9th EU Hitachi Science & Technology *forum* 2006

SUMMARY REPORT

ICT for Safety, Trust and Security:

Its impact on European citizens

19-21 May 2006, Warsaw

HITACHI
Inspire the Next

Contents

It is, again, a great pleasure to present the summary of the proceedings of the 9th EU Hitachi Science & Technology Forum on "ICT for safety, trust and security: its impact on European citizens". It took place in Warsaw and was officially opened by Prof. Kurzydlowski, Undersecretary of State, Ministry of Science and Higher Education and by Minister Mizuki of the Embassy of Japan to Poland.

The EU Hitachi Science & Technology Forum's main goal is to contribute to the public policy debate in Europe, an additional illustration of Hitachi's corporate philosophy, which is to contribute to society through science and technology.

Security, trust and safety threats are major issues in today's daily life. ICT has a great potential to cope with these concerns and, at the same time, ICT may create new problems for our society. This was at the core of the Forum participants' debates and discussions, which conclusions make most of this summary. It positively demonstrates that the Forum provided a very good opportunity for scientists, industry representatives, policy makers and general citizens to assess what could be the optimum ICT deployment for society.

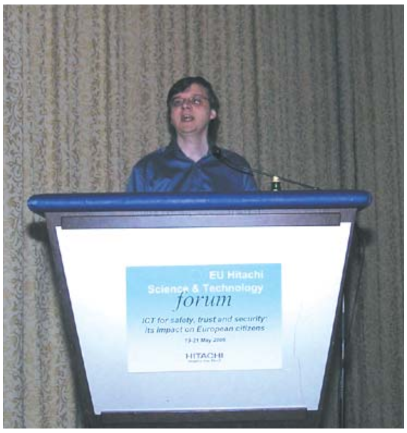
In Hitachi, we are always looking for improvements in the Forum outputs. This year we invited representatives from academia, the EU Institutions, Member States governments, and industry in addition to the Forum members thus enabling deeper interdisciplinary discussion. Also we had a small demonstration corner to show some relevant technologies. Finally, the moderators of the working sessions, all skilled professional in their fields, wrote the section of this report related to their working session.

I would like to address a special thanks to the 9th Forum general moderator, Dr. Jean Freymond, who has conducted this annual meeting in a very professional way. It goes without saying that the Forum success and reputation are made possible through the talent and commitment of our speakers, session moderators, Forum fellows and participants. To all of them, my deepest gratitude which goes also to my Hitachi colleagues whose commitment to the Forum is one of its key assets.

Michiharu Nakamura

Dr. Michiharu Nakamura
Executive Vice President & Executive Officer, Hitachi, Ltd.
Hitachi Group Chief Innovations Officer
Hitachi Group Chief Technology Officer

EU Hitachi
Science & Technology
forum
ICT for safety, trust and security:
its impact on European citizens
HITACHI



left to right:

Mr. Ko Takahashi,
Dr. Jacques Bus,
Mr. Martin Sadler,
Prof. Mieczyslaw Muraszkiewicz,
Sir Stephen Gomersall,
Mr. Bart Van Rijnsoever
and members of the audience

What is the EU Hitachi Science & Technology Forum?

Since its creation in 1910, Hitachi has kept its founder's commitment to contribute to society through technology. Once more, this longstanding commitment has been demonstrated by the setting up of the EU Hitachi Science & Technology Forum in 1998 by the Hitachi Corporate Office, Europe.

This Forum brings together European scientists and engineers who have all participated in long-term internships in the Hitachi laboratories or plants in Japan. The Forum was designed to meet two objectives. Firstly, it provides a platform where these Hitachi alumni can address and discuss societal issues related to science and technology in the daily life of European citizens. Secondly, it provides a yearly occasion for all European Hitachi alumni to meet friends and colleagues.

In 1998, the Forum concept was successfully tested at a meeting in France with the working theme: "R&D in SMEs, comparison between the EU and Japan". The meeting started on Friday evening and closed on Sunday afternoon, with large breaks giving free time to the participants. This format has been kept ever since.

