Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2007, vol. 12, no.2
(http://www.arraydev.com/commerce/jibc/)

Book review

Internet Governance: An Introduction

Edited by Ravi Kumar Jain Bandamutha
2007 The Icfai University Press, Hyderabad, India.

First Author's Name: **Arthur J. Cordell, PhD**
First Author's Title/Affiliation: **Special Advisor, Electronic Commerce Branch, Industry Canada**
Postal Address: **300 Slater St., Ottawa, Ontario, Canada K1A 0C8**
Email: ***cordell.arthur@ic.gc.ca***
Brief Biographic Description: Dr. Cordell is an economist by training. He has a long-standing interest in computers and communications. He created the idea of the “bit tax”, which is a way of accessing the untapped productivity of a networked economy. He is interested in the social, political and economic implications of information technology. Dr. Cordell is also an Adjunct Professor at Carleton University in Ottawa, Canada.

Second Author's Name: **Prabir K. Neogi, Ph.D.**
Second Author's Title/Affiliation: **Special Advisor, Electronic Commerce Branch, Industry Canada**
Postal Address: **300 Slater St., Ottawa, Ontario, Canada K1A 0C8**
Email: ***neogi.prabir@ic.gc.ca***
Brief Biographic Description: Dr. Neogi is a civil engineer by training with an extensive background in the computer industry. He has been active in a broad area of computer related policy areas for the Government of Canada. Among these are: privacy, broadband, net-neutrality, internet governance, electronic commerce, etc. He is on th Program Committee of the Telecommunications Policy Research Conference www.tprc.org The TPRC, a non-profit organization**,** hosts an forum for scholars engaged in publishable research on policy-relevant telecommunications and information issues.

The purpose of annual conference is to acquaint policy makers with the best of recent research and to familiarize researchers with the knowledge needs of policy makers.

Abstract

Internet Governance: An Introduction offers a complete guide to the “ins and outs” of Internet governance. Drawing on a range of international authors Internet Governance is best suited for those seeking an overview of the range of issues involved as the Internet becomes increasingly important to business and to society in general, affecting the daily lives of millions of people around the world.

Keywords: **Internet, governance, trust, confidence, oversight**

INTRODUCTION

The strength of Internet Governance: An Introduction, its broad range, becomes its weakness however as issues of Internet governance are seen to be important to almost every aspect of life: from the technical to human rights to economic development. However the range of coverage is why these reviewers unreservedly recommend the book for those who want an introduction to the area, or for those who are now dealing with one or more aspects of Internet governance but who would like to broaden their area of research.

As the book adequately demonstrates, many of the technical issues around the net are now being managed (albeit sometimes in too central a fashion, ie., US centric) and the issue of free speech and possible censoring intervention by nation states is yet to be managed adequately. Some wonder if some of the issues can ever be managed well on the net. Human rights, for example, is difficult to deal with in the non-net world; in the global networked environment where transparency is often lacking the issue of human rights can become even more difficult to manage.

Central to the success of the net is, for these reviewers, the issue of trust and confidence.

TRUST AND CONFIDENCE: THE NEED FOR OVERSIGHT

The exchanges that take place between buyers and sellers of goods and services are the lifeblood of an economy, just as the exchanges that take place between citizens, their elected representatives and providers of public services are the lifeblood of a polity. For an economy or polity to work well, the parties to these different kinds of exchanges must trust each other and have confidence that the institutional framework within which they are operating is stable and that it will yield consistent, reliable and predictable results.

The combined forces of technological change and globalization pose dramatic new challenges for public policy. In some respects, the Internet is similar to other ubiquitous communications networks that came before it. Just like the postal system, the telegraph and the telephone, we have come to rely on the Internet as an infrastructure that enables individuals and organizations to conduct commerce nationally and abroad, through the transmission of information. Like these other trusted networks, as we grow to depend on the Internet, a degree of safety and reliability is expected and needed.

But there is a key difference. Previous transportation and communications networks were birthed under the watchful eyes of regulatory or legislative bodies, at the national level or through international agreements. Users of such networks could have a modicum of confidence that their mail would not be tampered with, that railway lines would be inspected and maintained to ensure the safe running of trains, and that aircraft would take off and land at airports in an orderly manner through the operation of an internationally coordinated air traffic system, because there were entities tasked with fulfilling these responsibilities and empowered to do so. We can refer to these entities as the “theys”. In most aspects of our lives there is a “they” that can intervene if rules, written or unwritten, are breached.

