012). The actors police the space to protect the health and safety of citizens, or facilitate the “efficient” and “free” functioning of markets, or enforce boundaries of citizenship—to determine: who has rightful a claim to belonging; what is the nature of their rights; who are not legitimate citizens; what access to the space non-citizens are afforded; and what punishments befit transgression. Throughout *The Third Man*, the strategic actors (e.g. the Russians and the Americans) use different tactics to pursue different priorities, sometimes in cooperation and sometimes in discord. Their attitudes toward the agendas of other actors range from indifference, to ambivalence, to antipathy in cases of conflicting objectives. Ultimately, these attitudes are also inherent in power struggles over global flows of information and competing narratives of legitimacy about who should govern the internet and how.

II

In a 1972 interview with Peter C. Newman, which was lost, rediscovered, and then published in *Maclean’s* magazine in 2013, Marshall McLuhan made some provocative and startlingly prophetic pronouncements: “The new human occupation of the electronic age has become surveillance. CIA-style espionage is now the total human activity. Whether you call it audience rating, consumer surveys and so on—all men are now engaged as hunters of espionage.” Continuing along this line, he goes on to predict that, “The biggest job in the
world will be espionage. Around the world, people are spending more and more of their time watching the other guy. Espionage at the speed of light will become the biggest business in the world.” Venerated techno-utopian and a founding editor of Wired magazine, Kevin Kelly (2014) admits what McLuhan foretold forty years prior:

The internet is a tracking machine. It is engineered to track. We will ceaselessly self-track and be tracked by the greater network, corporations, and governments. Everything that can be measured is already tracked, and all that was previously unmeasurable is becoming quantified, digitized, and trackable.

The capacity to collect and analyze what a Big Data scientist at MIT calls the “data breadcrumbs” left behind from our digital lives is embedded in the technical and bureaucratic architectures of our information society (“Reinventing society in the wake of big data,” 2012).

McLuhan anticipated that electronic media would draw together humans within a Global Village in which we would all know the business of our neighbors, whether next-door or overseas. So-called social media, such as Facebook and Twitter, certainly facilitate correspondence with our global neighbors; but it is increasingly clear to people that even when they draw the curtains, some neighbors are still peering in surreptitiously. Businesses and governments are racing to build ever more sophisticated and expansive data armories. Again, these strategic actors are harvesting data for various purposes: to accelerate market exchange and reap “efficiencies” through targeted marketing; to protect users from cybersecurity problems (as in some uses of deep packet inspection); and to ferret out “unworthy” cyber citizens, whether criminals, terrorists, or undesirable consumers. An enormous amount of surveillance is undertaken in service of offline law enforcement. Like post-war Vienna, the Global Village is policed by interests that may be working together or at cross-purposes, and often not in view of each other.

III

Ongoing debates over internet governance are marked by technical and administrative complexities, and they have profound global implications for various arenas of public and private life (DeNardis, 2014). The internet has a currently unrivaled ability to observe and analyze human communication activities. As increasing aspects of life are mediated by internet-enabled media—commerce, education, health care, social organization, political action, domestic life, etc.—questions about who gets to manage these apparatuses of surveillance and control are increasingly urgent. The battle for internet governance—which rages not only among sovereign states but also corporations and political organizations with leverage over some or other component of the physical and administrative infrastructure supporting networked communications—is also a battle for a stake in determining and benefiting from technologies of social control. What sorts of mechanisms can be put in place to check the power afforded individuals and groups monitoring or policing the digital domain? What is the appropriate balance of distributed
control among the “stakeholders”—a label which in formal venues typically designates a rarified set of actors representing states, industry, and civil society?

These questions are far from closed.

My interests are particularly focused on the impending Internet of Things—or the more ambitious Internet of Everything, as has been recently trumpeted by Cisco, Intel, and others. Sometimes called the Industrial Internet, the Internet of Things describes a condition in which microprocessors and sensors connect virtually all objects, whether ordinary or technically sophisticated, within a digital, wireless communication network. Not only computers and electronic appliances, but also clothes, product packages, medical instruments and even human bodies are fitted with flexible, nano-sized, and relatively cheap chipsets. With the Internet of Things, the scope of ubiquitous connectivity is staggering. Cisco boasts that the Internet Protocol version 6 (IPv6) has the capacity to assign unique web addresses to 4.8 trillion objects for every star in the known universe (Bradley, Barbier, & Handler, 2013, p. 2). The Internet of Things presents enormous potential to improve the administration of health care services, to aid emergency response both in cases of personal injury and public crises, to enable better allocation of resources such as energy and food—these are, of course, many of the promises punctuating discourses on “Big Data.” But the Internet of Things will not develop in line with these purposes as a natural matter of course. Its development and deployment is a social process, dictated by the visions of vested interests and the power of those interests to marshal resources toward realizing their visions. That is to say that it is not obvious that this technological apparatus will be put to use more forcefully for health care than for targeted marketing. Perhaps the most zealous proponents of the Internet of Things are among a marketing and managerial elite who imagine a ubiquitous marketplace in which consumers and employees are “always on” (McGuigan & Manzerolle, forthcoming). Beyond the now normalized ambitions for tracking consumers across devices and as they move through virtual and physical commercial environments, marketers imagine connected devices and product packages that automate consumer decision-making to the point that a carton of milk will automatically trigger a purchase when it is nearly empty. Gartner (2013) research predicts that by 2017, some 10 percent of online consumer purchasing decisions will be delegated to connected devices and 80 percent of consumers will become data brokers, collecting their information and using it to barter with merchants for customized deals.

How this connected environment takes shape will not be a matter of pure technical superiority, ingenuous enterprising, or “free” market forces; it will be the outcome of political, social, and economic negotiation. The battle for Internet of the Things governance is already underway, as recently AT&T, Cisco, General Electric, IBM, and Intel have founded something called the Industrial Internet Consortium, with the intention of controlling the direction of the Internet of Things. These are profit-maximizing firms, with no mandate to deploy these technologies in the public interest; yet they have enormous collective power because they build and maintain the technical architecture of the Internet of Things. It is important that critical scholars and civil servants be vigilant in monitoring such organizations and imposing checks on corporate power over what is increasingly the infrastructure for everyday life.
References


McGuigan, Lee, & Manzerolle, Vincent. (forthcoming). ‘All the world’s a shopping cart’: Theorizing the political economy of ubiquitous media and markets. *New Media & Society*.


About the Author

Lee McGuigan is a doctoral student in the Annenberg School for Communication. He studies the business and cultural histories of television and advertising, the sociology of markets and consumption, and the political economy of technology. He holds a Master’s degree from the Faculty of Information and Media Studies at the University of Western Ontario. Lee is co-editor (with Vincent Manzerolle) of the book *The Audience Commodity in a Digital Age: Revisiting a Critical Theory of Commercial Media* (Peter Lang, 2014). His work has been published in *Television & New Media* and *the Journal of Communication Inquiry*. Lee comes from a fruit and vegetable farm in Cedar Springs, Ontario.
Cyberspace and Surveillance: Challenges to State Identity and Ontological Security in the Digital Age

By Robert Ralston

Increasing state surveillance of the internet and a seeming lack of global accountability and best practices regarding foreign and domestic internet policies demands the attention of students, scholars, and practitioners of media and communication, political science, sociology, computer science, and the like. With these concerns in mind, the 2014 Milton Wolf Seminar highlighted themes of surveillance, visibility, disclosure, and espionage in the digital age. This essay seeks to touch upon some of these themes, and to present a case for the study of ontological security in international relations as a way to explain, in part, U.S. practices of surveillance following the leaks by former National Security Administration (NSA) contractor Edward Snowden. Politically, the stakes are high as cyberpolitics becomes an issue of “high politics” in the study of international relations; states and the agents who produce narratives about the state frame cyber discourse in ways that attempt to justify practices of surveillance, espionage, and censorship. States justify intrusion into cyberspace in the name of stability and an idealized self-image. This, can prove violent and costly, with parallels to justifying war on the basis of empire in offline venues. In cyber venues, the United States in particular has had to justify state intrusion into cyber venues. Void of routinized responses to “traditional” threats, the state must reshape or reconfigure its self-image in order to combat the contradictions inherent in state intrusions into cyberspace. Taking in consideration such concerns and dynamics, this essay first sets out to explain ontological security in the study of international relations and the discursive practices of U.S. state agents in justifying state surveillance practices. It then concludes by drawing parallels between these discursive practices and various presentations at the 2014 Milton Wolf Seminar.

Ontological Security in International Relations Theory

Physical security concerns dominate realist accounts of security in world politics (Mitzen 2006: 342). Ontological security in international relations goes beyond the premise that states are solely concerned with physical security. The assumption that states only seek physical security, Mitzen (2006: 364) argues, constrains international relations theory by failing to explain why states may seek or continue conflict at the expense of physical security. Inherent in the conception of a state’s ontological security is the notion of the state as person, or at the very least, that states are concerned with their own self-image. 20 Ontological security is about constructing and maintaining the stability of a state’s self-image. Power, in this regard, can be understood in terms

---

20 See Wendt (2004) for a discussion of the validity and appropriateness of understanding the state as person in international relations theory.
of “a centralized body’s internal capacity to perceive its ability to operate upon its own self-image, as well as influence others and determine outcomes” (Steele 2010: 15). Thus, power is not solely based upon a state’s ability to make other actors do what they would otherwise not do, to pose material threats to other states, or assert global influence; power is about the state’s recognition that it can use and recreate its own self-image.

States put forward narratives about themselves through state agents, such as government officials. State actions must be justified, even if they go against the grain of international norms or expectations (Steele 2008: 10). What is particularly interesting about the U.S response to the Snowden disclosures is the manner in which the disclosures were framed, the contradictions that arose as a result of this framing, and how the narratives that the state produced regarding NSA practices harken back to the self-image-making of the U.S. state.

Why the United States?
When examining speeches made by U.S. state agents, publications regarding U.S. citizenship, and the ways the United States is presented in popular culture, common trends emerge: The United States is presented as exceptional, as a land of shared values—liberty, freedom, and prosperity—which were created by the nation’s founding fathers. David Campbell (1998: 131) suggests that America is an imagined community “par excellence.” America, like all other states, is dependent upon practices that make up its ontological being. However, as Campbell (1998) argues:

Defined, therefore, more by absence than presence, America is peculiarly dependent on representational practices for its being. Arguably more than any other state, the imprecise process of imagination is what constitutes American identity (p. 91).

Space and time in reference to U.S. identity is crucial to this analysis because successful fulfillment of ontological state security is predicated upon that state’s ability to maintain a consistent self-identity and self-image. Void of a people as a foundational element, the United States’ self-identity is quite fleeting, and, thus, hinges on representational, symbolic, and iconic imagery in order to ascribe to itself some form of identity (Campbell 1998: 132).

The U.S. State Narrative
In a speech made prior to Snowden’s disclosures, President Obama spoke of the necessity to secure cyber infrastructure while maintaining the internet as a free and open space:

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. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free.

In light of the Snowden disclosures, a contradiction arises between the actual behavior of the state through its national security agency and the self-image of the state. President Obama sends two distinct and seemingly irreconcilable messages regarding cyberspace: First, the United States, as a centralized power, recognizes the tensions that it must mediate between security and
liberty; Second, the United States has a vision for cyberspace, one focused on being “open and free.” But free for whom? U.S. security policy is decentralized insofar as it attempts to do too much while still trying to keep a constant self-image (See Campbell 1998 and Gould and Steele 2014). Cyberspace is not an “American thing,” but from cyberspace comes a multitude of images that only exacerbate the imagined nature of American identity. Thus, what cyberspace is and what cyberspace means, from an American perspective, is inherently American.

Addressing the “noise” surrounding the practices of the National Security Administration, President Obama first noted the history of intelligence gathering by the United States:

At the dawn of our Republic, a small, secret surveillance committee, born out of the Sons of Liberty, was established in Boston. And the group’s members included Paul Revere. At night, they would patrol the streets, reporting back any signs that the British were preparing raids against America’s early patriots.

In order to find footing and precedent in the face of ontological insecurity in cyberspace two rhetorical moves are deployed. First, history is resurfaced and reworked to create a seemingly appropriate metaphor for the present. This history is doused in a patriotic whitewash, whereby particular events are chosen but not others that are perhaps more indicative and relevant to the current situation. Further, the parallels put forward by Obama are not parallels at all; the nature of surveillance, global politics, globalization, and technology are not the same as they were 200 or so years ago. This history serves to maintain the state’s self-image over time. Campbell (1998: 130) notes that the American quasi-war with France “demonstrated how previously established discursive strategies of otherness could be invoked in novel circumstances to provide powerful modes of understanding.” Much in the same way, President Obama’s return to history serves not only to ground justifications for NSA activities in seemingly consistent practices of state surveillance, but also in actions against threats from an “other,” in this case, the British during the Revolutionary War. Threats in cyberspace come from a plethora of sources, including: other states, non-state actors, rogue Americans, or even cyberspace itself.

