From Civil to Cyber Rights

A perspective on cyber policy challenges in our connected world

Michael Litherland and Matt Bross
IP Partners Ltd. USA, London, Hong Kong.

***Abstract*— This paper provides a very basic examination of the challenges to ensure parity and fairness in the management and application of national, regional and global cyber policies regarding the collection and protection of personal and commercial data.**

We review the evolutionary impact of the digital world along with the phenomenal growth and economic power associated with it. This includes comparative positioning of the legal and technological challenges faced by many governments to provide comprehensive cyber policies and protections while simultaneously ensuring that privacy and freedom of internet users is respected.

A suggestion for a structured transnational approach to provide a common framework layer for cyber policy alignment and a system for reporting and arbitrating cross-border cyber infractions and differences in policies and standards is provided.

Keywords- Civil Rights, Cyber Rights, Cyber Policy, Cybersecurity, Social Media, Machine to Machine (M2M), Mobile Internet, Big Data, Analytics

I. INTRODUCTION

The world as many of us knew it doesn't exist anymore. A typical mobile internet user can carry their personal and direct access into the vast digital world right in their pocket or purse. Advanced communications technologies have connected people and businesses around the globe enabling an individual to quickly reach across vast distances, borders and cultures to engage and interact instantly with someone else.

Along with the benefits that personal global cyber access provides comes many risks and responsibilities across many sectors. Our intent is to examine the roles and responsibilities in our digital world, the value and impacts on users, and to suggest a possible collaborative method to ensure the balance between providing a safe internet enabled experience and protecting the privacy of individuals is respected and that a set of basic cyber rights can be established to provide guidance in promoting fair and open collaboration for common shared policies, measurements and reporting for this valuable global phenomena.

II. THE PLAYING FIELD

A. *The Connected World*

The evolution of technology and applications through mobility and cloud access has transformed cyberspace enabled society into the mobile internet enabled "pocket state" whereas any desired communications whether to another person, business or a social media sphere of influence is always on and instantly available. This communication reach between parties goes both ways and the activities and preferences of individual users and selected groups and demographics are collected, analyzed and profiled to provide commercial marketing intelligence and other statistically driven user data profile driven actions including government related surveillance.

B. *The Internet Economy and You*

The internet ecosystem is growing into the world's 5th largest economy reaching $4.2 trillion dollars by 2016 [1] and 3.6 billion users by 2017 [2]. This rapid growth of cyberspace and our reliance on it is based on affordable accessibility, ease of use and growing confidence to rely on its tools and applications for many aspects of our personal and professional lives.

Fig. 1. The Global Internet Economy

Cyberspace has become an integral enabler across private and public segments including financial, utilities, education, manufacturing, energy, health and is becoming more persuasive due to the rapidly growing machine-to-machine (M2M) and cloud communications infrastructure. In a nutshell, the internet has become the very foundation for the economic and operational viability of many nations. Therefore, the entity of cyberspace is leveraged, protected, used and at times abused

in respect to the wide ranging capabilities it provides to individuals, commercial and government sectors.

C. *The Data Value of the "Netizen"*

A "Netizen" is in effect "*the digital persona of you*" in cyberspace. For every moment you interact with the internet either directly or indirectly, your engagement for online activities, locations and opinions are linked to your unique user profile and it generates vast amounts of data regarding you as an individual which is then harvested and contributed to a wide array of statistical engines distributed among service providers, marketing firms and government entities. Over a cyber lifetime, your activities online will provide information that is widely used to determine direct and indirect marketing campaigns, political decisions, health, finance and other targeted demographic based issues. This information can be used for beneficial reasons but also abused as well.

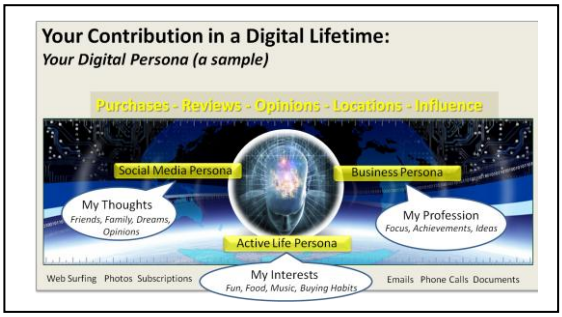

Fig. 2. Your Digital Persona

D. *Competing Interests in Cyberspace*

As a result of the growth and reliance on cyberspace, enormous amounts of private and commercial data are placed at risk for misuse and abuse. The direct and indirect responsibility and accountability to ensure the integrity and safety of cyberspace has become a growing competitive advantage on both the national and commercial landscape despite many attempts to establish collaborative ways for groups to meet and share strategies for prevention and management of cyber risks.

Finding the right balance to achieve that proactive protection mechanisms are in place while ensuring the privacy for the individuals and commercial interests involved are sometimes in conflict with the ambitions and requirements of government entities. While we do not debate the merits or strategy of the government entities capturing or harvesting the data, it is apparent that stronger guidance and oversight is needed with clearer rules of engagement for such activities especially when it is executed across national borders.