The topics and venues for the annual meetings since then have been:

1999	Germany: Information technology and its benefits to society
2000	Dublin: Electronic commerce and its impact on society
2001	Brussels : Life sciences and their impact on European society
2002	Budapest: Water Issues and their impact on European society
2003	Antwerp: Energy and its implications for European society
2004	Stockholm: Transport and IT: impact on European society
2005	Athens: Technology and its impact on the city of the future

In 1999, to allow Forum members greater involvement in the organisation of the event, a working group was created appointed for one year. With this development the Forum was to be run by its members, on topics selected by its members, for the benefit of its members. This was the Hitachi Corporate Office medium-term objective. Also, in September 1999 a newsletter, European Connextion, was launched as a link between Forum members and Hitachi and as a tool to promote the Forum proceedings.

Since 2001, at the request of Forum members, the meetings have included a presentation on current Hitachi R&D developments. Hitachi executives from the EU and Japan have attended the Forums and answered questions related to Hitachi’s activities.

The Forum relies on the support of experts who have a keen interest in European societal issues and contribute to its success through a strong personal commitment. These individuals comprise the Forum Fellowship. The Forum Fellows are: Mr. Mark Cantley (Advisor, DG Research, European Commission), Mr. Didier Gambier (Head of Unit, DG Research, European Commission), Mr. Dolf Gielen (International Energy Agency), Mr. Pierre Longin (President, Longin Conseil, Brussels), Mr. Antoine Ripoll (Senior Administrator, European Parliament), Dr. Florian Schmitz (Rechtsanwalt, Clifford Chance Pünder, Frankfurt) and Mr. Robert Verrue (Director General, DG Taxation and Customs Union).
The chairman of the Forum Fellows is Dr. Michiharu Nakamura (Executive Vice President & Executive Officer, Hitachi, Ltd.)

Hitachi, with the active participation of Forum members is committed to contribute to European Society by helping to shape policies which will improve the daily life of their fellow European citizens. In this respect, the EU Hitachi Science & Technology Forum wants to clearly bring the benefits of new technologies to all Europeans.

Forum Summary Report:

ICT for Safety, Trust and Security: Its impact on European citizens

EXECUTIVE SUMMARY

The 9th EU Hitachi Science & Technology Forum brought together around 130 scientists, engineers, executives and policy-makers around the theme "ICT for safety, trust and security: its impact on European citizens". The Forum addressed the role of information and communication technology (ICT) in combating security threats, safeguarding privacy and identity, and enabling trust in e-business and e-government services.

The Forum heard that as ICT becomes pervasive throughout society, citizens are confronted by safety, security and trust on many fronts. From surveillance by CCTV cameras as we walk down the street, and use of biometric data in passports, to the collection and exchange of medical data, and vulnerabilities in communication and power networks, these issues increasingly impinge into our daily lives.

The key issue, as set out by the keynote speakers, is balance. Technology, if left unchecked, can be abused; governments, if left unchecked, can go to extremes. As the invited speakers noted, we must strive to balance technology and culture (Prof. Muraszkiewicz); privacy and the common good (Mr. Davies); and the citizen and the state (Lord Erroll). The consequences if we do not are dire. Misuse of technology will create a backlash from the public and risks damaging the very values we are meant to be defending. We need security technology with a human face.

Fortunately, views of security are changing. Wider use of ICT, interconnection of networks, and greater sharing of content and resources mean we must think of security as an ‘open metropolis’ rather than as a ‘walled fortress’. New approaches and models for this more open environment - so-called ‘trusted computing’ - are a key focus for research. These models are necessary not only to establish the new ‘social contract’ championed by the keynote speakers, but also for economic reasons. Only through assurance-based models can businesses quantify the benefits of security and invest accordingly.

User requirements were a key theme. Security requirements differ markedly from one application to another: in some cases it is a matter of authorising the user rather than fully identifying them, so we must ensure that security is at an appropriate level. Where applications or datasets overlap, users should be able to control the personal data to which third parties have access. Furthermore, as Mr. Bousquet’s healthcare example clearly showed, different stakeholders will have different requirements of the same application. Hence the Forum identified a paradox here. On the one hand, trust and security must be made more explicit in social and economic transactions, so that players – businesses, governments, consumers, etc - can assess the real risks, costs and benefits. But from the technological point of view security features must be made more implicit, embedded in systems and applications in a way that is transparent to the end user and makes the solution easier to use.