Obama’s second rhetorical move is to argue for American exceptionalism. He goes on to note,

But America’s capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

The justification for (at least toned down) policies of NSA surveillance centers on the notion that “someone has to do it,” and “we can do it better than anyone else.” America’s status as “the world’s only superpower,” as President Obama declares, opens itself up for interrogation.

At the end of his speech on NSA reforms, President Obama demonstrates, perhaps unintentionally, that ontological insecurity is a powerful motivator for the United States in cyberspace:

_When you cut through the noise, what’s really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed._ Whether it’s the ability of
individuals to communicate ideas, to access information that would have once filled every great library in every country in the world, or to forge bonds with people on the other side of the globe, technology is remaking what is possible for individuals and for institutions and for the international order.

This is not to say that the United States consciously and reflexively recognizes its ontological insecurity in its relationship to cyberspace. However, the examples that are raised concerning the dangers of cyberspace—from cyberspace as a mechanism for terrorist mobilization to cyber wars of the future—do not paint an entirely clear picture of what makes cyberspace something truly different in global politics. This shift is not universal, or at least to the same degree, for every state. Cyberspace may provide a vehicle for dissent, organization, etc. for every state, but it burdens states that are fixed in terms of physical security and depend on an idealized self-image. States are pressured into explaining the contradictions that arise as a result of their self-image (freedom, openness, transparence, for example) and state-led intrusions into cyberspace.

Foreign Policies of the Internet: Surveillance and Disclosure Revisited

The 2014 Milton Wolf Seminar brought to bear, and framed well, this theoretical construction of state ontological security in international relations. In particular, many of the presentations dealt with the critical problematic of the balance that must be struck between state self-interest by way of national security and internet diplomacy, global governance, and transparency. Panelists discussed this problematic in various contexts ranging from state censorship of information, international law, and state sovereignty. The internet, and cyberspace more generally, has very real physical characteristics that are often forgotten in discourses of a “borderless digital world” or the metaphor of the internet as a “cloud.” Indeed, the internet is built upon a physical framework, logical building blocks, and interaction (Choucri 2012); and each of these “layers” carries very real political ramifications. State ontological security in cyberspace, as described above, assumes the structural realities of power in international relations regarding the internet, and seeks to elaborate upon how states, beyond concern for their physical security, come to justify surveillance practices on the internet. In this sense, the Milton Wolf Seminar proved invaluable as practitioners and scholars sought to elaborate upon the role of the internet, censorship, privacy, and surveillance in diverse contexts including the national policies and practices of Russia, South Africa, the United States, China, and Britain. Further, the seminar participants elaborated upon shifting or different physical as well as content-layer considerations that need to be taken into account, such as changing modes of internet use, types of surveillance practices, and statecraft in the digital age. The discussion held over the course of the two-day seminar invoked more questions than answers; analysis of such issues has thus far moved, as one seminar participant described, “glacially” alongside the need for internet governance. Thus, the seminar was both timely and a necessary given the salience of internet security, privacy, and surveillance in international politics, along with the perhaps shifting role of the state, and traditional concepts of international politics: state power, sovereignty, and global governance.
References:


About the Author

Robert Ralston is a second-year Master’s student in the Department of Political Science at Virginia Tech. His research interests broadly include international relations, critical security studies, cyberpolitics, and surveillance. Robert is writing a thesis that examines state ontological insecurity with respect to cyberspace, and how state surveillance practices are justified through narratives of liberty and security. He is originally from Glasgow, Scotland.

Twitter: @RobertJRalston
As the internet has come of age in the era of globalization, it has brought both significant benefits and new challenges to global communication. The multinational technology companies who provide internet services have had to weigh the benefits, costs, and risks involved in entering the industry. One major risk centers on their relationship with governments. Revelations of extensive government surveillance, the related movement to “internationalize” and democratize internet governance have introduced the potential for disruptive and perhaps seismic shifts in how the internet operates; multinational companies are in the process of developing strategies to address these foreign policy challenges and to protect their interests within the current global governance structure.

The theme for this year’s Milton Wolf Seminar was therefore timely. Significant portions of the discussions addressed how transformations occurring in global internet governance will influence corporate responses. The panelists identified three overarching themes as the drivers of the ongoing debates surrounding internet governance.

1. The multi-stakeholder model of governance,
2. Differing conceptions of Internet society, and
3. “Democratizing” international control over the Internet.

In each scenario, the multinational technology corporations play key roles in the evolution of the conversation and tailor their responses accordingly to meet future challenges.

**Multi-Stakeholder Governance**

The first theme, the multi-stakeholder model for inclusive internet governance, has remained highly contested in terms of its ability to effectively address all the needs and gaps in the current management of the internet. Panelists in the *Locating Internet Governance in the Diplomatic Machinery* session pointed to several destabilizing characteristics of the current multi-stakeholder model, such as: masking structural abuse of power, legitimizing powerful actors and enabling vulnerability to manipulation. Attempts to create an inclusive multi-stakeholder internet bill of rights—as the *Net Mundial conference* seeks to do—would face a large uphill battle against pushback from democratic and authoritarian governments alike. Despite this pushback, the panelists agreed on the need for greater transparency in internet governance decision-making processes and the need to include governments, industry (the technology corporations) and civil society (technology users as rights holders). The reticence of governments to include non-state actors—namely, business and civil society—in the policy formulation process reflects the greater challenge of successfully integrating multi-stakeholder involvement in internet governance. Where, then, is the resolution and how can multinational technology companies leverage their influence to respond to this challenge?

In the absence of a formal multi-stakeholder structure of internet governance, technology companies have created their own multi-stakeholder forums. The *Global Network Initiative*
(GNI), for instance, provides an informal forum for consultation between technology companies, non-profit human rights organizations, and responsible investing firms on how to safeguard user freedom of speech and right to privacy in the face of government intervention. Still nascent in its reach, the GNI has enabled technology companies: to learn how to respond to government demands for information, to assess and ameliorate their own impact on human rights, and to better communicate these policies to their users. Although none of the recommendations and solutions laid out by non-profit organizations are binding to technology companies, the forum provides a mechanism for technology companies to reform their practices in a way that mitigates risk. The Global Network Initiative and similar forums of engagement can therefore help to bring greater visibility to multi-stakeholder concerns surrounding internet governance and provide technology companies with the opportunity (if they are willing) to translate and integrate those concerns into their business policies.

Conceptions of the Internet Society

As highlighted by Seminar discussions, this second theme forces the technology sector to examine how their various countries of operation conceive of the internet society. Panelists in the Information Regimes and the Future of the Media session referred to different types of framing—such as freedom of expression versus the right to privacy—as the basis for how different societies view their relationship with the internet. Emphasis on the right to privacy, for instance, resonates strongly in many European countries. EU member states have been instrumental in codifying the right to privacy in several international treaties, such as the European Convention on Human Rights and the International Covenant on Civil and Political Rights. Alternately, the concept of freedom of speech on the internet resonates more strongly among US users, given its centrality in the American constitutional process and the Bill of Rights.

Outside of the Global North, especially within the BRICs (Brazil, Russia, India and China), framing of internet society is context-specific. Panelists in the Foreign Policies of the Internet: Key Actors and Debates session highlighted the social construction of the internet in Russia, for instance, through the lens of security imagery. The internet is a battlefield in cyber warfare, a space for crime and fraud, a space for propagating normative threats to traditional values, and a space for foreign agents. This imagery, along with the absence of voices for alternative social conceptions, explains why Russians are more comfortable with internet censorship than citizens in most other countries in the world. Panelists also described the Chinese conception of the ideal internet society as one that prioritizes justice over than freedom in terms of civil society’s relationship with government internet regulation.

However, government policy is not always an accurate reflection of the public opinion within the country, as exemplified by this Pew Research study on internet freedom in emerging markets. For instance, despite the widespread institutionalization of internet censorship in China, freedom of speech advocates have found ways to circumvent government system by setting up proxy servers as virtual private networks (VPNs) or speaking in code to get around automatic filters. Moreover, mass protests around the 2012 elections revealed that although many Russians support government control over information flows on the internet, a greater activist movement for freedom of expression in the blogosphere and social media is emerging, especially among the younger generation. Therefore, multinational technology companies must delicately balance the
demands of civil society, public opinion, and official government regulation in countries around the world.

Multinational technology corporations have a mixed record in taking the cultural considerations of internet governance into account. Three patterns emerge in the interaction between cultural influences and corporate behavior. First, some companies operate under unique political contexts; Chinese and Russian web companies employ human censors in order to comply with government regulations over the flow of information. Baidu and Sina Weibo in China and Yandex and Vkontakte in Russia represent homegrown businesses that reflect this trend. These instances demonstrate the potential complicity that businesses have in perpetuating government surveillance and absolute control over personal communications, information, and expression.

Second, some companies set the tone for conceiving the internet society, especially in post-conflict environments and areas with a large digital divide. The Contested Internets: Censorship and Surveillance as Fault Lines panel pointed to two examples in particular where this is the case: in sub-Saharan Africa, where internet connectivity is still novel to large parts of the continent, and in Myanmar, which is largely a blank slate for building up the information and communication systems infrastructure. In Myanmar, two companies are competing for the licensing rights to build the national telecommunications structure: One is the socially responsible Telenor, a Norwegian company who is a member of the Telecommunications Industry Dialogue on freedom of expression and right to privacy issues; And the other is the Qatari company Ooredoo, which was complicit in enabling smart filters and shutting down services during the Arab Spring. How these competing ideologies will play out in Myanmar’s post-authoritarian political and social scene reflects the power of technology companies in shaping internet society and connectivity.

Third, some companies evolve with civil society’s understanding of its internet rights. European Union regulations, for instance, reflect civil society’s vocalization of its concerns about rights to information privacy and the responsibility of multinational technology companies to those rights. As a result, multinational corporations either develop self-regulation strategies or better corporate social responsibility mechanisms to satisfy their consumer bases regarding privacy protection. In this scenario, government either plays the advocate role or the adversary role regarding corporate actions. As advocates, governments enforce regulations to protect user privacy and freedom of expression from corporate mishandling. As adversaries, governments provoke corporations into balancing legal compliance with government requests for information with their duty and responsibility to protect user information. In either case, corporations are therefore beginning to develop corporate social responsibility strategies and processes for dealing with this dilemma. Almost all of the major technology companies provide a transparency report documenting the number of government requests for information that they receive, and have issued human rights statements outlining rudimentary guidelines for conducting due diligence and impact assessments about how user information is safeguarded.

Democratizing International Control Over the Internet

The third theme discussed at the Seminar involves international control over internet governance. This highly contentious issue gained little traction before the Snowden revelations. The Internet Corporation for Assigned Names and Numbers (ICANN)—dominated by the United States in terms of representation and policy formulation—currently plays a central role in internet governance. However, as internet services and networks have globalized, states have pushed to
“democratize” control over internet governance by bringing its administration under an international body. Although attempts at the World Summit for Information Society and the World Conference on International Telecommunications in Dubai failed to bring internet governance underneath the International Telecommunications Union (ITU), the revelations about US government surveillance activities have now invigorated alternative proposals. The Strategies for Governing Communications: Between the Global and the Local panel, for instance, discussed German and Brazilian proposals to route data traffic through internal national servers rather than relying on the American-dominated system. Brazil, in particular, has been championing responsible internet governance through its own legislation (a bill of rights for the Internet passed its Chamber of Deputies in March 2014) and its hosting of the global Net Mundial conference in April 2014. As a result of international pressures following the exposure of American surveillance activities, the United States has promised to decrease its control over ICANN (the National Telecommunications and Information Administration of the US Commerce Department oversees key ICANN functions) in order to repair its relationships with foreign governments. All of these drastic changes to internet governance ultimately promise to have a great impact on how multinational technology companies operate in different countries.

The main concern of multinational technology corporations is that more international control over internet governance will only increase the number of instances of government censorship and will stifle innovation in the websphere with onerous bureaucratic policies. In response, technology companies have organized into industry alliances, such as the Global Government Surveillance Reform alliance, that lobby for changes in internet governance. These industry groups are informal and fledgling at best, but they reflect the growing trend of industry banding together. By leveraging their networks and government contacts, multinational technology companies plan to influence the direction of these negotiations and clamor for greater participation in the multi-stakeholder process.

Multinational technology corporations are only beginning to conceive of how they fit into the larger geopolitical context of internet governance. They are taking both collective and individual action to mitigate the impact of these changes as a way to preserve their interests and to advocate (occasionally) on the behalf of others. As further proposals from governments and international organizations shift the course of conversations about internet governance, technology companies will be at the forefront of those important decision-making processes and will continue to devise – as they currently do—their own unique strategies for meeting future challenges.