In the early days of the Internet (before the name Internet was even coined), development and use was characterized by a small group of academics and researchers who knew each other and formed a community of interest. As in any typical small community, behaviour on the net was self-regulating. While a small town needs a sheriff as final law officer, the closeness of inhabitants means that people will behave in ways that seek to avoid shame for themselves and their families. As communities grow there is a concomitant growth in anonymity. Anonymity allows for behaviour that might be unthinkable in a small community. The old adage “A change in quantity leads to a change in quality” applies to communities and applies to the net as well. When the net was a small group, self-regulation was adequate. When a community is small it too is largely self-regulating. When the community grows to a large city there is a need for both regulation and enforcement. There is a need for oversight and sanctions, where needed

The Internet has evolved at an unprecedented rate and since it consists of an agglomeration of autonomous networks bound together by the Internet Protocol, it has characteristics quite unlike those of the earlier trusted networks. One characteristic of the public Internet is that, since it consists of many thousands of autonomous networks spanning a large number of jurisdictions, it has no well defined “they”. There is no gatekeeper or “watchdog” person or agency to oversee activities on the Internet: a “they” that can step in when governance or “policing” is necessary to curb inappropriate or criminal use. While users may think that Internet Service Providers (ISPs) are tasked with this responsibility, it is not clear that they are empowered to do so or are even required by law in various jurisdictions.

As the Internet has grown a fundamental problem has been exposed: it is virtually impossible to regulate or enforce the behaviour of users. With all previous networks there has been an enforcement mechanism to provide sanctions where misbehaviour or outright criminal activities take place. In the world created by the automobile, society learned early on that both the drivers and their vehicles needed to be licensed, and rules of the road created and enforced for public safety and security. Network after network (rail, airlines, telecommunications, broadcasting, etc.) all have a "they". A “they” as in: "if you break the law, they will (take away your license, send you to jail, issue a fine, etc.).

Governance is therefore presented with a wholly unique situation. Society has ramped up a small research network into a global “network of networks” with some 1 billion users in some 200 countries, that is increasingly critical to national and global economic well-being, and there is no “they”. There is no mechanism for regulation or enforcement. There are local "theys". But their power is limited to one or a few jurisdictions. It is a profound challenge to retrofit this necessary functionality while the Internet continues to expand rapidly and its proponents try to accelerate its adoption and use by increasing numbers of unsophisticated users.

Governments and policy makers around the world are slowly getting used to the fact that the public space of the Internet can be a “dark and dangerous” street with many unsavoury actors wanting to cheat us (with scams) threaten us (with cyber-crimes like fraud, identity theft, etc), harass us (with spam) or otherwise grab our attention Cyber citizens are traversing this public space with increasing care and some are deciding not to enter this public space at all. Some are choosing not to go online, even to go to a secure private space. There is concern that the security of the private space in the cyber-world does not bear the same resemblance to the security of the private space in the industrial world. For many, online banking does not offer the same sort of trust and confidence as “bricks and mortar” banking. Online shopping, while convenient, means giving up credit card information to the uncertainty of cyber-space.

Spam has become a significant worldwide problem that clogs networks, consumes resources and, due to its implication in virus distribution, identity theft facilitation and other criminal activities, significantly erodes trust in electronic commerce. If left unchecked, spam could bring the Internet to its knees. Cyber-crime, Internet fraud and identity theft are likely to become even more serious problems. Cyber-crime could become the Achilles heel of the global electronic payments system.

Governance issues take on a sense of urgency. A technical solution such as linking individuals to unique IP addresses is compelling. However, unless there is an oversight mechanism, a “they”, to administer sanctions as necessary, such a fix will not solve the problems. Needed is a marriage of the technical to the institutional that will provide the oversight necessary, the oversight that can allow for effective governance.

The historical role of governments in ensuring the orderly implementation of broad, general purpose technologies which are enabling and transformative in nature is well-known. One need only consider the extensive frameworks of legislation and ways of behaving that surround railroads, postal systems, electricity, the telephone and the automobile. The Internet is a new entrant. And there is a great need for innovative thinking and policy making if the thorny issues of governance are to be adequately addressed.

The task of building an environment of trust in the digital economy is complex. What makes it particularly difficult is to try to do it in “Internet time”, as opposed to the slow, organic way in which the previous industrial infrastructure of trust was developed. Added to this, society is trying to retrofit a host of security features into an open system, the Internet, a system designed for convenience, research and ease of use. It is like building a community without locks anywhere and suddenly learning that locks on doors, on stores, on banks - locks and security are needed everywhere. The additional constraint is that a retrofit is needed as soon as possible, and that all players should "more or less" agree on the nature of the retrofit !

CONCLUSION

Much has been made of the uniqueness of the Internet. The new world of information technology. It has been claimed that this new world will be new and novel and unlike anything that has come before. This is only partially true. The technology is new but the need for trust and confidence remains the same. Governance will have to ensure that the trust and confidence of the “bricks and mortar” world is matched in the online Internet world. For the Internet to achieve its maximum social and political potential there will have to be agreed upon and effective rules of the road, both nationally and globally. This new technology will have its own unique regulatory framework, but it will only flourish if there is some agreement and acceptance of both broad and specific governance approaches aimed at buttressing the vital areas of trust and confidence.