

Session title: **Privacy in a New Global Context: Trapped Between Culture, Laws, and Technology**

When? Saturday, February 20, 2010: 1:30 PM-4:30 PM
Where? Room 1A (San Diego Convention Center)

Socrates Was Wrong: How Far Is Privacy on the Decline?
Stephan Lechner, JRC Institute for the Protection and Security of the Citizen, Ispra, Italy

Electronic data processing? Fine with me! Since more than 30 years now our personal data are being processed electronically - we all got used to it and do not think a lot about it any more. But we should: the risk has changed. Computing concepts of the 70ies have mostly disappeared and today's data guards are not trusted civil servants in a mainframe environment any more. They often are low-paid (though smart and capable!) employees, be it for reasons of cost cutting in IT operations or for concentration on the core business where IT is just a side issue. Simultaneously, data storage capacities have grown immensely in the last 10 years such that today it is extremely simple to carry away gigabytes of valuable data in your pocket. This combination of low salaries, high value data (literally at the guards' fingertips) and expert knowledge has created a huge risk, and the say of ancient Greek Socrates that guards are protected by a noble lie does not hold any more: Today they are not protected at all! It already happened. Stolen data being bought by governments for millions sounds like an espionage story, but in 2008 it visibly happened when Germany took a new approach to fight tax evasion. Also the US put up a lot of pressure against Swiss banking offshore models, and traditional laws could not be combined with law enforcement requirements in the digital world. Telecommunications data got stolen and partly published, blackmail approaches were launched, business models abandoned, legal backdoors sought and found. The damage went into the millions and got life threatening for some of the involved parties; others stumbled and fell. Who guards the guards? But the main trend remained unbroken: More and more data are becoming available to more and more low-paid persons. The problem is not with technical IT security any more but with Socrates' question of "Who guards the guards?"

It is now time to properly address this challenge and come to a more holistic approach to information security, covering areas such as international harmonization of criminal laws, better appreciation of the economic value of personal data, understanding each others' cultural background on privacy and creating interoperable standards and regulations. There are a number of options for next steps in a global information environment, but all of them would require us to take information security more serious and not treat it as a technical matter or an exotic infrastructure issue alone.

When Law Meets Technology: Interdisciplinary Privacy Aspects
Claudia Cevenini, University of Bologna, Bologna, Italy

The law intervenes to regulate social, economic and technological phenomena; faced with contrasting interests and values, it needs to decide which ones should prevail and which ones instead succumb. Privacy law has the delicate task of understanding if and upon what conditions and procedures personal data may be processed - and to what extent one can control its own data: right to be left alone versus right to know. The rapid evolution of technology has set new and substantial challenges to the legislator: passing from paper to bits has actually enormously amplified the potential consequences of data mishandling. Regulating a phenomenon requires first of all to understand it fully. Law and ICT have traditionally constituted two quite separate and impermeable areas, speaking different languages, addressing different issues and following different reasoning paths. Last but not least: ICT is global, while the law is national or at least regional. In the Information Society this separation between the two disciplines appears no longer rational. Privacy now strongly needs to be addressed from an interdisciplinary perspective, set between fast-moving ICT and trailing legal provisions: finding a common understanding and generating synergies between law and technology is of basic importance. What should the role of the law be? Preventing misbehaviour by threatening a sanction or acting as an enabler, by actively supporting the development and use of safer, privacy-compatible technologies? EU Member State legislation sometimes imposes very strict rules to protect privacy and foresees severe sanctions. However, control is necessarily limited and while several data controllers perceive the regulation as bulky and of limited effectiveness, especially with reference to certain problems, such as spamming, only a limited number of data

mishandlings are punished. Should law always lag behind ICT or act preventively by setting a basic framework which may flexibly adapt to the future? A big issue in technology law concerns the trade-off between the need for certainty and stability of the law and the urge to keep the pace with an extremely rapid technological evolution. An overview over European and international data protection rules will be provided. The need for further action in both areas, laws and information technologies, will be presented.

Breach Disclosure Laws Contribution to Data Protection and Security
Deirdre K. Mulligan , UC Berkeley, Berkeley, CA

no summary

Dragon Kicked Awake: How China Handles Data Security
Zhong Chen , Peking University, Beijing 102600, China

As a country with myriad and rapidly increasing volume of Internet and mobile phone users, China is facing the critical challenges on the management of its information assets, and tradeoff between the control, management the Internet and keeping people's privacy and rights to express themselves online freely. Till the end of June 2009, China has 12.96 million domain name and 338 million subscribers of Internet, and 155million subscribers of mobile phone internet access, and ranks as No.1 in the world. Internet security has become a key issue while large scale e-business and e-payment growing up based on the Internet in China. Now China has entered into a new era of trustworthy Internet. Much more research and development efforts on Internet security are encouraged by both scientific and industrial management body of the government through its five-year-plan of national key projects. Through this talk, I will give: (1) an outline of China Internet infrastructure and applications; (2) the challenges of data security and privacy for both the government and the individuals; (3) the great efforts on the policy, legislation and standardization during last two decades ; (4) some case studies regarding to security, privacy and cyber-crime in China; (5) some R&D topics and achievements in China.

Privacy in Real Life: Many Don't Care, Some Guess, and Only Few Know
Sead Muftic , Royal Technical University, Stockholm, Sweden

"Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within them that is considered inherently special or personally sensitive. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time. Privacy can be seen as an aspect of security — one in which trade-offs between the interests of one group and another can become particularly clear." (Wikipedia) With advances of digital applications, environments and data banks, privacy more and more related to issues of controlling storage and distribution of personal data in the digital form. There are three possibilities to achieve that goal: technical (security solutions), organizational solutions, and regulatory (legal) solutions. Use of each of them individually depends, on one hand, on complexity, sometimes even price, and on the other hands on awareness of individuals, organizations, institutions in charge, and even entire societies. In this talk we will review first three different types of sensitive personal data that can be used as models for privacy concerns: identification data, financial data and medical data. We will review various technology solutions available today, various organizational forms, and various European and US regulations. Conclusions will be offered in the form of practical guidelines to individual to increase control and protection of their own personal data in order to improve privacy and security concerns.