About the Author

Ryan Spagnolo is a second year master’s student and a Hitachi Center for Technology and International Affairs Scholar at The Fletcher School of Law and Diplomacy at Tufts University. His academic research focuses on multinational technology companies’ responses to government surveillance and global Internet governance challenges. Professionally, Ryan has previously worked as a marketing associate for Apprise Software and as a program officer for the American Bar Association’s Section of Administrative Law and Regulatory Practice in Washington, DC. He has also served as an Economic Sector intern for the U.S. Department of State Mission to the European Union. He holds a B.A. in History, cum laude, from Cornell University. Twitter: @RyanSpagnolo
INTERNET GOVERNANCE, TECHNICAL STANDARDS AND THE "TREE" ANTENNAS

By Diego Vicentin

Just as soon as I arrived from Brazil in the US, to join the CITP-Princeton team as graduate fellow, the curious image of cellular antennas disguised as trees caught my attention. It is common to see these "tree" antennas right beside the road while travelling from Princeton to New York, Philly, or Boston. Besides the purpose of avoiding visual pollution, this attempt at producing a friendlier landscape is representative of our relation with information and communication infrastructure. The technical and political apparatus that supports the mode of operation of digital technologies is predominantly invisible to the end user. Only the ones who really pay attention can see the antenna behind the fake tree branches. Normally that is not the case. The majority of users take infrastructure for granted, rendering it invisible. Whereas such invisibility might be seen as an unintended result of both the technical complexity of digital communication networks and its decentralized form of governance, in fact, it is commonly used as a power strategy to avoid accountability as well as broader political participation in technological governance.

Fortunately, Edward Snowden’s revelations have shed light on the issue of technological governance, bringing technology into the mainstream of contemporary political discussion. We must understand and discuss the strong connections between politics and technology in order to transform invisibility into transparency. The process of shaping information and communication infrastructure and operations should be transparent to the extent that individuals can the dynamics, the political dilemmas, and the embedded power relations.

It was in the best spirit of shedding light on the connection between policy and technology that the discussions took place at the 2014 Milton Wolf Seminar at the Diplomatic Academy of Vienna. The Seminar focused specifically on internet governance and its current and future implications for international relations, national sovereignty, privacy, and surveillance. The discussions, however, were not limited to these topics and other themes arose, including the one I am particularly interested in: the standards development process.

Although this theme was not the focus of any presentation, the word "standard" was mentioned countless times during the seminar because one must inevitably speak about technical standards when discussing issues of internet governance. Digital networks rely on technical standards in order to assure interoperability and work as true means of communication. Developing technical standards is making governance by design—or in other words, making technology governance de facto. It is a way of partially defining the terms through which the exchange of information will occur. These are the points I will stress in this blog post while trying to connect my research interest on standards development with the central topics discussed at the 2014 Milton Wolf Seminar.

Privacy, security and surveillance.
The December 2013 UN adoption of the resolution "*Right to Privacy in the Digital Age*" was an important step towards protecting the right to privacy in cyberspace. It is widely known that Brazil and Germany drafted the text as a political response to the revelations of NSA spying activities in these countries, which included surveillance of Brazilian President Dilma Rousseff and German Chancellor Angela Merkel. The international community expressed wide support for the drafting and proposing of the resolution, considering it an important measure, even though, in practice, it does not stop or even diminish surveillance. At the opening of NetMundial internet governance meeting in São Paulo, President Rousseff indicated in her speech that the UN resolution was only the very first step towards privacy protection. As a second step, I would suggest (to Brazil, Germany and whoever else is concerned) that they start paying attention to the development and adoption of crypto standards.

It is fairly known today that the NSA has undermined crypto standards in order to monitor the secure communications of internet users. To put in the exact words of the NSA’s memo which was leaked by Mr. Snowden and partially published by *The New York Times*: “For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies...Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable.” Because of the NSA’s activities, sensitive data like medical records, online banking, and private e-mail communication becomes more vulnerable. But, how is the NSA breaking these encryptions?

According to Snowden’s revelations, the NSA’s decryption program (named Bullrun) includes simultaneous strategies that includes coercing and/or paying private companies who produce security software to include backdoors in their own products. I am referring to the case of RSA’s BSafe software, which included a flawed algorithm as a default. Subsequently, the algorithm in question (named as Dual_EC_DRBG) was included also in crypto standards approved by the National Institute of Standards and Technology (NSIT) and by ISO/IEC as an option among other existing algorithms for core techniques in crypto applications. This means that the NSA succeeded in inserting a flawed technique into widely used and recognized security standards. This fact leads us to another question: how were they able to influence the standardization process in that way?

Since only the NSA has the key to exploiting the flaw produced by the Dual_EC_DRBG algorithm, we might adopt a naïve view and assume that before the Snowden leaks the backdoor was only a mere supposition raised by two crypto experts in 2007; and that the algorithm was technically defensible and therefore could be included in crypto standards. It turns out, however, that technical excellence is not the only one or even the most important part of the standards creation process.

To influence the development of a standard, one specific organization (like the NSA or any other) must have accumulated technical expertise as well as the ability to manage the bureaucratic structure of a given standards development organization (SDO). They must understand the internal policies and procedures of the SDO in question and use them to guide the process toward the desired outcome. Dominating the language, the proper specific vocabulary that every SDO seems to have, is also essential. An engineer very familiar with standards development once told me that “every word matters” in the standards drafting process. Making alliances with other stakeholders and negotiating appropriately with those who have conflicting interests is also critical. Of course, such a task becomes easier if people from your organization occupy leading positions in the SDO structure, such as chairman of the working group responsible for drafting the standard.
These are only the basic requirements necessary for really taking part in the game of building ICT standards. There are several active SDOs developing standards in the ICT arena, all of which vary in their structure and practices. Just to give a few examples, SDOs differ regarding their technical scope, geographical area of influence, openness, and membership and participation rules. If a determined company or organization wants to exert some level of influence in the whole standardization ecosystem it must be present in all relevant SDOs. In other words, the ability to influence the standards development process is directly related to the organization’s ability to participate in different standardization bodies. This provides an indication of how costly it is to participate in standards development and potentially explains why the NSA had to spend so much money on its decryption program ($250 million-a-year).

To clarify my point, let’s examine an example of security standard that might have been suffered from NSA influence. The IPSEC is a standard that provides data authentication, integrity, and confidentiality as it transfers between communication points across IP networks. To put it differently, IPSEC is a fundamental crypto tool that should provide protection to individual data packets while they are being transferred. It is standardized by the Internet Engineering Task Force (IETF), a widely respected “technical community” responsible for drafting internet protocols. The work is mainly done via online mailing lists and face-to-face interactions within different working groups (WGs) dedicated to key technical areas. Participation is open to everyone; and contributions can be made in face-to-face meetings as well as online. Mailing list interactions are published and open to public scrutiny. I tend to agree with Laura DeNardis: regarding governance and procedures, “IETF is an open standards-setting organization, with processes that adhere to democratic principles of transparency and participation (2014:70).”

But the IPSEC case indicates that this openness and transparency might not be enough. Right in the middle of the Bullrun program revelations, a respected free software activist, John Gilmore, published comments about his experience as an IPSEC WG contributor, stressing that the NSA had undermined the IPSEC standards by making it “incredibly complicated.” He highlighted the participation of the NSA employees in the working group as well as their leadership roles, which included serving as the document editors. Gilmore went on to note that, “every once in a while, someone not an NSA employee, but who had longstanding ties to NSA, would make a suggestion that reduced privacy or security, but which seemed to make sense when viewed by people who didn’t know much about crypto.” Gilmore’s observations seem to explain why the highest goals of IPSEC were not achieved. As professor Ed Felten wrote at Freedom to Tinker: “a successful and widely deployed IPSEC would have been a game-changer for Internet security, putting lots of traffic under cryptographic protection” but “indeed, IPSEC has not had anything like the impact one might have expected.”

So we may conclude that the NSA succeeded in undermining a standard with real potential for increasing online security and privacy protection. In contrast to what happened with BSafe, the strategy the NSA adopted in the IPSEC case was to create problems in the development process in order to produce a weak and complicated standard. From my perspective, what the NSA is doing is policy by design. It is interfering with the process of shaping crypto standards in order to ensure the continuity and the feasibility of their mass surveillance policy. It is a perverse policy because it undermines online security, internet freedom, and the human right to privacy.

Governments and civil society organizations committed to the defense of online freedom, privacy, and security should participate in the “technical communities” and help to shape standards that
protect these values. More than that, they must help to shape the ways that these communities operate in order to make the process of constructing standards more inclusive, open, and transparent. Internet governance depends on the technopolitical nature of standards. The main argument here is not new; it goes back at least to Lessig’s “Code is Law.” But it must be remembered and reinforced, against enduring misconceptions that the technical operation of the internet is a separate issue from its political, social and commercial dimensions. This is the blindness that does not allow one to see the antenna behind the fake tree branches.

About the Author

Diego Vicentin is a Ph.D. candidate in Sociology at the University of Campinas (Brazil) and research fellow (2013-2014) in the Center for Information Technology Policy at Princeton University (USA). Diego has been studying the development history and the operation mode of cell phone networks by exploring its technical and political aspects. Currently he is investigating the intersection between politics and technology specifically with regard to decision-making related to the technical standards of mobile broadband networks. Twitter: @diego_jv
MAKING ACCESS VISIBLE: REPRESENTATIONS OF THE INTERNET

By Willow Williamson

Marshall McLuhan’s often quoted “the Medium is the Message” took on a new resonance for me as I absorbed the discussions from the 2014 Milton Wolf Seminar. What exactly is “the medium” of the internet; and who gets to define what it contains, decide where it is located, and make decisions about information and communication flows? These were some of the questions that participants discussed at this year’s Milton Wolf Seminar on “Foreign Policies of the Internet.” Panelists examined the layers of meaning contained within and represented by the internet, ranging from the physicality of its infrastructure and ownership, to what it represents as an idea, to how these layers affect international communications and relations. Underlying these conversations were the questions: What happens when international norms are in conflict? And, whose voices are heard and represented in determining and negotiating those norms?

Privacy Versus Security

Since 9/11 and the passage of the Patriot Act, ongoing conversation in the United States places privacy in opposition to security. These debates are not new, as evidenced by David Vincent’s historical account of the privacy versus security debate regarding the United Kingdom Postal Service in 1844 (see also opendemocracy.net article). Most recently, the Snowden leaks brought the issue of state actors using covert surveillance into international diplomatic negotiations. How does the concept of freedom and a free internet fit into this privacy versus security (through surveillance) discourse? One problem is that this binary ignores historical experiences of how security has been used as a way to invade individual and group rights. The debate highlights disparities in US society between those who have assumed the privilege of privacy in public spaces and those who have experienced invasions of privacy in public spaces through practices such as racial profiling. In the post-9/11 world, the idea of privileging security over privacy was, in part, critical to the passage of the Patriot Act. But, for those who were personally and physically affected by the kinds of impositions that the Patriot Act allows have a differing conception of privacy from those who have not experienced how taking away privacy can profoundly impact daily life. Examples of these impositions include intrusions into the home and tracking activities, contacts, and correspondence. There are also other effects ranging from: who gets pulled off of flights for extra questioning, to who is put onto no-fly lists, to self-censoring activities such as what books individuals choose to check out from libraries for fear of raising red flags.

There has been significant scholarly work on how the concept of security extends beyond the state to private spaces of the home as well as on how security works in daily lives and impacts individuals and families. Feminist scholarship in particular has looked at broadening the idea of what is included in world politics to include “the personal and previously invisible spheres.” Laura Sjoberg argues that “looking at war(s) from the perspective of people marginalized in global politics reveals war(s) as lived, experienced, and felt, rather than just made of fought.” In a journal article conversation between Cynthia Enloe and Carole Cohn, Enloe states that she sees,

---

21 Thussu, International Communication, 58.
22 Ackerly, Stern, and True, Feminist Methodologies for International Relations, 7.
23 Sjoberg, Gendering Global Conflict: Toward a Feminist Theory of War, 248.
the “international” as embedded in the national and in the local. And, like you [Cohn], I also see—or, better, have been taught by other feminists to see—the “political” in many spaces that others imagine are purely economic, or cultural, or private.  

Can we identify similarities in the concept of surveillance? And how does this play into definitions of human rights of the internet? As panelist Sejal Parmar reminded us, a potential step away from the binary of privacy and surveillance is to instead focus on freedom of expression as a human right and a response to state surveillance. What do we mean by surveillance? David Vincent suggested that it is first of all an act of doing an inspection. But then the question becomes: what do we do with the information and does it change people’s behavior to know they are being watched?