As we strive to achieve these objectives, the Forum concluded that we must seek a distinctively European approach. Europe is much more heterogeneous than North America and has very different needs. We must play to our strengths and our values so as to build a European security culture. These values – such as respect for privacy and human rights – can be drivers of innovation and a source of competitiveness for European firms in world markets.

The Forum arrived at recommendations in four key areas:

- Greater emphasis is needed on education so as to raise awareness of trust & security issues amongst users, and to stimulate and actively support users in exercising their legal rights.
- Research has a major contribution to make in developing privacy-enhancing technologies and more user-friendly systems. Such efforts should take greater account of user requirements and preferences. As well as technology, research is needed into the socio-economic context of security, such as business and social models for trusted computing.
- Standardisation will be important in a number of respects: stimulating market take-up of security technologies and solutions; boosting consumers’ confidence in products and services; and strengthening the position of European suppliers in world markets.
- Regulation is an important driver of innovation in this area. More effective regulation is needed so as to keep pace with – and even anticipate – the technology developments.

INTRODUCTION

Around 130 participants attended the 9th EU Hitachi Science & Technology Forum held in Warsaw, Poland from 19th-21st May 2006. The theme for this year's Forum was "ICT for Safety, Trust and Security: Its Impact on European Citizens". As usual, the gathering attracted a diverse range of scientists, engineers, executives and policy-makers.
Dr. Jean Freymond, Director of the Centre for Applied Studies in International Negotiations (CASIN), Geneva, served as Forum General Moderator, drawing linkages between the presentations and encouraging participants to engage in a constructive analysis of the issues. In his opening remarks, Dr. Freymond welcomed Forum members and contributors. It had taken the Forum quite a while to get around to this topic, he noted. But it is now very central in modern society and there are many important ethical, legal and social questions to solve.
Mr. Ko Takahashi, General Manager of Hitachi Corporate Office, Europe, welcomed participants to Warsaw. This year's event would introduce a number of innovations, he explained. Firstly, guest moderators had been invited to prepare conclusions and short written reports on the parallel working sessions. Secondly, industry representation at the event had been extended. And to meet requests for more information on Hitachi's own activities in Europe, Sir Stephen Gomersall was to deliver an overview presentation on Sunday morning.
Mr. Takahashi expressed his appreciation to the guest speakers for agreeing to participate in the meeting and to Dr. Freymond for agreeing to act as general moderator.

Prof. Krzysztof Kurzydlowski, Undersecretary of State, Polish Ministry of Education and Science, said he was pleased to address such a distinguished gathering and welcomed participants on behalf of the Polish government. He offered his congratulations for selecting such an interesting topic. Poland had made remarkable progress over the last 16 years, Prof. Kurzydlowski noted, but it was still far from being satisfied. This was a totally different country to 1989 but much more remained to be done. Poland was a good place for technology, for investment and for business, and it looked forward to the future with confidence.
Prof. Kurzydlowski wished the Forum a rewarding discussion and a successful meeting.

H.E.M Ikuo Mizuki, Minister, Embassy of Japan to Poland, said he was honoured to be invited to the meeting, and thanked the organisers and his Polish hosts. Poland was emerging as the economic dynamo of Central & Eastern Europe, Mr. Mizuki noted, and was attracting strong interest from Japanese companies. It has a strong academic base in science and information and communication technologies (ICT). Investment by Japanese companies is expected to grow rapidly. The two countries have a long history of co-operation in science, technology and culture, most recently through Japan's support for the Mangha Japanese Culture Centre, Krakow. Users in Poland and elsewhere are looking to ICT as a platform for new services but there are numerous threats to safety and security. Mr. Mizuki hoped the Forum would provide the opportunity to share opinions on how to address these. On behalf of the Japanese government he wished participants a fruitful and successful meeting.

Dr. Michiharu Nakamura, Executive Vice President & Executive Officer, Hitachi Ltd, presented Forum Fellowships to Antoine Ripoll, Senior Administrator in the European Parliament, and Didier Gambier, Head of Unit for ITER, DG Research, European Commission.