III. CYBER RIGHTS AND THE CONFIDENCE GAP

To provide a perspective on the future we can reflect on the past. Civil rights conveyed the following basic tenets towards an individual:

"Civil and political rights are a class of rights that protect individuals' freedom from infringement by governments and private organizations, and ensure one's ability to participate in the civil and political life of the state without discrimination or repression." [3]

How would that apply those tenets to Cyber Rights? The challenge we all face is that upon entering cyberspace we are in effect operating in a borderless world where an expectation of privacy and freedom are desired and expected but not always respected.

Both good and bad actors have generally unfettered access to reach across the globe to engage and interact with individuals, commercial and government entities. Tools, applications and processes are put in place to help mitigate cyber risk but we still find that government directed privacy breach incursions and criminal activity finds a way to interject itself at local, national and international levels. These issues continue to create a growing gap in confidence towards certain commercial and government entities which diminishes the view that open cooperation between governments will provide a fair and equitable path forward.

As a Netizen the confidence gap is becoming greater because as an individual reading the variety of headlined stories on commercial security breaches of personal information and reports of different types of government intrusions into privacy and wide spread data mining of user information you aren't really sure who you can trust.

A. *The Cyber Policy Loop*

Over the last decade there have been many advances in technology that has extended the reach of cyberspace into all aspects of our private and professional lives. The mechanisms to provide essential cyber policies which in turn focus on safety and integrity of the systems, processes and activities which happen there are evolving to meet the technology challenges posed by this vast expansion of cyberspace. Government agencies have applied laws and regulations to stem the tide of online criminal activities and to also harvest available internet driven revenue sources when possible for economic benefit. These varied collections of cyber policies and laws are generally focused on the "national interest" of the originator thus end or extend across borders and create potential conflicts.

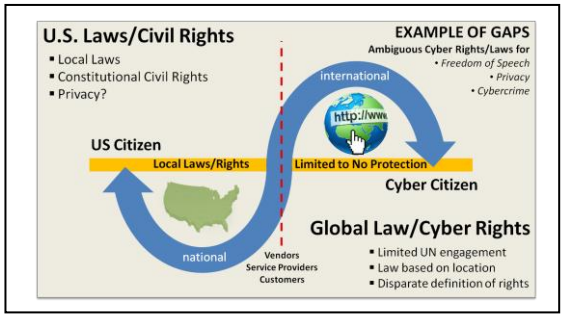

Fig. 3. The Cyber Rights Policy Gap Challenge (U.S. Example)

When considering the application of cyber policies, laws and regulations the background of the technology itself, how it is used individually, commercially and by governments is taken into account. Depending on your reference point, the application and appropriate execution and measurement of cyber security and cyber policy compliance is achieved through either government level or commercially driven mechanisms.

For example a brief summary of several types of policies treaties, standards and requirements and their general intent are:

- International Cyber Security Treaties - define a scope of expected engagement norms and rules between nations
- National Cyber Security Policies - defined at a Government level
- IT (Cyber) Security Policies - defined at a corporate or institutional level
- Cyber Security Standards - agreed at a collective level for a given technology or process and provides a guideline specification for meeting a set or subset of requirements
- Cyber Security Requirements - required to meet minimum operational acceptance and included as part of commercial agreements

At this point many governments and agencies have issued or updated their cyber strategies. The European Union Agency for IT Security (ENSIA) has listed them from around the world [4].

Country	Security Strategy/Date
Austria	Austrian Cyber Security Strategy (2013)
Czech Republic	Cyber Security Strategy of Czech Republic for the 2011-2015 Period (2011)
Estonia	Estonian Cyber Security Strategy (2008)
Finland	Finland's Cyber Security Strategy (2013)
France	Information systems defence and security, France's strategy (2011)
Germany	Cyber Security Strategy for Germany (2011)
Hungary	Hungary National Cyber Security Strategy (2013)
Lithuania	Programme for the development of electronic information security (cyber security) for 2011-2019
Luxembourg	National strategy on cyber security (2011)
The Netherlands	The national cyber security strategy (2011)
Poland	Govermental Program for Protection of Cyberspace for the years 2011-2016 (2011)
Romania	Cyber Security Strategy in Romania (2011)
Slovak Republic	National Strategy for Information security in the Slovak Republic (2008)
United Kingdom	Cyber Security Strategy of the United Kingdom
Australia	Australia Cyber Security Strategy (2011)
Canada	Canada's cyber security strategy (2010)
India	India National Cyber Security Strategy (2013)
Japan	Japan Information Security Strategy for protecting the nation (2010)
New Zealand	New Zealand Cyber Security Strategy (2011)
Norway	Norway National Strategy for Information Security (2012)
Russian Federation	The Information Security Doctrine of the Russian Federation (2000)
South Africa	Cyber Security policy of South Africa (2010)
Switzerland	National strategy for Switzerlands's protection against cyber risks (2012)
United States	U.S. International Strategy for cyberspace (2011)

While only a sampling, most of these national Cyber Security strategies have common themes and ideas but those generally end at the border of that nation and their area of interests.