Internet access points in the home can lead to both freedom of expression and an increased possibility for monitoring and control in the domestic context. Who in our families get monitored and by whom? How do we negotiate privacy and surveillance within our own families? Individual freedom and expression can increase the potential for more individual surveillance. Marianne Franklin pointed out that westernized concepts of private space and abuse as existing behind locked doors become blurred when we conceive of the internet as a public space. This is further complicated by differing conceptions of publicness and freedom around the world. For Franklin, the important point is to understand not just the way we use the internet but that the way it is then used on us.

The binary of privacy/security is also complicated by the ways that private and public spaces are conceptualized on the internet. If the internet is understood as an open and public space, where are the spaces for private communication? What is the interaction between those public and private spaces and ideas of what is necessary, appropriate, justified, accepted, or battled against? Ko Fuji categorized interactions as part of the content layer of the internet. We can make distinctions between what is private and public (blogs, twitter) content. Monroe Price defined these categories of interaction as open terrains of speech where you are talking to the world and closed terrains of speech where you are talking to each other. Surveillance practices, however, do not differentiate between these categories and push at the boundaries between open and closed speech terrains. These boundaries interplay with shifting notions of information regimes and decisions on how to use the media, what qualifies as news, and who or what gets attention.

**Governance Versus Individual Autonomy**

Communication access, as both a form of individual and state power, makes reach and influence possible. Governments and other actors have long competed for control over both the means and content of communication. The first international governance platform of the ITU was formed to regulate telegraph wires for the purposes of interoperability. Over time, the governance of communication systems has evolved and expanded. “Multistakeholderism” has been used to describe how internet governance has become more inclusive of civil society groups and other non-governmental stakeholders. But, who actually has access to a seat at the table and what are the

---

mechanisms for input? (see this article regarding the April 2014 multi-stakeholder meeting NetMundial on internet governance in Brazil)

For panelist, Nishant Shah, discussions on the idea of multistakeholderism as an ideal evoke the ways that the language of multistakeholderism makes the process of becoming a multistakeholder invisible. Some Milton Wolf presentations did the work of making the multistakeholder process more visible. Shawn Powers’ presentation laid out the history of the concept of multistakeholderism, which emerged from 1970s debates about how to share natural resources. Multistakeholderism, according to Powers, can be used to mask structural abuses of power, legitimate powerful actors, and is vulnerable to manipulation. He gave examples of the composition of internet governance groups including Internet Corporation for Assigned Names and Numbers (ICANN), The Internet Society (ISOC), and Internet Engineering Task Force (ITEF) to illustrate who is actually participating in these purported multistakeholder groups. Members of ISOC and ITEF were primarily from the private sector, with very little diversity in terms of gender and race. Panelist Richard Hill stressed that some versions of multistakeholderism are actually about the US retaining or expanding its power. For him, the threat to a multistakeholder process comes from private companies and from governments because of their failure to control companies in dominant positions.

Hill also pointed out that the “freedom to connect” is not the same as the right to connect. In her presentation, Madeline Carr explored the US approach to internet freedom as a foreign policy, as typified by Hillary Clinton’s famous 2010 Internet freedom speech. Several possible contradictions are contained in the US internet strategy, such as the way that the US deploys technology to undermine autocracies while supporting those same governments. (For more examples, see this New York Times article). The Internet in a Suitcase Project, and mesh networks more generally, are a way to create closed systems for dissidents or those without access to gain access points for communication. This program and others focus on circumventing state censorship and blockages. But access is also about access to commerce. But, again, who controls this access; who benefits; and how are these concerns related to the idea of what the Internet represents?

Coverage of Michelle Obama’s March 2014 China visit highlighted her mention of freedom of speech as a universal human right. Hill pointed out that US framing of the internet as a space for freedom of speech in fact translates into the perception that the US is trying to export its ideas of free speech, which allow greater freedom of speech than many other countries. He pointed out that the US simultaneously attempts to export its ideas of intellectual property rights, which, in contrast, are more restrictive that those of some other countries. As Hill argued, “this can be viewed as somewhat hypocritical and might weaken the message in favor of free speech.” In his view, the restrictions on free speech currently permitted in international law are too broad, so proponents of free speech should be calling for modifications of the existing treaty provisions. According to panelist Ko Fujii, one way around this framing has been for the US to instead talk about the free flow of information or data, which becomes an economic argument. Panelist, Daniel McCarthy questioned whether debate will turn into transparency versus privacy binary as a way to articulate the ways that states conceptualize the free flow of data and define open and closed information. States are interested in articulating both security and capacity; and as social technical systems, telecom policy becomes a primary way to present state identity. However, both authoritarian and democratic regimes are using the internet for surveillance. Philip Howard questioned whether the binary of democracy -vs.- authoritarianism could be replaced with open -
vs.- closed to describe approaches to communication. There are differing conceptions of what is permissible content, who should have access, and who decides these parameters.

Sarah Logan reminded participants that power in the information age is then defined by which sets of norms prevail in terms of access. Daniel McCarthy added that there are also colonial legacies to consider in terms of these power relationships. There are linkages between the different layers of governance and resources and capacity to determine or influence outcomes. Alison Gillwald stressed that there are conflicts between the ideas of universal rights and issues of surveillance that increase state power. These disconnects in the way that market reform is then emphasized over democratic rights and reforms points to a lack of clarity in terms of the foreign policy of the internet and engagement in global governance debates. These contradictions become material. Panelist Ben Wagner shared a few data visualizations of the material implications of these contradictions including a map that highlighted the export of surveillance equipment from private sector companies in the EU to China and countries in Africa and the Middle East. Thus, access to the internet and the language of creating more access has multiple capacities and contradictions.

Going forward

The discussions during this year's seminar analyzed how the internet as communications infrastructure and the internet as an ideal continues to develop; highlighted the conflicts inherent in this evolution; and stressed the need for a global conversation about the future of the internet that incorporates varying definitions and contexts. Some of the concepts that complicate current and future conversations about the internet include shifting understandings of private and public space and what it means to have access. Access refers not only to who is able to connect to the internet and information but also who takes part in conversations about how the internet will develop. This discussion links into larger global debates about universal human rights and norms. Governments and non-state actors are using the internet as a way to measure and express power. This reminds us that the ethics and ethos of communication and information flows will continually be under negotiation.

About the Author

Willow Williamson is an International Relations PhD student at American University in the School of International Service, where she received a MA in International Media. Her research is focused on public diplomacy, intercultural communication, gender, and technology. She has worked internationally in the fields of multimedia production, education, and computer science, participating in diverse projects that have brought her to Senegal, Turkey and Spain. She also holds a MFA in Composition and New Media from California Institute of the Arts and a BA in Music Composition and Media Technology from Mills College. Twitter: @willowfw
About the Milton Wolf Seminar Series

Initiated in 2001, the Milton Wolf Seminar represents an effort to explore cutting edge issues facing diplomacy and international relations. Between 2001 and 2013, 378 students have participated in the Milton Wolf Seminar. The 2014 seminar was jointly organized by the Center for Global Communication Studies (CGCS) at the University of Pennsylvania’s Annenberg School for Communication, The American Austrian Foundation (AAF), and the Diplomatic Academy of Vienna (DA). Guests include those working for state and multi-lateral organizations, journalists, media development practitioners, academics, and a select group of highly engaged graduate students interested in the seminar themes.

The organizers envision the Milton Wolf Seminar as a meeting place for media practitioners, diplomats, academics, and students to share their perspectives, formulate new ideas, and identify areas where further research is needed. While the seminar will incorporate various speakers and panels, it is designed as a two-day continuing conversation in which all participants are encouraged to openly engage in dialogue and explore potential synergies and future collaborations. In order to encourage an open exchange of ideas, seminar attendance is limited only to invited participants and students.

About Milton A. Wolf

Milton A. Wolf was an economist, investor and real estate developer who served as President Jimmy Carter’s ambassador to Austria in the late 1970s, where he played a key role in arranging details of the meeting between President Carter and Soviet President Leonid I. Brezhnev for the signing of the Salt II Strategic Arms Limitation Treaty.

Austria’s dedication to humanitarian efforts – taking in over 200,000 freedom fighters from the Hungarian Revolution in 1956, and Czech refugees from the Prague Spring in 1968 – convinced Ambassador Wolf that the Austrian people supported individuals of any race, religion or culture. This understanding ignited Ambassador Wolf’s determination to reward Austria with his loyalty by strengthening Austro-American relations. In 1984, The American Austrian Foundation, Inc. (AAF) was founded, and Ambassador Wolf served as its Chairman from 1990 until his death in 2005.

He initiated and funded the Milton Wolf Fellowships for Young Journalists, (40 Austrian journalists were awarded fellowships to attend Duke University’s Visiting Media Fellowship Program) and the Milton Wolf Seminar for Journalists and Diplomats with the late Ambassador Ernst Sucharipa, then-director of the Diplomatic Academy.

Ambassador Wolf received the Austrian Great Gold Medal of Honor with Sash (Austria’s highest decoration) and the Austrian Cross of Merit for Science/Arts First Class.
Previous Milton Wolf Seminar Topics

2013: “Diplomatic Maneuvers and Journalistic Coverage in a Time of Reset, Pivot and Rebalance”


2011: “Picking up the Pieces: Fragmented Sovereignties and Emerging Information Flows”


2003: “The Role of Media & Diplomacy in Ethnic Conflicts”


2001: “Technology, Policy & Media”
ABOUT THE 2014 MILTON WOLF SEMINAR

Thematic Overview

Filmed on location in 1948 in the post-World War II rubble of Vienna, *The Third Man* highlighted the classic Cold War themes of espionage, surveillance and visibility. Vienna also provided the setting for the 2014 Milton Wolf Seminar, which examined the resurgence of these themes in contemporary international relations and journalism.

The ongoing series of leaks by Edward Snowden provides a stark reminder that new communication technologies also pose new opportunities for surveillance and state power articulation. Conversely, these same technologies also afford old and new media organizations with unprecedented capacities for counter-surveillance and disclosure on a global scale. As states from around the world formulated responses to the American spying program, journalists conveyed these actions to their readers. International condemnation of the US spying program was sharp and swift ranging from calls for UN resolutions on privacy to reform of internet governance institutions. Much to the chagrin of many state actors, press revelations regarding similar surveillance programs by states around the world were equally sharp and swift.

The NSA surveillance regime, while perhaps the most visible, is but one of many examples of state surveillance programs revealed during 2013. More recent leaks outlined similar domestic and cross border surveillance activities by countries such as France, Germany, Sweden, the UK, and Spain. *Folha de São Paulo* in *The Guardian, Australia* published investigations outlining systematic diplomatic espionage activities conducted by Brazil and Australia, two of the most strident critics of the NSA activities.

Embedded in each of these examples is a series of ongoing tensions: between privacy and surveillance; between disclosure and secrecy; and between information sovereignty and global information flows. Rather than looking backward at these events, the 2014 Milton Wolf Seminar looked forward, exploring a range of potential diplomatic and regulatory solutions to evolving issues of surveillance and disclosure, or what we call foreign policies of the Internet. Discussions focused on how non-Western and Western countries are developing their own Internet foreign policy strategies, the role of media and diplomatic actors in translating those strategies, and the implications of these activities for the evolving global Internet. Panels explored the role of diplomats, international organizations, the private sector, civil society and the press in influencing internet governance.

---

25 On November 2, Brazilian President Dilma Rousseff called for a draft resolution on privacy in the digital age on the floor of the United Nations. Just days later, *Folha de São Paulo* published an expose documenting the depth and breadth of the Brazilian diplomatic espionage program.
Suggested Further Reading

In this section, we have included a list of selected readings that address topics related to this year's Seminar theme as well as publications authored by our presenters. We hope you might review some of these materials in advance of the Seminar.

General Readings

- Obama, Barack. 2014. “Remarks by the President on Review of Signals Intelligence.”
- Sasso, Brendan. 2014. "Obama Administration Denies 'Abandoning the Internet',' The National Journal, March 19, 2014:
- Tufekci, Zeynep. "Is the Internet Good or Bad? Yes." MATTER, 2014:

Publications by Panelists

- Internet Policy Observatory – Many of the panelists featured on April 1st are part of the Center for Global Communication Studies Internet Policy Observatory project. You may want to check out the project website for background reading and reports originating out of the project.
• Franklin, Marianne 2013, *Digital Dilemmas; Power, Resistance and the Internet.* Oxford: Oxford University Press.
• Logan, Sarah. 2013. "Has Snowden left international relations stuck in a transit lounge?" East Asia Policy Forum, July 11.
• Price, Monroe. 2014, forthcoming. “Strategic Architectures.” Chapter 6 in *Seeking Resilience, Confronting Anxiety: Strategic Communicators in Global Markets for Loyalties*
Final Agenda

**DAY ONE: MARCH 30, 2014**

6:00 – 8:00 PM **Welcome Reception (Hotel Johann Strauss)**

**DAY TWO: MARCH 31, 2014**

9:00 – 9:15AM **Registration** *(Foyer of the Diplomatic Academy)*

9:15 – 10:00 AM **Introduction** *(Festsaal, Diplomatic Academy)*

In this opening session, the host institutions will introduce the Milton Wolf Seminar themes and the participants. Coffee and tea will be provided.

