This fast changing environment provides a fertile ground for what Jeffrey calls a "rogue" element – an unpredictable individual (hacker) who poses a threat to the network, a computer system, or the state. Mafia boy is a prime example of this phenomenon. Another example of a new threat is provided by the Ahmed Ressam case. The case fuelled the fears of many Canadians and Americans about the "sense of threat from the outside." Many observers were surprised by the ease with which Mr. Ressam used a forged passport to enter Canada and plan for terrorist activities in the U.S.

While the new environment and threats affect nearly everybody, discussion about how to address new challenges and ensure our safety/security has been restricted to government officials and a few experts. A more inclusive debate should take place. Among other matters, the schizophrenic attitudes exhibited in Canada and other countries, where "Orwellian fears"concerning the potential for invasive surveillance and criminal use of technology co-exist with an apathy about privacy, should be addressed. The debate should include other questions such as:

- How to ensure that the cure for threats to both, sovereignty and privacy, is not worse than the disease?
- How many of our rights to privacy are we prepared to give up to business for profit, to the state for law enforcement purposes, to our fellow citizens for "entertainment?"
- What are the tools needed to create a balance between deterring legitimate threats and ensuring our fundamental freedoms (i.e., freedom of thought, belief, opinion and expression), legal rights (i.e., rights related to search and seizure), diversity and culture?

Finding answers to the last question is particularly pertinent. The right balance is key in reconfiguring social relations and structures to fit new realities, which are mostly technologically determined. *In order to find a right balance between deterrence to threats and freedoms/rights, trust is essential.* Lack of trust interferes in e-commerce, for instance (i.e., willingness to use credit cards over the Internet). Trust allows societies to make tough choices and is crucial for social cohesion. One may perceive trust in cyberspace as giving up personal privacy. Therefore, among the key challenges today is to counter the declining levels of trust. A *Charter of Information Rights and Responsibilities* could be instrumental in creating this much needed balance, while addressing questions concerning trust. However, ensuring that our environment is safe and secure involves more than just the police. Civil society, government and business all should be included in the discussions on the domestic as well as the global level. On a related note the digital divide is not only about access, but also inclusion.

1.2. New Threats to Privacy and Sovereignty, Reg Whitaker (York University)

Reg Whitaker suggested that the threats to privacy and sovereignty posed by new technology are analogous for both the state and an individual. New technology poses threats to the boundaries of both states and individuals. The sovereignty of states is diminishing at the same time as individuals' private space is shrinking. As a result, new geopolitical and social structures are developing.