KEYNOTE SPEECHES

The Safer World and Its Enemies

Prof. Mieczyslaw Muraszkiewicz, Deputy Director, Institute for Computer & Information Engineering, Warsaw University of Technology

Prof. Muraszkiewicz introduced himself as "I*ch bin Ingenieur*", which hopefully improved his credibility for such a technical audience, and said he felt privileged to share his thoughts and opinions with the Forum.
The title of his talk, he explained, was derived from the book The Open Society and its Enemies by the philosopher of science Karl Popper. The relationship between technology and culture, he would argue, is asymmetric in favour of technology.
What is technology?, Prof. Muraszkiewicz asked. We live in a universe of tools and machines, procedures and processes, and products and services that we use for transforming both the material and immaterial worlds. Technology is often perceived as a major factor in economic and societal transformations, and a major instrument of progress and betterment. Thus, one view of technology is overwhelmingly positive.
But, Prof. Muraszkiewicz continued, people are usually aware of threats, perils and negative consequences of technology. One only has to think of Hiroshima, Chernobyl, thalidomide and BSE to see the dangers technology can cause.
Why do we love technology? Marshal McLuhan, author of The Global Village, had argued that technology enhances and strengthens our abilities, attributes and senses. In other words, Prof. Muraszkiewicz went on, "Technology satisfies our individual and collective ego and we get bigger through technology".
Culture, on the other hand, has very different attributes. It is an invisible universe of symbols, archetypes, beliefs, relations, values, laws, responsibilities and duties that have been constructed and established over a prolonged period. "Culture is a controlling mechanism which imposes values and behavioural patterns". Most importantly, culture transforms individuals and non-coherent groups into communities and societies. Culture tempers and moderates our individual and collective ego, and thus is a counterweight to technology.
How can these two factors co-exist? Prof. Muraszkiewicz maintained that often they don't and that technology tends to displace culture. Technology has become today's mythology or religion. Yet it has no spiritual basis and often only arouses anxieties and fear.
Returning to his title, Prof. Muraszkiewicz asked "So, who are the enemies of the safer world?" The answer,

he maintained, is us. It is we who design and use technology for hostile purposes. We have to reconcile technology and culture and find a better balance between the two. The consequences if we do not will be dire. Culture defines our sense of life and provides us with a social anchor: it is what makes us human. We must use technology to drive and reinforce culture rather than to destroy it.

Prof. Muraszkiewicz cited the MOST initiative (Mobile Open Society through Wireless Technology, www.most-program.org) as an example of an open and participatory approach. Funded by the European Commission, MOST has set up a foundation that brings together universities, industry and public agencies operating in Central and Eastern Europe to boost the development of civic society through appropriate use of wireless technologies.

The Powder Keg: Government Power, Citizens' Rights and the Common Good
Mr. Simon Davies, Visiting Fellow, London School of Economics; Director, Privacy International

Mr. Davies said it was a thrill to be in Warsaw and he was looking forward to the debate.

"What should we take away from this Forum?", he asked. The central issue, as he saw it, was trust. Technology and society are changing rapidly: we need a formula for the 21st century that will engender trust. Europe's technology challenge is to implement ICTs that create benefits for the citizen, nurture economic growth and result in a safer and better society. In doing so we must also protect citizens' rights, encourage freedom of choice and improve accountability of government.

One example of how not to do it, Mr. Davies argued, was the UK's approach to identity cards. Such a radical cultural change needs the trust and support of the population. This was clearly lacking in the UK, yet the government was pressing ahead regardless. Moreover, it was doing so on an unprecedented scale and using old technology. "We need a much more sensitive handling of the matrix of trust", Mr. Davies noted.

Privacy is one of the most politically sensitive elements of any project. We have to find the right balance between users' desire for privacy and the needs of disclosure for the "common good". At present, the scales are tipped much too much towards the latter, Mr. Davies argued.

Mr. Davies saw the tension between 'privacy' and the 'common good' as the crux of the problem.

Governments take maintenance of the common good as their primary mandate. This leads them down a number of avenues which may in fact conflict with the interests of individual citizens. Firstly, they tend to fast-track policy development, bolting-on systems and procedures to existing structures ('function creep'). Secondly, they abandon data privacy principles, allowing data collected for one purpose to be used for another or for identities to be matched across different datasets ('identity creep'). Thirdly, there is an endemic use of delegated legislation which avoids full legislative scrutiny ('exemption creep').