- **Katharine Eltz-Aulitzky**, Executive Director, *The American Austrian Foundation*
- **Monroe Price**, Director, Center for Global Communications Studies, *Annenberg School for Communication University of Pennsylvania*
- **Werner Neudeck**, Professor of International Economics & Dean, Master of Advanced International Studies (MAIS) Program, *Diplomatic Academy Vienna*

10:00 AM – 12:00 PM **Session 1: Surveillance and Disclosure: Cold War Legacies and Future Directions** *(Festsaal)*

The series of revelations regarding surveillance activities taking place around the world has crystalized attention on the importance of information sovereignty for international relations. New technologies have transformed global communication flows and offered the promise of a global village, while simultaneously reviving and intensifying many of the major themes of the Cold War: surveillance, and disclosure and information sovereignty and global information flows. This panel will set the stage for the two days of discussion at the Milton Wolf Seminar. Panelists will discuss the past, present and future, identifying historical precedents and lessons from previous information regimes, outlining the stakes involved regarding the current debates about privacy and surveillance, and pointing toward future directions. Given the realities of current information structures, international relations, and global information flows, what are the possible pathways ahead?

**Panelists:**

- **Raphael F. Perl** *(Moderator and Panelist)*, Executive Director, *Partnership for Peace Consortium, George C. Marshall Center*
- **Marianne Franklin**, Professor of Global Media & Politics, *Goldsmiths, UK*
- **Philip N. Howard**, Professor of Communication, Information and International Studies, *University of Washington*; and Professor, *School of Public Policy, Central European University*
- **David Vincent**, Professor of Social History, *The Open University, UK*
12:00 – 1:00 PM Welcome Lunch

1:00 – 3:00 PM Session 2: Locating Internet Governance in the Diplomatic Machinery (Festsaal)

Broader awareness of state surveillance and cross-border espionage using new technology has heightened diplomatic, public, and media attention to the current and future role of internet governance. This panel will explore how various corporate, multilateral and state actors are attempting to assert control over internet governance issues and discuss the current challenges and future directions for internet governance in light of recent events.

Panelists:
- **Shawn Powers** (Moderator and Panelist), Assistant Professor, Georgia State University
- **Richard Hill**, Partner, Hill & Associates
- **Ko Fujii**, Consulting Fellow, PHP Institute
- **Reinhard Posch**, Chief Information Officer, The Federal Republic of Austria

3:15 – 5:15 PM Session 3: Information Regimes and the Future of the Media (Festsaal)

Internet governance, surveillance regimes, and state responses have multiple implications for the media, both old and new. First, state investments in surveillance, espionage, circumvention technologies, and the like impact press freedom and autonomy. Second, journalists have played a critical role in covering revelations about surveillance activities, transmitting state and multilateral responses to the public. Finally, the governance and construction of new technological systems are often opaque and hard to translate to the public. Press coverage is thus critical to any process of reform or change. Panelists will discuss the role of old and new media actors and advocacy organizations in each of these areas, outlining current challenges and future directions.

Panelists:
- **Steven M. Ellis** (Moderator and Panelist), Senior Press Freedom Adviser, Europe and North America, International Press Institute (IPI)
- **Andrei Richter**, Director, Office of the OSCE Representative on Freedom of the Media
- **Emily Parker**, Digital Diplomacy Advisor, Senior Fellow, the New America Foundation
- **Sejal Parmar**, Assistant Professor, Department of Legal Studies, Center for Media and Communication Studies, Central European University

7:00 – 10:00PM Heurigen Fuhrgassl Huber

The word *Heurigen* means both new wines (*heuer* meaning "this year"), and the establishment in which it is served. *Heurigen* have become a synonym for what is best in Vienna – hospitality, gemütlichkeit and joie de vivre mingled with a little melancholy, good solid food and refreshing dry wine.
DAY THREE: APRIL 1, 2014

9:00 – 10:45 AM Session 4: Foreign Policies of the Internet: Key Actors and Debates (Festsaal)

Featuring academics focusing on national case studies, this panel will provide a critical perspective on how key global powers are deploying foreign policies related to the internet. Panelists will focus specifically on how major powers like China, Russia, and the United States are seeking to influence and shape internet governance at home and abroad, and the implications of those activities for the global internet.

Panelists:

- **Daniel McCarthy** (Moderator and Panelist), Fellow in Global Politics, Department of Government, London School of Economics
- **Madeline Carr**, Lecturer in International Politics and the Cyber Dimension, Aberystwyth University; co-Editor, Circuit
- **Gregory Asmolov**, Doctoral Candidate, Media & Communications, London School of Economics; Contributor, Global Voices; Co-Founder, Help Map
- **Sarah Logan**, Doctoral Candidate, School of International, Political & Strategic Studies, Australia National University; co-Editor, Circuit

11:00 AM – 12:30 PM Session 5: Contested Internets: Censorship and Surveillance as Fault Lines (Festsaal)

Historically, discussions about internet governance have typically centered on the operations of institutions such as The Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU), and the Internet Governance Forum (IGF). While multi-stakeholderism and technical governance questions remain critical, this panel focuses on key emerging points of contention surrounding global internet governance. In this session, panelists will provide their perspectives on issues such as speech, surveillance, and censorship, and the present realities and future potential of multi-stakeholder internet governance.

Panelists

- **Ben Wagner** (Moderator and Panelist), Internet Policy Observatory Post-Doctoral Research Fellow, Center for Global Communication Studies, Annenberg School for Communication at the University of Pennsylvania
- **Andrea Calderaro**, Researcher, Centre for Media Freedom and Media Pluralism, European University Institute
- **Allison Gillwald**, Executive Director, ICT Africa
- **Elena Zinovieva**, Associate Professor, MGIMO University

12:30 – 1:30 PM Lunch
1:30 – 3:15 Session 6: Strategies for Governing Communications: Between the Global and the Local (Festsaal)

How are local and global concepts used to govern communications? This session will examine how key players in international debates surrounding information sovereignty and internet governance such as India, Germany, and Brazil are employing concepts of a local rather than a global Internet, allowing them to diverge from global norms and, in some cases, even reshaping global Internet governance. It will examine the implications of these efforts for multi-stakeholderism and the future of foreign policies of the internet.

Panelists:

- Monroe Price (Moderator)
- Nishant Shah, Co-Founder and Director of Research, Centre for Internet and Society
- Wolfgang Schulz, Professor, Hans-Bredow Institut
- Sérgio Branco, Director, The Institute for Technology & Society

3:30 – 4:00 Wrap Up Discussion (Festsaal)

We invite all interested panelists and participants to join us for a final round of discussion.

4:00 – 4:45 Emerging Scholar Discussion Session (Festsaal)

During this afternoon meeting we will continue the discussion focused on how this relates to the work of the Emerging Scholars. Emerging scholars will be invited to describe how the issues discussed relate to their own projects and activities.

Panelists:

- Amelia Arsenault (Moderator), Assistant Professor, Georgia State University
- Colin Agur, PhD Candidate, Columbia University
- Anthony Cho, MA Candidate, Fletcher School, Tufts University
- Rosemary Clark, PhD Candidate, Annenberg School for Communication, UPenn
- Lee McGuigan, PhD Candidate, Annenberg School for Communication, UPenn
- Robert Ralston, MA Candidate, Virginia Tech
- Ryan Spagnolo, MA Candidate, Fletcher School, Tufts University
- Diego Vicentin, PhD Candidate University of Campinas, Brazil, Graduate Fellow, Center for Information Technology Policy at Princeton University
- Willow Williamson, PhD Candidate, American University

7:00 Cocktail Reception at the residence of the US Ambassador to Austria, Alexa Wesner
Panelist Biographies

Arsenault, Amelia
Amelia Arsenault is an Assistant Professor of Communication at Georgia State University and serves as the Media and Democracy Research Fellow at the Center for Global Communication Studies at the University of Pennsylvania, Annenberg School. Her scholarly interests center on how different international and domestic actors have attempted to leverage the changing dynamics of communications systems, and the ramifications of those activities for international relations, political and social power relationships, and north/south inequality. In this capacity, she has conducted research on global media ownership, the impact of international donors in southern African communications development, network theory, new media, and public diplomacy. Her co-edited book The Connective Mindshift (with Rhonda Zaharna and Ali Fischer) on the subject of collaborative and networked public diplomacy was released in May 2013. Her scholarly work has appeared in the International Journal of Communication, International Sociology, The ANNALS of the American Academy of Political and Social Science, and Information, Communication, and Society. She holds a B.A. in Film and History from Dartmouth College and an MSc in Global Media and Communication from the London School of Economics and Political Science, and a PhD from the University of Southern California Annenberg School. Prior to her academic career, she spent several years as the film coordinator for the Zimbabwe International Film Festival Trust, a non-profit visual literacy organization in Harare, Zimbabwe. Twitter: @Amelia263

Asmolov, Gregory
Gregory Asmolov is a contributor to "Runet Echo", a project of "Global Voices Online" that analyzes the Russian Internet. He has consulted on information technology, new media, and social media projects for The World Bank and Internews Network, and worked as a research assistant at the Berkman Center for Internet and Society, Harvard University.

Gregory has taught two undergraduate classes at the Sammy Ofer Communication School at the Interdisciplinary Center in Herzliya (Israel), and lectures and conducts trainings about the social and political role of new media in U.S, Russia, Israel and other countries. Gregory has worked as a journalist for major Russian newspapers Kommersant and Novaya Gazeta, and served as news editor and analyst for Israeli TV.

Gregory is a co-founder of "Help Map", a crowdsourcing platform which was used to coordinate assistance to victims of wildfires in Russia in 2010 and won a Russian National Internet Award for best project in the "State and Society" category. Currently he and his colleagues are developing Rynda.org, a new crowdsourcing platform for coordination of mutual aid in crisis situations.
Gregory holds a MA in Global Communication from George Washington University (Washington, DC) and BA in Communication and International Affairs from the Hebrew University in Jerusalem. Twitter: @pustovek

Branco, Jr., Sérgio

Sérgio Branco, Jr., is a Member and Director at Institute of Technology and Society of Rio de Janeiro (ITS-Rio) and Vice-Director of the JD courses at the IBMEC University. Mr. Branco holds a Masters in Law and a Doctorate Degree in Civil Law from Rio de Janeiro State University (UERJ). He is a specialist in Cinema (Fundação Getulio Vargas-Rio) and in intellectual property (Pontifical Catholic University-Rio). Former researcher and project leader at the Center for Technology and Society at the Fundação Getulio Vargas School of Law in Rio de Janeiro (2005-2013). He is also a former chief-attorney of the Brazilian National Institute of Information Technology – ITI, in Brasilia (2005-2006). Lawyer (1997-present). Twitter: @sergiobranco

Calderaro, Andrea

Andrea Calderaro, PhD, is a researcher at the Centre for Media Freedom and Media Pluralism at the European University Institute. His research focuses on ICTs and International Politics. He works on the relation between ICTs and conflict transformation, and their opportunities to support resilience and enhance freedom of expression. His publications include the guest-editing of ‘Policy and Internet’ special issue on “Online Collective Action and Policy Chance” (2013), and the inaugural issue of the International Journal of E-Politics, IJEP - “E-Politics in a Global Context” (2010).

He serves as Chair of the ECPR Internet & Politics standing group, a member of the CSISAC board at the OECD, and he is an Executive Member of the International Communication Section of the International Studies Association. Previously, he has been Adjunct Professor at the University La Sapienza of Rome in “New Media and International Relations”, Visiting Fellow at the California Institute of Technology, and directed the “ICTs for the Global Governance of Peace and Security” Project at the University of Oslo (2012). He served as expert consultant to the European Commission, European Parliament, Tactical Technology Collective, and the OECD.

He holds his PhD and M.Phil in Internet and International Politics from the European University Institute. Twitter: @andreacalderaro
Carr, Madeline

Madeline has a background in new media and communications technology having worked at the forefront of print, film and web design in the private sector for many years. She received her PhD from the Australian National University's Department of International Relations and is now a lecturer in International Politics and the Cyber Dimension at Aberystwyth University. Madeline's past research has looked at the political history of the Internet, conceptions of power and cyber security, Internet governance and the global politics of network neutrality. Her PhD thesis, ‘The Irony of the Information Age: US Power and the Internet in International Relations’, engaged with core issues of state power, emerging technology and political decision-making. She is now focusing on the promotion of norms in and through the politics of Internet governance and the problem of state cooperation on cyber security.

