Current Developments in Privacy Frameworks: Towards Global Interoperability

Mexico City – November 2011

CSISAC Statement

Mr. Chairman, ladies and gentlemen, thank you for the opportunity to represent the Civil Society Information Society Advisory Council (CSISAC) today about recent developments in international privacy frameworks and efforts towards global interoperability. This is a wonderful occasion and I am grateful for the opportunity to participate today.

In our increasingly interconnected era, protecting privacy has never been a greater challenge for individuals. Recent repeated incidents of high profile privacy invasions and the following public outcries demonstrate a general erosion of trust and a pressing need for consistent, universally enforced, and rigorous privacy protections.

Innovation, the free flow of information, and trans-border interoperability are all-possible while still protecting privacy. Times have certainly changed since the OECD’s seminal privacy guidelines adopted in 1980. However, the principled, technologically neutral approach to privacy protection adopted by those guidelines allow them to play a continuing role in helping to bring about an interoperable world that upholds the respect for privacy.

In light of these changing times, it is worthwhile to explore ways in which guidelines can be reexamined to ensure that they continue to offer users sufficient protection amidst new and future challenges in data processing. However, the potential utility of the Guidelines (as well as of other international privacy instruments such as Convention 108), will never be realized if they are not first adopted and enforced.

It should now be definitively recognized that self-regulation fails to provide any reasonable mechanisms for ensuring the respect of users’ privacy expectations, especially in a market where people’s personal data has increasingly become commodified. This is particularly the case in behavioral targeting, where there is currently no direct business-to-customer relationship in place to provide even the most basic of market pressures on third party advertisers. There can be little realistic expectation that such a market will self-correct, as competitive forces drive market players away from privacy protective frameworks, instead of towards them.
Clear privacy principles would also provide guidance for companies in product development. These obligations are not onerous in terms of innovation. As many online services are facilitative, with the stated objective of providing users with a platform to best ‘share’ content, the obligation for primary consent should not be unduly prohibitive on legitimate innovations.

**Privacy Laws**

In terms of adoption, a number of Latin American countries, Mexico and Peru among them, should be congratulated for recently implementing domestic privacy frameworks. Professor Greenleaf, in a recent study, notes that 78 national data privacy laws have now been adopted by countries around the world providing—at least in theory—comprehensive frameworks for private sector data protection. Increasingly these privacy protective frameworks appear outside Europe, with 29 legal privacy laws adopted to date.

Even in those member states which has passed laws, there are serious questions about the level of enforcement and different interpretations of the same principles which together have the effect of not delivering the require level of protection. Also, some governments, and even some Member States, have yet to meet their obligations to uphold the principles in the Privacy Guidelines by enacting suitable laws. The Madrid declaration, now signed by over 100 organizations and 180 privacy experts from around the world, called upon all OECD Members to do so in 2009. This has not yet occurred. Such adoption represents a critical first step towards achieving interoperability and towards free transborder data flows.

**Interoperability**

The best and surest means of achieving interoperability is through universal adoption of binding and enforceable privacy laws. It should be noted that while such interoperability remains in the theoretical phase, transborder data flows should be limited by a comparable protection criteria of some sort. To permit organizations to bypass domestic privacy protections merely through the act of outsourcing is counterproductive. Similarly, a ‘race to the bottom’ approach to interoperability will not be far better than the existing self-regulatory model, and will fail to address user trust issues or to adequately protect privacy rights.

Nobody can disagree with the concept of interoperability as an abstract objective, but as Mme La Bail from European Union said, it must not be at the expense of high standards. We also agree with the representative of the Council of Europe when he said that human rights should be the baseline of any interoperability concept.

Civil society is skeptic of some current proposals for interoperability, including the APEC CBPR. We aren't sure if it will be sufficiently robust to ensure that the privacy standards are maintained. We remain suspicious that some of the new language about accountability and flexibility is really a disguise for lesser protection, with an objective of preventing privacy regulation from hindering new
business models and offshoring, even when these may not meet desired standards (despite protestations to the contrary).

While we wait for the ideal of universal adoption of adequate privacy protections to be realized, steps must be taken to ensure, in the meantime, that outsourcing is not used as a means of bypassing domestic privacy protections. An adequate level of protection must be ensured. CSISAC notes the importance of this. Lack of assurance over this factor was, in fact, one reason for its decision not to endorse the OECD’s Communiqué on high-level principles for Internet policy-making this past summer.

With cloud computing becoming an increasingly necessary part of the online experience --I myself wrote this speech ‘in the cloud’-- ensuring comparable protection across different regions and in spite of transborder flows becomes an even more important issue. The move to the cloud asks users to entrust a third party with their most closely guarded documents and materials. Information once kept safe in their own home, these will now in many cases, be held by organizations answering to foreign laws. Yet users may still attach high expectations of privacy to this data based on domestic sensibilities.

**Enforcement**

While everyone agrees on the importance and necessity for better enforcement, we must also emphasize the need for data protection agencies to practice greater transparency and accountability, both when they are the sole enforcement agencies for domestic compliance, but also when they cooperate with other agencies abroad. Individuals DPAs have done much good work but many criticisms of their effectiveness remain. Domestic compliance is still a problem and some DPAs still do not have enough enforcement authority.

When there is a transnational dimension to their enforcement, how can DPAs ensure effective cross-border cooperation for cases that affect a number of consumers and users within the OECD? Cross border enforcement cooperation, such as the OECD-GPEN and APEC-CPEA have been established, yet there remains to be evidence of any practical outcomes or cases. In this way, cross-border enforcement is a crucial yet complex issue for global privacy protection. As with interoperability more generally, cross-border enforcement must not come at the cost of high standards and more can surely be done to ensure its protection.

Thank you,

**Katitza Rodriguez on behalf of the Civil Society Information Society Advisory Council**