The United Nations has recently organized and convened a forum on Internet Governance in Bali during October 2013. This is a new initiative focused on multi-national Cyber policy. [5].

B. Finding a Collective Path Forward

If you take the variety of cyber policies created and published around the world at a national level and sit with a highlighter to compare and contrast the similarities versus differences in each it becomes very evident that the common ideas for cyber policies and strategies far outnumber the differences. So the challenge is, why can't we agree on a common international version of the same guidelines and policies as a framework for the future of cyberspace?

There have been several attempts by private groups and forums to generate a common thread of cooperative international cyber policy for cyberspace but even these have struggled to reach beyond the forum idea stage due to the resistance or inability of governments and certain industries to accept or be bound by a set of cyber guidelines that may be in conflict with their own self-interests. These competing interests and policies represent yet another challenge but within those collective groups of cyber focused policies and laws, many common threads do exist and it is paramount to find and negotiate a clear path forward to bring a mechanism in place that leverages the best practices and methodology of each contribution into a single cohesive cyber framework that is acceptable to all.

A framework describing the potential core areas of focus for an international resolution or treaty between nations for Cyberspace was outlined in: Cybersecurity Treaties - a Skeptics View [6], as follows:

- limits what states can do to one another in the cyber realm
- Imposes on them duties to ensure that private actors within their borders do not engage in certain bad cyber acts
- Establishes mechanisms of interstate cooperation to track and redress malicious cyber operations
- Clarifies definitions (such as which acts constitute war and various crimes) in order to prevent mistaken interpretations and prevent misunderstanding or escalation
- Creates an international organization to facilitate cooperation and monitoring

What is still missing in this and other areas of policy and strategic focus on Cyberspace is the formal terms of reference for protecting the individual rights (privacy and freedom) of the internet users (Netizens) themselves.

The key issue is that Cyber rights are a different animal altogether from the technological, crime and national security

focus for many groups but some considerations of protection and rights should be accounted for. There are several groups discussing these core issues. For example, Computer Professionals for Social Responsibility (CSPR) [7] are working on the tenets of basic cyber rights. The CSPR cyber rights working group is seeking the following agreement for basic user cyber rights:

- The right to assemble in online communities
- The right to speak freely
- The right to privacy online
- The right to access regardless of income, location, or disability

Cyber rights are one gap that needs further development and inclusion into the broader discussion for international norms for Cyberspace. We propose that any future discussions should include the scope of an individual's "cyber rights" as an integral piece of any future international cyber treaty, resolution or policy.

IV. CONCLUSIONS

As we have seen by the recent releases of information regarding surveillance programs both in-country and internationally, the desired cyber right to privacy is sometimes usurped by the determined greater good for personal safety and proactive reduction of risk. When directed by the appropriate courts, privacy intrusion can be accomplished in a manner consistent with the protection of due-process and fairness under the law especially in criminal cases, child pornography, terrorism and other illegal activities. The debate of how much is too much and how far is too far when initiating and executing the surveillance programs is a debate that is still ongoing and a point of great contention both locally and internationally. In addition, the commercial collection, harvesting and sharing of personal information is also being contested and viewed as a unwarranted or unapproved intrusion into personal lives. The balance between national security interests, commercial data acquisition and respecting personal privacy must be found,.

Cyber security and supporting technology standards as a whole are being addressed across a wide spectrum of commercially driven activities in cooperation with government entities. The need to address the wider ranging issue of Cyber Privacy (Cyber Rights) and associated policies is still very fragmented due to national level concerns and interests. There is a need for a private (commercially) led activity to drive the privacy and rights aspects of cyberspace in cooperation with leading governments to secure a common framework. This can be accomplished in part through the activities promoted by the EWI Cyber40 group and supplemented with direct engagement with the appropriate groups within the international community to establish a legally acceptable international framework (agreement in principle) and forward it for consideration.

ACKNOWLEDGMENT

In appreciation to the East-West Institute (EWI) Cyber40 members and active representatives who continue to lead the way in promoting a fair and equitable path forward for Cyber Security strategic policy issues worldwide.

REFERENCES

[1] Boston Consulting Group Report on Internet Economy [March 2012].
[2] Cisco Systems Internet Usage Projection [May 2013]
[3] Summary Definition of US Civil Rights. Wikipedia [Oct 2013]
[4] The EU Agency for IT Security (ENSIA) National Cyber Strategy List
[5] UN forum on Internet Governance [First session Oct 2013]
[6] Cybersecurity Treaties, a Skeptics View. Jack Goldsmith, Stanford edu
[7] Computer Professionals for Social Responsibility (CPSR.ORG)