Twitter: @MadelineCarr

Ellis, Steven

Steven M. Ellis coordinates press freedom activities in Europe and North America for the International Press Institute (IPI), the world’s oldest global press freedom organisation, representing editors, media executives and leading journalists. Before joining IPI he was a reporter for daily newspaper The Metropolitan News-Enterprise, covering courts and the legal community in Los Angeles. He graduated magna cum laude from the Michigan State University Detroit College of Law and is a licensed attorney in Illinois and Michigan, where he practiced law after serving as a legal clerk in the Office of Executive Counsel to the Governor of Michigan. He also holds a bachelor's degree in advertising and has worked in public and government relations. Twitter: @steven_m_ellis

Franklin, Marianne

Dr. Marianne Franklin has a background in History, Music, and Politics she has held teaching and research positions in Humanities, Social Science, and Engineering faculties; the University of Auckland (NZ), University of Amsterdam (NL), University for Humanistics (NL), and Columbia University (USA).

A recipient of research funding from the Social Science Research Council (USA) and Ford Foundation, her past and current research addresses these developments from the following angles: digital publics; power, resistance and the Internet; ICTs for Development and Internet Governance debates; diasporas, everyday life, and the web; transnational social movements online and on the ground; music, culture, and politics.

Co-Chair of the Internet Rights and Principles Dynamic Coalition at the UN Internet Governance Forum, she has also held office in other international associations; on the International Communications Section Executive and as Chair of the Feminist Theory and Gender Studies Section
of the International Studies Association. She is member of the international editorial board of Information, Communication and Society, the International Feminist Journal of Politics, and Review of Policy Research. Editor of the Key Thinkers: Past and Present series in Information, Communication, and Society 2006-2011, she was one of the founding co-editors of the RIPE Series in Global Political Economy (Routledge). Her latest book is Digital Dilemmas; Power, Resistance and the Internet (Oxford University Press, 2013). Twitter: @GloComm

**Fujii, Ko**
Ko Fujii is a consulting fellow at the PHP Institute, a Tokyo-based think tank. His research topic includes strategic global communications, public diplomacy, and media and Internet policy. As a public relations and government relations professional with strong focus on the tech sector, Ko was until very recently Head of Public Policy and Government Relations for Google in Japan. Before that, he was a public affairs consultant at FleishmanHillard Japan, representing in Tokyo some of the world’s largest tech/non-tech companies as well as public/nonprofit institutions. Policy areas of expertise include intellectual property, cyber security, free expression, cross-border data flows, privacy, competition, e-government, Internet governance, spectrum and broadband, digital diplomacy, and technology in disaster relief and rural development. Ko originally comes from the Japanese government, having worked for the Science and Technology Agency, the Agency for Cultural Affairs, and most recently the Ministry of Education, Culture, Sports, Science and Technology as Deputy Director for International Science and Technology Affairs. Ko has a bachelor’s degree in Law from the University of Tokyo, and an MBA from Kellogg School of Management at Northwestern University, majoring in Marketing and Public/Nonprofit Management.

**Gillwald, Alison**
Alison Gillwald is Executive Director of Research ICT Africa and Adjunct Professor at the University of Cape Town’s Graduate School of Business, Management of Infrastructure Reform and Regulation programme. Prior to this she was Associate Professor at the Witwatersrand University’s Graduate School of Public and Development Management, where she founded the Learning Information Networking and Knowledge (LINK) Centre in 1999 with the purposes of fast tracking ICT policy and regulatory training in Southern Africa. She did so after serving a term on the founding Council of the South African Telecommunications Regulatory Authority (SATRA). Before joining SATRA in 1997 she established the Independent Broadcasting Authority's Policy Department and was responsible for coordinating the Triple Inquiry into Public Service Broadcasting, Local Content and Cross-media Control. She was appointed to the African Ministers’ Advisory Group in 2000 and in 2002 she chaired the National Digital Advisory Body appointed by the Minister of Communication. She has served on the board of the public broadcaster, the South African Broadcasting Corporation, Womensnet and Media Monitoring Project and publicly-listed company AVUSA. She has consulted to infoDev, the African Development Bank, Government of Mauritius,
International Telecommunications Union, Commonwealth Telecommunications Organisation, United Nations Department of Economic and Social Affairs, the South African Presidency, Treasury, Department of Trade and Industry, and Competition Commission. She is founding editor of the Southern African Journal of Information and Communication and is published in the areas of telecommunications and broadcasting policy and regulation, gender and politics more broadly. She is on the review panels of several major ICT conferences including TPRC and ICTD and referees for the leading sector journals including Telecommunications Policy, Info and Communications & Strategies.

**Hill, Richard**

Richard Hill is the principal of Hill & Associates in Geneva, Switzerland. He has an extensive background in information systems, telecommunications, negotiation, mediation, and conflict management. Richard was the Secretary for the ITU-T Study Groups dealing with numbering and tariffing issues, network operations, and economic and policy issues; he was the Secretary for the preparatory process for the 2012 World Conference on International Telecommunications and headed the secretariat team dealing with substantive issues at the Conference. He has facilitated numerous complex international negotiations regarding sensitive policy matters.

He is a Centre for Dispute Resolution (CEDR) accredited mediator, has been trained as a mediator by the World Intellectual Property Organization (WIPO), has been trained and certified in family and victim-offender mediator and was for five years the labor-relations mediator at ITU. He has taken law courses in Geneva and Lausanne, and has attended, spoken at, and chaired seminars accredited for continuing education by the UK Law Society. He has published papers on mediation and computer-related intellectual property issues and the standard reference book to X.435.

In addition, Richard has a long professional background in Information Technology (IT) and Telecommunications. Richard holds a Ph.D. in Statistics from Harvard University and a B.S. in Mathematics from M.I.T. Prior to his studies in the U.S.A., he obtained the Maturita’ from the Liceo Scientifico A. Righi in Rome, Italy.

**Howard, Philip N.**

Philip N. Howard is a professor in the Department of Communication at the University of Washington and in the School of Public Policy at the Central European University. He directs the Digital Activism Research Project, the World Information Access Project and the Project on Information Technology and Political Islam. These research projects—supported by the National Science Foundation, US Institutes of Peace, and Intel’s People and Practices Group—investigate patterns of technology diffusion between and within developing countries and the role of new information technologies in political communication systems around the world.
His most recent books include *Democracy’s Fourth Wave? Digital Media and the Arab Spring* (New York, NY: Oxford University Press, 2012), *Castells and the Media* (London, UK: Polity, 2011) and *The Digital Origins of Dictatorship and Democracy* (New York, NY: Oxford University Press, 2010). He is the author of *New Media Campaigns and the Managed Citizen* (New York: Cambridge University Press, 2006), about how digital information technologies are used to manipulate public opinion in the United States. His books have won praise from across the social sciences, with awards from the American Political Science Association, the American Sociological Association, and the International Communication Association. He has edited *Society Online: The Internet in Context* (Thousand Oaks, CA: Sage, 2004, with Steve Jones) and the *Handbook of Internet Politics* (London: Routledge, 2008, with Andrew Chadwick). He has authored numerous journal articles examining the role of new information and communication technologies in politics and social development, including pieces in the *American Behavioral Scientist*, the *Annals of the American Academy of Political and Social Science*, and *New Media & Society*. He has worked on several NSF projects, serving on the advisory board of the Survey2000 and Survey2001 Projects, and co-managing a project about *Information and Communication Technologies in Central Asia*. He teaches courses on research methods, politics online, and international development. Howard has been a Fellow at the Pew Internet & American Life Project in Washington D.C., the LSE’s Stanhope Centre for Communications Policy Research, Stanford University’s Center for Advanced Study in the Behavioral Sciences, and is currently a fellow at Princeton University’s Center for Information Technology Policy. His BA is in political science from Innis College at the University of Toronto, his MSc is in economics from the London School of Economics, and his PhD is in sociology from Northwestern University. Twitter: @pnhoward

**Logan, Sarah**

Sarah is a PhD candidate in the Department of International Relations at the Australian National University (ANU), and was previously a visiting scholar at Columbia University and the London School of Economics and Political Science. Her thesis analyses counter-radicalisation policies in the United Kingdom and the United States and focuses on online counter-radicalisation. Sarah’s broader research interests revolve around the impact of the internet on international politics, especially the evolution of political community in international relations and the impact of ICT on political institutions in fragile states. She blogs at [www ircircuit com](http://www.ircircuit.com). Her work has been published by the Canadian International Council, the Lowy Institute’s Interpreter blog, Open Democracy, and ANU’s State, Society and Governance in Melanesia program. She presented on both viral hate speech and online counter-radicalisation at the UN Internet Governance Forum in 2012. Twitter: @circt
**McCarthy, Daniel**

Dr. Daniel McCarthy (PhD Aberystwyth 2011) is a Fellow in Global Politics in the Department of Government at the London School of Economics. He was previously an ESRC Postdoctoral Fellow at the University of Sussex and Lecturer in Security Studies in the Department of International Politics, Aberystwyth University. His research interests centre upon the role of technology and the non-human world in global politics.

His current research project explores the nature of technology as a form of institutional power in international politics through an examination of the Internet in American foreign policy. His other interests include theories of social property relations and uneven and combined development in International Relations, concepts of property in American foreign policy, and the relationship between culture and technology in processes of technological development. Twitter: @DRMcCarthy1

**Neudeck, Werner**

Werner Neudeck is the Dean for the Joint Postgraduate Program (MAIS) of the Diplomatic Academy of Vienna (DA) and the University of Vienna and a Professor of International Economics at the DA.

Upon graduation from the University of Vienna (Economics) Werner Neudeck pursued graduate studies at the University of Oxford and in 1980 was awarded a doctorate in Economics from the University of Vienna. He has been a Professor of International Economics at the University of Vienna, Webster University, Johns Hopkins University, SAIS Bologna Center and since 1997 at the Diplomatic Academy. From 1992-1999 he was the senior economist at the International Monetary Fund, Joint Vienna Institute. His research interests include health economics, history of economic thought, principal-agent theory, monetary economics and economics of the EU.

**Parker, Emily**

Emily Parker is the author of "Now I Know Who My Comrades Are: Voices From the Internet Underground" which will be published by Sarah Crichton Books/Farrar, Straus & Giroux in February, 2014. Emily is currently digital diplomacy advisor and senior fellow at the New America Foundation, where she has been writing her book and working on a US-China innovation project. Previously, Emily was a member of Secretary Clinton’s Policy Planning staff at the U.S. Department of State, where she covered 21st-century statecraft, innovation, and technology. While at State she advised on issues related to Internet freedom and open government, and traveled to the Middle East to explore the role of new media in post-revolutionary Egypt.

Emily is a founder of Code4Country, the first open government coding marathon between the
United States and Russia. Code4Country brought together Russian and American software developers to identify technological solutions to challenges of government transparency. Emily is a former International Affairs Fellow at the Council on Foreign Relations, an Arthur Ross Fellow at Asia Society's Center on U.S.-China Relations and a Global Policy Fellow at Carnegie Moscow Center, where she researched the role of blogging and social media in today's Russia.


Parmar, Sejal

Sejal Parmar joined the Legal Studies Department at the Central European University (CEU) in August 2012. Her research and teaching lie broadly in the field of international human rights law. Her current research focuses on the recent approach of UN human rights bodies, particularly the Human Rights Council and the Human Rights Committee, towards freedom of expression and its interplay with other rights such as equality and freedom of religion.

Prior to coming to the CEU, Sejal worked for over four and a half years as Senior Legal Officer at ARTICLE 19, the leading international human rights NGO on freedom of expression, and for two years as the Human Rights Coordinator at Doughty Street Chambers in London. She also taught international and European human rights law courses at Queen Mary, University of London and the University of Edinburgh. Previously, she held research positions at NYU Law School, the Amsterdam Centre for International Law and the University of Wisconsin, Madison.

