Expert Meeting on

CYBERLAWS AND REGULATIONS FOR ENHANCING E-COMMERCE:

INCLUDING CASE STUDIES AND LESSONS LEARNED

25-27 March 2015

Beyond Cyberlaws and Regulations for Enhancing E-Commerce and Trust in the Digital Communication of the Future

By

Thomas Andersson

President

International Organization for Knowledge Economy and Enterprise Development

Beyond Cyberlaws and Regulations for Enhancing E-commerce and Trust in the Digital Communication of the Future

Thomas Andersson[1]

International Organization for Knowledge Economy and Enterprise Development

1. Introduction

Congratulations to UNCTAD for organising this event on issues that are of central importance for enabling higher level of trust and realising the potential opportunities now at hand in electronic commerce worldwide. The issues raised here today are certainly not new but their importance keeps rising and the challenges are about to take new shape.

Let me first briefly reflect on the need for creating trust online, and particularly in view of the rise under way of big data, the Internet of things and cloud computing! We will then turn to the current state of play with regard to handling some of the most pressing issues in this area. Third we discuss what is needed, beyond regulatory and legislative work, to address the issues of cyber-security, privacy and data-governance.

2. Introduction

First of all, it is worthwhile to consider why we have a problem in the first place. Many would perhaps think this is because of unresolved regulatory and legal issues. While there is some truth to that, most fundamentally the reason for trouble is a growing disconnect between the expanding benefits from massive collection, storage and processing of personal data, on the one hand, and the lack of responses on the part of users or service providers to protect privacy, on the other hand.

We may think it is OK for us to continue with "business as usual". Let me be clear, that is NOT a viable strategy any more. Traditional systems for identity management and data governance have reached their limit. Individual users run into a myriad of diverse identity issues every day. Not only does this result in unwanted outcomes

[1] The author is President of the International Organisation for Knowledge Economy and Enterprise Development (IKED) and can be contacted at thomas.andersson@iked.org. Among other assignments, he is also the Chairman of the GINI (Global Identity Networking of Individuals) consortium, previously a support action with the European Commission on identity management in digital communications.

and negative experiences. As a result, we have massive distortions in behavior, including resistance to using your credit card and engaging in electronic commerce in many situations when that could have realized major benefits.

We observe severe barriers and challenges for manufacturers and vendors, with the consequences more serious where compromising trust is more delicate, and in activities and environments that are particularly vulnerable to costly security breaches and misuse of data.

With Convergence, Big Data, Cloud Computing, the Internet of Things, massively enhanced Broadband and Computational Capacity, we are moving into a new situation. With seamless interactive communication, constant processing of authentication and authorization in-real-time, encompassing billions of users and trillions of devices, a wealth of new services stands to be developed and scaled in ways never seen before. These are set to take advantages of opportunities for two-way interactive information exchange, activating users, consumers and citizens to identity outstanding issues and be part of formulating responses - partly through behavioural adjustments - enabling previously unthinkable improvements in health, education/learning processes, commerce, transport and logistics systems, and so forth.

Some of this is now happening within the context of smart cities. In Europe, some 90% of all European cities with more than half a million habitants have already developed such agendas, according to a recent report for the European Parliament. While the same may be true of the United States and other developed countries, a similar development is under way across Asia, the Middle East, Africa, and elsewhere. The reason why we see such action at the City level is probably because this offers an appropriate proximity to clusters and individual communities and companies, while also faced with a tangible responsibility to resolve and act on outstanding issues. The nation state, by contrast, tends to be bogged down in more heavy-handed policy processes and also - in some sense - more abstract and over-arching considerations which are not easily resolved, as we will come back to. The smart city interacts in turn with smart cars, smart buildings, smart offices. In all this, the ability to measure, share, and respond to real-life developments in real-time, on terms that are acceptable to all, and enable trust, is essential for what progress can be made.

Today, when there is a security breach, money is lost in your bank account. Or, perhaps a competitor gains inside information and will grab a deal at your expense. Such consequences are already troubling. But, in the world under way, your car may be gone at the time you arrive at the parking lot in the morning, or the car or the refrigerator will kill you in action, when somebody else gains control of the vehicle or device you depend on.

Already today it is increasingly problematic for financial and other sectors to insure and protect themselves against the risks of cybercrime taking advantage of security glitches. In the world under way, unless there is effective counter-action, it will become impossible.

3. Current State of Play

So what is the current state of play with regard to handling identity management, privacy, security and trust for online commercial transactions? Of course, a range of factors are at work here, including legal, technological, and economic ones.
Many countries have worked hard to develop ambitious e-ID solutions, to provide an identity assurance that is sufficiently reliable to match with various needed purposes. The trend is for such policies to become more conducive to innovation and increase responsiveness to changing market conditions.

There has also been extensive multilateral effort, in the OECD, the ITU, UNCTAD and elsewhere to work out common principles and approaches capable of transcending national borders.

Despite these efforts, ongoing since more than 15 years, identity management in the digital world is marked by fragmentation, the consequences of which - if anything - are worsening by the day. They include violation of minimum disclosure principles, data-use beyond its original purpose, and lack of user control for privacy preservation, with users unaware how their private information is put to use.