Mr. Davies was particularly concerned about "function creep", where systems designed for one purpose were then extended for another. The UK national DNA database, for example, was originally set up to cover a strictly limited set of criminal offences: murder, burglary, sexual assault and grievous bodily harm. After 18 months, and without prior consultation, the system was extended to include all individuals charged, reported, cautioned or convicted of any recordable offence. This was subsequently extended to allow DNA to be stored indefinitely, regardless of acquittal or innocence. And with advances in genome technology, soon it may be possible to identify an individual's characteristics from their DNA. All of this has happened within 10 years and constitutes a major change in the social contract between government and its citizens.

Another example of function creep is the European Arrest Warrant. Again, this started out as a legal instrument for a narrow set of offences: terrorism, organised crime, murder, and child exploitation. Within one year it had been extended to cover 15 other offences, including arson and fraud, and within two years over 30 offences qualified.

How do we stop misuse of technology by politicians, Mr. Davies asked? The answer, he maintained, was to forge an agreement – a new social contract – in society through involving the public at all levels. The current situation carries major risks; we can't continue the current trends in tracking, monitoring, etc, without a significant backlash. Citizens will draw the line against intrusion and by then it will be too late. So, we have to re-establish new models of trust that respect citizen's rights and have more checks and balances. "This", concluded Mr. Davies, "will be the most vital concept any of us will deal with".

The Citizen and the State
The Earl of Erroll, the House of Lords, UK

Merlin Hay, Lord Erroll, welcomed the opportunity to address the Forum, although felt that many of the other speakers were better qualified on the subject. His role, he maintained, was as "a representative of a benign bureaucracy protecting citizens from harm".

Identity is now firmly on the political agenda across Europe, Lord Erroll noted. Identity (ID) cards, e-commerce and online access to government services all require us to prove who we are. The purpose of ID is to help citizens and keep them safe. Central government tries to enforce a unique ID for each individual but often different types of ID are required, such as when interacting with local government services. Why should I trust 'them' with my identity? is a question many citizens ask of government. The question was a legitimate one, Lord Erroll argued. We only have to look at history to know that mistakes can and will be made: governments can abuse power; personal details can be sold; identification mistakes will be made; and the State will cover up its mistakes. People are corruptible in all sorts of ways and the new technologies mean the consequences of corruption can be much higher.

Another key question for citizens, Lord Erroll suggested, was: "Who needs to know who I am and why?" This leads to the issue of identification versus authorisation.

In many instances, full identification of an individual or user is not necessary to gain access to a system or service. The key security issue is not "who am I" but "can I do it?" Biometric traits, such as fingerprints and iris scans, are often used in this context, for instance in building access systems. Such systems have a rejection rate of around 2%, but even this is too high for a high volume use such as at a large airport. There is also the issue of inclusion: ensuring certain social groups, such as the disabled, are not excluded through use of biometric techniques.

People should be allowed to have different personas, Lord Erroll argued: one for your work, one for your sports club, one for online shopping, etc. We have to think what things are for and adapt the technology accordingly. Thus, ID smartcards could have a variety of uses: to show a criminal record on a passport; to show creditworthiness for financial transactions; to show medical history for health services, etc. But we need to be able to control who has access to such data and for what purposes.

Finally, Lord Erroll contrasted policy-makers' preoccupation with identity with the very low priority given to e-crime. Yet the latter is much more of a problem in everyday life. E-crime is a relatively low policing priority and is not monitored or reported on effectively. As a result we still lack data on the real cost for society or for individuals. The law is also outdated, in the UK at least, in terms of liability for identity fraud. E-crime needs to be much higher up the political agenda, Lord Erroll believed.

"We are currently trying to control too much using rules and processes, instead we should govern using the principles upon which we want to build our society" Lord Erroll concluded. We cannot control modern economies and corporations with this type of approach. We need a better balance between the citizen and the state and must not let one side take over completely from the other.

KEYNOTE SPEECHES: RESPONSE

Sir Stephen Gomersall, Chief Executive for Europe, Hitachi Ltd.

Sir Stephen welcomed participants on behalf of Hitachi and thanked Minister Kurzydlowski and Ambassador Mizuki for their contributions. Central & Eastern Europe was very important for Hitachi, a factor underlined by the setting up of a new business development office which will open later this year.