Perl, Raphael

Raphael Francis Perl currently serves as the Executive Director of the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes at the George C. Marshall Center in Garmisch Partenkirchen, Germany. Prior to assuming his current position in December 2011, Dr. Perl held the position of Head of Anti-Terrorism Issues at the Organization for Security and Cooperation in Europe (OSCE) in Vienna, Austria. Prior to his assignment to the OSCE, Mr. Perl served as a senior national security policy analyst with the Congressional Research Service of the Library of Congress in Washington, D.C. A graduate of Georgetown University’s Foreign Service and Law Schools, he is the author of more than 100 congressional and academic publications, including *National Strategy for Combating Terrorism: Background and Issues for Congress* (Congressional Research Service CRS 2007), *Combating Terrorism: The Challenge of Measuring Effectiveness* (CRS 2007), *International Terrorism: Threat, Policy, and Response* (CRS, 2007), *Trends in Terrorism: 2006* (CRS, 2006), and

Dr. Perl speaks regularly at academic institutions and international and governmental policy fora; has testified before Congress on terrorism policy issues, including the 9/11 Commission Report recommendations; and has addressed the U.N. General Assembly on the role of regional organizations in implementing its global counter-terrorism strategy. As a fellow at the National Academy of Engineering, he was project director for an interdisciplinary team involved in assessing terrorist risk. Mr. Perl is a retired U.S. Army Reserve Colonel and National War College graduate with service in the Office of the Secretary of Defense.

Posch, Reinhard

Reinhard Posch received his PhD at Graz University of Technology, where he was appointed Full Professor in Applied Information Processing and Communications in 1984. He has served as Head of the Institute of Applied Information Processing and Communications Technology (IAIK-TU Graz) and Scientific Director of the Austrian Secure Information Technology Center (A-SIT) since 1986.

Since 2001, he is the Chief Information Officer (CIO) for the Federal Government of Austria, responsible for strategic coordination of activities in the field of ICT including all levels of government.

Professor Posch was named Chairman of the Board of Trustees of the Stiftung Secure Information and Communication Technologies (SIC) in Graz in 2003. From 2007 to 2011, he was Chairman of the Management Board of the European Network and Information Security Agency (ENISA), and in 2012 became Member of the IT Rat der Weisen, giving professional advice to European Commission Vice-Presidents Neelie Kroes and Maroš Šefčovič in the area of IT security and assisting in the implementation of the Digital Agenda for Europe. He is active in several European Commission committees; notably, he is a member of the steering board of the European Cloud Partnership. Professor Posch has been awarded the "IFIP Outstanding Service Award", the "IFIP SilverCore Award", the ID Peoples Award 2006 and the Grand Decoration of Honour in Silver for Services to the Republic of Austria, among many other honors. Twitter: @poschr

Powers, Shawn

Shawn Powers (PhD, University of Southern California) is an assistant professor in the Department of Communication at Georgia State University. His research specializes in international political communication with particular attention to the geopolitics of information and technology policy. Powers is a faculty affiliate of GSU’s Transcultural Violence and Conflict initiative and co-leads its’ British Council and U.S. Institute of Peace funded project on Civic Approaches to Religious Conflict. Powers is also an associate director at the Center for International Media Education where he co-directs an Open Society Foundations sponsored project on Critical Thinking in Iraqi High Education. In 2010, Powers helped launch GSU’s Global Business & Media program in Istanbul, Turkey and continues to oversee the initiative as co-director. Twitter: @shawnpowers
Price, Monroe

Monroe Price serves as Director of the Center for Global Communication Studies at the Annenberg School for Communication, University of Pennsylvania and Director of the Stanhope Centre for Communications Policy Research in London. Professor Price is the Joseph and Sadie Danciger Professor of Law and Director of the Howard M. Squadron Program in Law, Media and Society at the Cardozo School of Law, where he served as Dean from 1982 to 1991. He graduated magna cum laude from Yale, where he was executive editor of the Yale Law Journal. He clerked for Associate Justice Potter Stewart of the U.S. Supreme Court and was an assistant to Secretary of Labor W. Willard Wirtz. Price was founding director of the Program in Comparative Media Law and Policy at Wolfson College, Oxford, and a Member of the School of Social Sciences at the Institute for Advanced Study in Princeton. He was deputy director of California Indian Legal Services, one of the founders of the Native American Rights Fund, and author of Law and the American Indian. Among his many books are Media and Sovereignty; Television, The Public Sphere and National Identity; and a treatise on cable television.

Richter, Andrei

Andrei Richter (Andrey Rikhter) is the Director of the OSCE Office of the Representative on Freedom of the Media, and a professor at the School of Journalism, Moscow State University, where he teaches on mass media law. Born in Kharkov, Ukraine, in 1959, he has university degrees in law, foreign languages, and a doctorate in journalism. Richter was a commissioner of the International Commission of Jurists (ICJ) and the chair of the Law Section of the International Association for Media and Communication Research (IAMCR). Richter sits on editorial boards of a number of international journals on communications and the media. He has authored more than 200 publications on media law in Russian, English, Albanian, Armenian, Azeri, Bosnian, Tajik, Ukrainian, Serbian, Slovak, German and French, including the only standard media law textbook for journalism students of Russian colleges and universities (2002, 2009), a textbook on online media law (2014), as well as UNESCO-published textbook on international standards of media regulation (2011) and a book on censorship and freedom of the media in post-Soviet countries (in English, 2007).
Schulz, Wolfgang

Prof. Dr. Wolfgang Schulz studied Law and Journalism in Hamburg. Since 1997, he has taught the optional special subject on information and communication in the Department of Law at the University of Hamburg; he has been also a member of the state office for legal examinations since January 2000. In July 2009 he completed habilitation through the Faculty of Law at the University of Hamburg, and was granted Venia Legendi in public law, media law and legal philosophy.

Since November 2011, Professor Schultz has held the university professorship in "Media Law and Public Law including Theoretical Foundations" at the Faculty of Law at the University of Hamburg. This comprises a joint placement of the University of Hamburg and the Hans Bredow Institute. The focus of this professorship is on research at the Hans Bredow Institute. Prior to that, Professor Schulz acted as deputy business director as well as head of the Hans Bredow Institute's area of media and telecommunications, and has been a member of the board of directors since 2001. In February 2012 he was also appointed director at the Humboldt Institute for Internet and Society in Berlin.

His work emphasizes the freedom of communication, problems of legal regulation with regard to media contents, questions of law in new media, above all in digital television, and the legal bases of journalism, but also the jurisprudential bases of freedom of communication and the implications of the changing public sphere on law. In addition, he works on the forms taken by the State's functions, for instance, in the framework of concepts of "regulated self-regulation" of "informational regulation". Many of his projects are designed internationally comparative. Twitter: @WWSchulz

Shah, Nishant

Dr. Nishant Shah is the co-founder and Director-Research at the Centre for Internet and Society, Bangalore, India. He is an International Tandem Partner at the Centre for Digital Cultures, Leuphana University, Germany and a Knowledge Partner with the Hivos Knowledge Programme, The Netherlands. In these varied roles, he has been committed to producing infrastructure, frameworks and collaborations in the global south to understand and analyse the ways in which emergence and growth of digital technologies have shaped the contemporary social, political and cultural milieu. He is the editor for a series of monographs on 'Histories of Internet(s) in India' that looks at the complicated relationship that technologies have with questions of gender, sexuality, body, city, governance, archiving and gaming in a country like India. He is also the principle researcher for a research programme that produced the four-volume anthology 'Digital AlterNatives With a Cause?' that examines the ways in which young people’s relationship with digital technologies produces changes in their immediate environments.

His Ph.D. thesis builds a framework to examine the technosocial identities that are produced at the intersection of law, digital technologies and everyday cultural practices in emerging information societies like India. Nishant was an Asia Research fellow looking at the cost and infrastructure of building IT Cities like Shanghai. He is the author of a recent thought-piece titled ‘Whose Change is it Anyway? – Towards a future of digital technologies and citizen action in emerging information societies’ that seeks to revisit the debates around digital activism and change in the global context.
His current interests are in critically intervening in debates around Digital Humanities and conditions of change mediated by technologies.

Nishant is on the steering committee of the MacArthur Foundation’s Digital Media and Learning Project (USA) as well as on the Media Art Histories collective (Latvia). He has been deeply involved with the Inter-Asia Cultural Studies Consortium (Taiwan/S. Korea/Hong Kong) and is one of the key partners of the global Network of Centres for Internet and Society housed at the Berkman Centre for Internet & Society, USA. His work is committed to encouraging multi-stakeholder dialogue and hence he regularly does public consultations and trainings for civil society and NGOs, governments, academic partners and private corporate entities. He is a regular speaker at events like Republica and Video Vortex. He is a regular columnist with India’s leading English language newspaper The Indian Express. His academic and research publications reflect his political stance on open access and open knowledge infrastructure and are all available for free download and distribution under open license.

**Vincent, David**

David Vincent is Professor of Social History in the Department of History at the Open University. He was an undergraduate at the University of York and gained a PhD at Sidney Sussex College Cambridge. He became Lecturer in History at Keele University in 1974, leaving as Professor of Social History and Deputy Vice Chancellor in 2003 to take up the post of Pro Vice Chancellor (Strategy and External Affairs) at the OU. He became a full-time member of the History Department in 2010. He is a Visiting Fellow of Kellogg College, Oxford and a Fellow of the Royal Historical Society and the Royal Society of Arts.

Professor Vincent’s research interests cover working-class autobiography, British and European Literacy, and the cultural and political histories of secrecy and privacy. He is the author or editor of fifteen books, including The Culture of Secrecy: Britain, 1832-1998. His most recent work is I hope I don’t intrude: Privacy and its dilemmas since 1800. This explores the origins of modern debates about privacy through the prism of a fictional character, the eponymous hero of Paul Pry, a play first performed in 1825. He is now writing Privacy. A Short History (Polity) and preparing contributions to A History of English Autobiography (CUP) and for The Oxford Handbook of the History of Education (OUP). He has written on the historical context of the current controversies over government surveillance, including ‘Surveillance, Privacy and History’, History and Policy October 2013.

David Vincent is a member of the British and Irish History Research Group and the Localising Emotions Research Group.
Wagner, Ben

Ben Wagner is a post-doctoral fellow at The Annenberg School for Communication at University of Pennsylvania and is currently completing a PhD on the globalised governance of freedom of expression online at European University Institute in Florence. His research focuses on Internet Governance, digital foreign policy and human rights in the Middle East, Europe and North America and has been published in Telecommunications Policy, Politics, JITP and the International Journal of Communications.

Ben was previously a Visiting Fellow at Humboldt University in Berlin, the European Council on Foreign Relations and Human Rights Watch and studied in has studied political science and public administration in Munich, Leiden and Granada. In recent years he has also served as an academic expert for the European Commission, UNESCO, Hivos, the Open Society Institute and the European Parliament. Twitter: @benwagner_r

Zinovieva, Elena

Elena Zinovieva holds a PhD in Political Science and is Associate Professor at the Department of World Political Processes, MGIMO University. She is the author of several research articles and books about internet governance and cybersecurity, including "International Internet Governance: Conflict and Collaboration".
EMERGING SCHOLAR DELEGATES

Agur, Colin

Colin Agur is a PhD candidate in Communications at Columbia University's Graduate School of Journalism. His dissertation focuses on cultural and sociological aspects of mobile phone use in India. His research involves examination of policy documents (1991-present), interviews of policymakers, telecom executives and users, and observation of mobile phone use across India.

At Columbia, he developed and taught a course ("Mobile Revolutions: Markets, Politics, Journalism") that explored contemporary issues related to the mobile phone.

Since 2011, he has been a Visiting Fellow at Yale Law School's Information Society Project. His work there has focused on telephone surveillance and the Fourth Amendment. Twitter: @colinagur

Cho, Woon (Anthony)

Anthony (Woon) Cho is a M.A. student at The Fletcher School of Law and Diplomacy with a focus on international negotiation and conflict resolution in the East Asia region and current serves as a staff editor for The Fletcher Forum. His academic interests include public and private security, cyberspace relations, and U.S.-East Asia Relations. His recent research analyzed the cyber-attack strategies of North Korea and its implications for future negotiations. Prior to coming to The Fletcher School, Anthony received a Fulbright Grant to South Korea where he stayed for two years. He received his B.A. in International Studies at the University of North Carolina – Chapel Hill.

Clark, Rosemary

Rosemary Clark is a doctoral student at the Annenberg School for Communication and a 2013 graduate of Ursinus College, where she earned her Bachelor of Arts in Media & Communication Studies and English. Her research can be summarized as a twofold feminist approach to media activism. As an undergraduate student of feminist media studies, much of her research revolved around deconstructing mass media representations of women and girls using critical feminist frameworks. As an Annenberg student, her research has turned toward understanding how and why contemporary American feminists use digital space to mobilize direct action against disempowering media representations and to delineate the boundaries of their feminist
activist identities. Rosemary's work pairs traditional and new media studies with feminist and social movement theories and employs a range of methodologies, including textual and content analysis, discourse analysis, network analysis, and ethnography.