Many providers of digital services traditionally follow the “lock-in” principle concerning users’ data and information. Users are "forced" to register at each service provider and get stuck with a multitude of partial identities, many of which will soon be outdated while mechanisms are lacking for enacting their removal or invalidation.

The consequences worsen the more valuable the transactions and the more vulnerable the subjects involved, and the more dependent we become on online services.

As a result, today's environment for digital communication is marked by serious gaps in security, privacy, trust, and usability. In the struggle to cope with it all, we observe troubling trade-offs, e.g. between privacy and security, and between usability and security.

Part of the problem has to do with the genuine cross-border nature of the digital world. Identity management must work out and accommodate discrepancies between multiple jurisdictions. Gone are the days when the OECD dominated this area. There is now a tidal wave of new users in emerging and developing countries going on line notably through mobile communication. The obstacles to securing trusted and efficient cross-border trade is, however, holding back the potential for vibrant electronic commerce and digital exchange especially among this wider circle of new players. The ability to address the cross-border issues at hand will thus be essential for capturing future opportunities especially for developing and emerging economies.

As a second explanation, technical progress is moving so much faster than policy. This implies that there is no way for the policy-making process to provide detailed relevant regulation and standardization suitable for coping with the precise needs of technologies or markets over time (a policy that may look right at one point may subsequently appear as a source of distraction, distortion and impediment to new solutions).

Third, resolving the issues inherently requires the involvement of multiple stakeholders. Users, for instance, interact in various capacities, as citizens, customers, employees, employers, service providers or identity providers, with a multitude of specific needs and requirements at stake. Relying parties and data bases are likewise affected in multiple ways. Different kinds of operators influence what can be done and need to be part of any viable solution.

We are thus, in effect, in a stage of complexity which threatens to become untenable. The situation cannot be resolved by traditional legal and regulatory responses alone.

4. Need of Coherent Actions

So, what actions are needed - beyond adopting relevant legislation - to address the issues of cybercrime, privacy and data protection across jurisdictions, and notably so in the world that is under way?

Surely, a lot is required. Consider the following needs:

- Creating conditions that are more conducive to interoperability and coordination,
- Putting in place effective collaboration to back a coherent system for electronic identities, apt to handling derived identities, operating for humans as well as for devices.
- Ensuring trust interoperability between Cryptographic Rootkeys.
- Paving the way for trusted search and other e-services, operating across sectoral and national boundaries.

But, above all, we must reduce uncertainty and build trust by enabling users to access digital services on more understandable conditions, offering them a fair sense of control, a say, and a share in the returns to the value of their personal information, I would argue this is a prerequisite for capturing the opportunities at hand, and to steer away from chaos. In other words, the key task has to do with:

- putting users more in control of their digital identity, including what data they share, and of their privacy.

Why then is that such a problem, and what is required to improve the situation? Following years of combined research and consultations, the so-called GINI project[2] concluded:

-- Users today do not have the means to articulate demands for security and trust, and they are lacking information on the way their private information is currently used and for what purposes.

[2] The GINI (Global Identity Networking of Individuals) consortium is a previous support action with the European Commission which is currently in a stage of implementation, entailing various initiatives to instill concrete action in support of orderly identity management and trust in digital communication. See further www.gini-sa.eu

-- While users are in need of professional services support in order to gain control of, and a return from, use of their private information, currently viable business cases are basically lacking, hampering the rise of operators offering users the tools required for managing orderly choices in this regard.

It was further concluded that users should be able to:

- Decouple the activation of digital identities from any particular identifier, and to support the use of multiple identities and/or identifiers.
- Exercise full control as to who is able to verify their identities and through which processes.
- Have control of every phase of their digital identities' life cycle (creation, change, management, revocation, etc.).

Ways should be identified to support the rise of a wider identity ecosystem linding support to a strengthened position for users along these lines. This, in turn, requires setting in motion a *process* for several initiatives to be taken in parallel, to underpin the development of a coherent ecosystem in which users as well as relying parties and data bases are able to collaborate around the provision of viable identity management services. Effective work on regulations and standards capable of sustaining interoperability, while technology-neutral and prone to competition and innovation, are an important building block. Progress in the development of such standards can partly be achieved by industry itself, and in some instances by individual countries - or groups of countries, as in the European Union or other regions - spurring progress as forerunners. At the same time, in the stage where we now find ourselves, we cannot afford to fall short of better mechanisms for seamless cross-border solutions with global reach.

More development work and experimentation are needed in formulating the indicated user requirements, a sort of procurement strategy that must entail effective stakeholder participation, backed by incentives that bite along with monitoring and certification mechanisms that are lending credibility and enabling trust. It is thus important for policymakers to increase their effort to spur innovation in this area, while looking for ways to exchange experience and collaborate in the international area, including through standard and regulatory reforms that are open-ended but conducive to the application and diffusion of solutions that strengthen user-control and trust.

Why, if this is possible, have such initiatives not already been taken? Overcoming the present fragmentation in identity management is, in fact, a daunting task. The costs of not acting are however about to increase dramatically and more and more players are bound to become aware what is at stake. Those who take the lead in developing a more coherent approach in this area will gain an edge in electronic commerce and the prospective new opportunities at hand in trade and development more broadly.