Responding to the keynote presentations, Sir Stephen said Hitachi was a technology company and technology had received serious challenges from the speakers. Prof. Muraszkiewicz had characterised technology as a "barbarian at the gate". Mr. Davies had argued that technology without culture will bear no fruit. He had asked us to consider whether the debate is really about technology or politics? And Lord Erroll had offered fascinating insights from the political scene. The presentations served to emphasize that technology without compassion is full of risks. He looked forward to interventions from elsewhere in Europe and to hearing the views of the private sector.

PERSPECTIVE I: EUROPEAN COMMISSION

ICT for Trust and Security: The European Perspective

Dr. Jacques Bus, DG Information Society and Media, Head of Unit, ICT for Trust and Security, European Commission

New technology requires a paradigm shift in our approach to security, Dr. Bus maintained.

Drawing an analogy, he described the historical approach to security as being a 'walled fortress': we operated from a physical location with closed doors; security was seen as protection; and we set out to defend our data and systems. The approach required in today's networked world is very different, and is best characterised as an 'open metropolis'. The environment is open, unbounded and interconnected; we view trust as an enabler; and we aim to share our content and resources.

The stakes are high, in both economic and social terms, Dr. Bus argued. For instance, Reuters estimates that viruses cost businesses $55bn in 2003, roughly twice as much as the previous year. As Mr. Davies had outlined, the likely cost of rolling out the UK ID card scheme will range from £10.6bn to £19.2bn.

The European Commission addresses these issues through a wide-ranging programme of research in ICT for trust and security. One focus area is resilient ICT-based infrastructures. Today's infrastructures and utilities are highly interconnected, complex and vulnerable. In September 2003, for instance, the Italian electricity grid collapsed leaving almost 50 million people without electricity for one day. In October 2004 part of France Telecom's IT infrastructure went down, leaving 15 million people without telephone for two days. EU research is looking at how to build dependable, resilient ICT infrastructures; how to manage and control large-scale dependable systems; and how to understand and manage interdependencies.

A second area for research is trust, focusing on privacy-enhancing technologies that empower citizens to use data in their own way. In a third area, biometrics, work aims to ensure lifelong secure access to data and services without compromising trust and privacy. Fourthly, there is the issue of trust in the internet, aiming to combat computer hacking and ensure security in 'always on' and mobile environments. Research here includes work on security architectures, intelligent networks, and forensics.

Looking to the future, Dr. Bus saw the main challenge as being the increasing pervasiveness of ICT in our daily lives. We rely on the internet and other networks for more and more services and day-to-day activities. Networks themselves are becoming more complex and interconnected, and intertwined with critical infrastructures. Plus, ubiquitous sensors and RFID mean the internet does not just connect people but also things. We have to build networks and systems that are dependable, reliable and secure enough for us to trust such a world.

PERSPECTIVE II: CIVIL SOCIETY

The Good, the Bad and the Ugly: Security Technology and Human Rights

Dr. Ian Brown, Senior Research Manager, the Cambridge-MIT Institute, Board Member of European Digital Rights (EDRi)

Despite the title of his talk, Dr. Brown said he was optimistic and hoped Forum members would agree with his assessment.
"Who cares about human rights?", Dr. Brown asked. He identified three main groups: citizens, who want to be treated with dignity and respect; regulators, who want to make sure law is being followed; and legislators, who are being pressured to create new legislation by unhappy voters.
To respect human rights concerns, security technology should have three main facets, Dr. Brown argued. Firstly, it should be minimally invasive, which means being targeted and gathering the minimum of personal data. A good example is the monitoring of transport containers, where typically only 10% - those considered at highest risk – are scanned. Widespread use of CCTV was a bad example, since it gathers personal data while merely displacing the problem to other areas. In the 'ugly' category are government schemes, such as ID cards and communications data retention, which treat entire populations as criminals.

A second feature is that technology must be effective, providing the benefits claimed at a reasonable cost. Stronger cockpit doors and better street lighting are good examples; face recognition that identifies petty criminals but leads to few arrests is a bad example. Worst of all are schemes such as the US$15bn US-VISIT programme which identifies just low-level criminals.
Thirdly, security technology must be strategic. It should not be used in a way that creates new community grievances, such as more racially biased police searches. Humans don't want to live in a risk-free world and we should not damage the values the "war on terror" is supposed to be defending, e.g. by censoring websites or undertaking wiretaps without a warrant. "Fix the causes of problems, not the surface symptoms", Dr. Brown implored.
Can we be safe and free? As an optimist, Dr. Brown believed we could. Engineers have a vital role in ensuring technology protects our freedom and security. Minimally-invasive, effective and strategic technology can do that. Vastly expensive mass surveillance and censorship technologies cannot.