**McGuigan, Lee**

Lee McGuigan is a doctoral student in the Annenberg School for Communication. He studies the business and cultural histories of television and advertising, the sociology of markets and consumption, and the political economy of technology. He holds a Master's degree from the Faculty of Information and Media Studies at the University of Western Ontario. Lee is co-editor (with Vincent Manzerolle) of the book *The Audience Commodity in a Digital Age: Revisiting a Critical Theory of Commercial Media* (Peter Lang, 2014). His work has been published in *Television & New Media* and *the Journal of Communication Inquiry*. Lee comes from a fruit and vegetable farm in Cedar Springs, Ontario.

**Ralston, Robert**

Robert Ralston is a second-year Master’s student in the Department of Political Science at Virginia Tech. His research interests broadly include international relations, critical security studies, cyberpolitics, and surveillance. Robert is writing a thesis that examines state ontological insecurity with respect to cyberspace, and how state surveillance practices are justified through narratives of liberty and security. He is originally from Glasgow, Scotland. Twitter: [@RobertJRalston](http://twitter.com/RobertJRalston)

**Spagnolo, Ryan**

Ryan Spagnolo is a second year master's student and a Hitachi Center for Technology and International Affairs Scholar at The Fletcher School of Law and Diplomacy at Tufts University. His academic research focuses on multinational technology companies’ responses to government surveillance and global Internet governance challenges. Professionally, Ryan has previously worked as a marketing associate for Apprise Software and as a program officer for the American Bar Association’s Section of Administrative Law and Regulatory Practice in Washington, DC. He has also served as an Economic Sector intern for the U.S. Department of State Mission to the European Union. He holds a B.A. in History, *cum laude*, from Cornell University. Twitter: [@RyanSpagnolo](http://twitter.com/RyanSpagnolo)
**Vicentin, Diego**

Diego Vicentin is a Ph.D. candidate in Sociology at the University of Campinas (Brazil) and research fellow (2013-2014) in the Center for Information Technology Policy at Princeton University (USA). Diego has been studying the development history and the operation mode of cell phone networks by exploring its technical and political aspects. Currently he is investigating the intersection between politics and technology specifically with regard to decision-making related to the technical standards of mobile broadband networks. Twitter: @diego_jv

---

**Williamson, Willow**

Willow Williamson is an International Relations PhD student at American University in the School of International Service, where she received a MA in International Media. Her research is focused on public diplomacy, intercultural communication, gender, and technology. She has worked internationally in the fields of multimedia production, education, and computer science, participating in diverse projects that have brought her to Senegal, Turkey and Spain. She also holds a MFA in Composition and New Media from California Institute of the Arts and a BA in Music Composition and Media Technology from Mills College. Twitter: @willowfw
PARTICIPANTS FROM THE DIPLOMATIC ACADEMY OF VIENNA

Hardwick, Nicola

Nicola Hardwick is a second-year student of the Diplomatic Academy of Vienna’s MAIS programme. She received a BA in Politics and International Relations from the Royal Holloway College, University of London and a MSc in Global Governance and Diplomacy from St. Antony's College at the University of Oxford. She is the co-founder Royal Holloway Diplomatic Society and works as the Senior Assistant Editor for e-International Relations Online Journal (UK). She holds Austrian and UK citizenship.

Hooker, Catherine

Catherine Hooker, a US citizen, is a second-year student of the Diplomatic Academy of Vienna’s MAIS programme. She received a B.A. in Political Science & Germanic Studies and a B.F.A. in Fine Art Photography from Indiana University, as well as a number of scholarships and awards for academic excellence.

Iuga, Anamaria

Anamaria Iuga is a first-year Master’s student at the Diplomatic Academy of Vienna. She holds a BA in International Relations and European Studies from the Babeș-Bolyai University in Cluj-Napoca, Romania. She also served as the Chairperson of the European Students Society in Cluj-Napoca.
Kraus, Konstantin

Konstantin Kraus is an Environmental Technology and International Affairs student at the Diplomatic Academy of Vienna. He has worked for international organisations such as the World Economic Forum and the European Youth Parliament, as well as financial institutions including AXA Private Equity, Deutsche Bank, and Societe Generale. He holds a BA (Hons) in Economics and East European Studies from University College London and studied at MGIMO (Moscow State Institute of International Relations), Fudan University, and Peking University.

Lustig, Darrah

Darrah Lustig is a first-year Master’s student at the Diplomatic Academy of Vienna, where she studies International Relations. She also holds a MA in Comparative Literature from Dartmouth College. She hopes to enjoy a career at the intersection of her research and academic interests in public information and journalism. She holds a US as well as an Austrian citizenship.

McDowell, Kirsten

Kirsten McDowell is a second-year Master's student at the Diplomatic Academy of Vienna. Her research interests include security studies, nuclear nonproliferation, money laundering and drug trafficking. In addition to working for the Permanent Mission of Afghanistan, Kirsten is writing a thesis analyzing non-proliferation initiatives like the PSI and how they are being used to combat the proliferation of nuclear weapons. She is a native of New Jersey in the United States. Twitter: @KirMcDowell

Medvedeva, Anastasia

Anastasia Medvedeva is a first-year student of the Diplomatic Academy of Vienna's ETIA MSc Programme. She studied Psychology, English and French at the Moscow State Linguistic University, where she is also enrolled in a PhD programme. Her work experience includes the Russian Centre for Science and Culture and working for the Russia Today TV Channel.
Scholten, Jan Willem

Jan Willem Scholten is a second-year student of the Diplomatic Academy of Vienna’s MAIS programme. He attended Pre-University College – open to talented Dutch secondary school students – at the University of Leiden and holds a BA in Philosophy, Politics and Economics (PPE) from the Corpus Christi College of the University of Oxford. Among his extracurricular activities, he served as President of the Oxford International Relations Society and Oxford University Society of Bibliophiles. In 2009 he co-authored “Noughts and Crosses: An Assessment of Structures of Power between Journalism, Science and Politics” (Original title: Boter, kaas en eieren: Machtsverhoudingen tussen journalisten, wetenschappers en politici nader bekeken), Druno and Dekker Publishers, Noordwijkerhout, the Netherlands.

Tsiklis, Liudmila

Liudmila Tsiklis is a second-year student of the Diplomatic Academy of Vienna’s MAIS programme. She received a Bachelor of Commerce with Command of Foreign Languages (English and Italian) from the Moscow State Institute of International Relations (MGIMO University). For several years she also worked as a analyst at the Department of Development of International Projects at the JSC Audit-Consulting Group Business Systems Development.

Vićić, Jelena

Jelena Vićić is a first-year student of the Master of Advanced International Studies (MAIS) Programme at the Diplomatic Academy of Vienna. She holds a Bachelor of Arts ( Majors: Journalism and Mass Communication, Politics and International Relations) from the American University in Bulgaria. She also participated in an International Student Exchange Program at New Mexico State University. She holds a Serbian citizenship.
ABOUT THE ORGANIZERS

The American Austrian Foundation (AAF)

The American Austrian Foundation (AAF) was established in 1984, by a group of Americans and Austrians with an interest in promoting a positive relationship between the two countries. The AAF partners with NGOs, governments and individuals to bridge the gap between professionals in developed countries and countries in transition, by providing fellowships to attend post-graduate educational programs in medicine, media and the arts. The American Austrian Foundation is a public non-profit organization incorporated under the laws of Delaware and has 501(c) (3) status with the United States Internal Revenue Service.

Center for Global Communication Studies (CGCS) at the Annenberg School for Communication, University of Pennsylvania

The Center for Global Communication Studies (CGCS) is a leader in international education and training in comparative media law and policy. It affords students, academics, lawyers, regulators, civil society representatives and others the opportunity to evaluate and discuss comparative, global and international communications issues. Working with the Annenberg School, the University of Pennsylvania, and research centers, scholars and practitioners from around the world, CGCS provides research opportunities for graduate students; organizes conferences and trainings; and provides consulting and advisory assistance to academic centers, governments, and NGOs. CGCS draws on various disciplines, including law, political science, and international relations, among others. The Center's research and policy work addresses issues of media regulation, media and democracy, measuring and evaluation of media development programs, public service broadcasting, and the media's role in conflict and post-conflict environments.

The Diplomatic Academy of Vienna (DA)

The Diplomatic Academy of Vienna (DA) offers post-graduate training for the varied challenges of an international career. The DA equips its students with the academic qualifications, language training, intercultural competences and management skills, which are essential and often decisive prerequisites for many international professions and a subsequent interesting career. Furthermore, the DA offers a Summer Course for German as a foreign language and Austrian Studies. In addition to its study programmes, the DA organizes conferences and a great number of public lectures with well-known political, diplomatic, business and cultural figures. Publications of the DA ("Favorita Papers") offer substantive contributions from academicians taken from selected conferences in the field of international relations.
The Organizing Team

Arsenault, Amelia

Amelia Arsenault is an Assistant Professor of Communication at Georgia State University and serves as the Media and Democracy Research Fellow at the Center for Global Communication Studies at the University of Pennsylvania, Annenberg School. Her scholarly interests center on how different international and domestic actors have attempted to leverage the changing dynamics of communications systems, and the ramifications of those activities for international relations, political and social power relationships, and north/south inequality. In this capacity, she has conducted research on global media ownership, the impact of international donors in southern African communications development, network theory, new media, and public diplomacy. Her co-edited book The Connective Mindshift (with Rhonda Zaharna and Ali Fischer) on the subject of collaborative and networked public diplomacy was released in May 2013. Her scholarly work has appeared in the International Journal of Communication, International Sociology, The ANNALS of the American Academy of Political and Social Science, and Information, Communication, and Society. She holds a B.A. in Film and History from Dartmouth College and an MSc in Global Media and Communication from the London School of Economics and Political Science, and a PhD from the University of Southern California Annenberg School. Prior to her academic career, she spent several years as the film coordinator for the Zimbabwe International Film Festival Trust, a non-profit visual literacy organization in Harare, Zimbabwe. Twitter: @Amelia263

Eltz-Aulitzky, Katharine

Katharine Eltz-Aulitzky is the Executive Director of The American Austrian Foundation (AAF). The AAF has offices in New York, Vienna and Salzburg.

She oversees the AAF’s programs in medicine, media and the arts, and is responsible for fundraising and program content.
Price, Monroe

Monroe Price serves as Director of the Center for Global Communication Studies at the Annenberg School for Communication, University of Pennsylvania and Director of the Stanhope Centre for Communications Policy Research in London. Professor Price is the Joseph and Sadie Danciger Professor of Law and Director of the Howard M. Squadron Program in Law, Media and Society at the Cardozo School of Law, where he served as Dean from 1982 to 1991. He graduated magna cum laude from Yale, where he was executive editor of the Yale Law Journal. He clerked for Associate Justice Potter Stewart of the U.S. Supreme Court and was an assistant to Secretary of Labor W. Willard Wirtz.

Price was founding director of the Program in Comparative Media Law and Policy at Wolfson College, Oxford, and a Member of the School of Social Sciences at the Institute for Advanced Study in Princeton. He was deputy director of California Indian Legal Services, one of the founders of the Native American Rights Fund, and author of Law and the American Indian. Among his many books are Media and Sovereignty; Television, The Public Sphere and National Identity; and a treatise on cable television.

Neudeck, Werner

Werner Neudeck is the Dean for the Joint Postgraduate Program (MAIS) of the Diplomatic Academy of Vienna (DA) and the University of Vienna and a Professor of International Economics at the DA.

Upon graduation from the University of Vienna (Economics) Werner Neudeck pursued graduate studies at the University of Oxford and in 1980 was awarded a doctorate in Economics from the University of Vienna. He has been a Professor of International Economics at the University of Vienna, Webster University, Johns Hopkins University, SAIS Bologna Center and since 1997 at the Diplomatic Academy. From 1992-1999 he was the senior economist at the International Monetary Fund, Joint Vienna Institute. His research interests include health economics, history of economic thought, principal-agent theory, monetary economics and economics of the EU.

Wozonig, Nadja

Nadja Wozonig is the Assistant to the Director of the Diplomatic Academy of Vienna. She is also in charge of press and publications there.

She studied Political Science and Communication Science at the University of Vienna. Prior to her current position she worked on an EU Enlargement project, for the Austrian Parliament, ORF (Austrian Broadcasting Corporation) Enterprise, and some other projects. She joined the Diplomatic Academy of Vienna in September 2009.
ACKNOWLEDGEMENTS
We gratefully acknowledge the financial support provided by The Wolf Family Foundation, Organization of International Conferences Department of the Austrian Foreign Ministry, and The U.S. Embassy in Vienna. We appreciate the support given by the academic partner institutions and thank the panelists for donating their time. We would also like to thank Laura Schwartz-Henderson, Andrea Highbloom, and Ben Wagner at the Annenberg School for Communication; Nadja Wozonig at the Diplomatic Academy; and Sioban Healy at The American Austrian Foundation for their hard work in helping to organize the 2014 seminar.