of children. Common norms and parameters are hard to develop even among developed industrialised countries. *In order to prevent a similar fate to that of ancient Greece, efforts should be made to set baseline standards and bridge jurisdictional boundaries.*

Some participants said that finding the balance between deterrence to threats and freedoms/rights is not new. The dilemma comes especially into focus when weighing law enforcement against freedoms/rights. There is an acceptable latitude for legitimate law enforcement rooted in a general understanding that rights are not absolute. *The real question is how to effect containment on a law enforcement latitude. Determining containment is perhaps best done on a case by case basis.*

A point was added that there exists no adequate oversight of enforcement at the domestic level, and none at all at the global level. *Transparency should be enhanced to reduce the risk of plummeting trust.* Some said that the presence of an oversight mechanism is sometimes as valuable as oversight itself. In other words, the threat of punishment is an effective compliance tool.

A set of privacy principles:
1. Notice. The notice provides customers with clear and conspicuous notice of information practices, including what information is collected, how it is collected, held, shared and used. It may include:
- transparency of data collection
- methods for collecting information both, directly from individual customers and from 3rd parties
- what information is retained and for how long
- whether or not information is combined from multiple sources
- whether or not information is disclosed to other parties.

2. Relevance. Only that information which is necessary to perform a specified set of tasks is collected.
3. Security. All information is safeguarded with appropriate security methods and technologies.
4. Choice. Consent through notice and an opportunity to opt-out or explicit permission obtained in advance will be sought in advance of collecting, holding, using or sharing information.
5. Sensitive Information. Without expressed and informed consent, sensitive information will not be shared.
6. Access and Accuracy. Reasonable access to information will be offered to the owners of that information, subject to legal, technological or security constraints. Reasonable efforts will be made to give owners the opportunity to correct or delete information and keep it accurate.
7. Discrimination. Discrimination on the basis of collected information should be prevented.

Two views emerged about how to best regulate privacy:
1. Combination of self regulation and government regulation (i.e., combining Ethical Information Management with litigation)
2. Government regulation

Some participants suggested that self regulation could adequately meet privacy requirements if a set of privacy principles is observed, under the threat of litigation. A suggestion was made that *Ethical information management could include 3rd party audits*. Auditors would examine how a firm handles information and give a seal of approval when it does so ethically.