PERSPECTIVE III: INDUSTRY

Who Should Pay for Safety, Trust and Security?

Mr. Martin Sadler, Director, HP Security Laboratory, Hewlett Packard

Our dependence on ICT is continuing to increase, Mr. Sadler explained, and cybercrime is becoming organised. We are seeing a shift from 'hacking for fame' to 'hacking for gain'.
At present we have a very limited understanding of important issues: how software is produced; how systems are designed and solutions deployed; security mechanisms and the epidemiology of attacks; and economic drivers. "We are still stuck in the dark ages", Mr. Sadler maintained, "and don't understand what we need to do. As a consequence, businesses don't know what priority to give to security or how much to invest in it."
"Why don't we do better?", Mr. Sadler asked. He saw two reasons. Firstly, we do not invest enough because of a reluctance to pay and to share. Everyone thinks "someone else should pay". Secondly, it is difficult to quantify benefits, as evidenced by typical service-level agreements for security. To quantify the situation we need to know what is happening.

In preventing cybercrime we need to shift from security to assurance. It is not enough to secure: we have to know it is secure and be able to demonstrate it. This means putting controls in place to provide 24x7 assurance. Better modelling of security within organisations is another key requirement. Models can become the basis for negotiation, which in turn can become the basis for commercial contracts. Trusted computing allows us to trust data from others.
With these innovations we can move towards paying for security based on risk profiles of different organisations: those who can attest (prove) their security the best pay less. Similarly, the more you share, the less you should pay. Trusted computing provides the basis for an economic model, Mr. Sadler concluded.

Privacy Protection in Biometrics

Mr. Bart Van Rijnsoever, Department Head, Information & Security Systems, Philips Research

Biometrics is "a great technology with many benefits", Mr. van Rijnsoever enthused. Biometrics enhance the security of many services. They also add much convenience for the end-user when replacing passwords and PIN-codes. Examples of biometric applications include security services (automated fingerprint identification system, visa information system), biometric passports and identity cards, biometric access control systems (e.g. for building access, computer or mobile phone log-on, electronic banking), and biometric ticketing (e.g. boarding cards, stadium tickets).
Mr. van Rijnsoever saw three main privacy issues in relation to biometrics. Firstly, there was identity theft where biometric data could be abused through copying or stealing. Secondly, there is the issue of 'cross-matching' where biometric data could be used to find a person's identity in one or more databases. Thirdly, with the science of genomics progressing at an amazing rate, there is the possibility to derive medical information from biometric data.
Biometric template protection provides a means of safeguarding information and protecting against misuse. This is a way of storing representations of biometric data, rather than the data itself. Access is through encrypted passwords which are very hard to break.

Advantages of this approach include safe storage in centralised databases, low-cost storage (due to the small template size), and fast read-out and matching time. Philips is investigating application of the system to a biometric ePassport.

Holistic Security in a European Environment

Dr. Stephan Lechner, Head of Security Research, Siemens AG Corporate Technology

Europe is still highly heterogeneous, Dr. Lechner explained. The European Union has 25 Member States and 20 official languages, with key differences in wealth, size, history and culture. Although we have many common objective and interests, "by gut feeling we are not necessarily European", he surmised.

This fragmentation is reflected in the security arena. Diverse terminology and technologies, different national laws and interpretations of EU regulations, different needs and security implementations, and mutual distrust are key characteristics of the European security scene. The United States, with its more unified market and system of government, experiences none of these problems. The issue is clear, Dr. Lechner maintained: "If the EU copies North America in its approach to security it will end up in a mess because these systems are not tailored to EU needs."

Instead we must strive towards a distinctive European approach to security, Dr. Lechner argued. Firstly, we should see security as an opportunity rather than a problem. Security is much more than spam and spyware. We need a holistic approach that creates an attractive value proposition for users. Research has much to contribute here.

Europe does not have a single ‘homeland’ like the United States. Infrastructure will continue to be governed and protected at national level. But since the networks are increasingly interconnected at European level, we need new technological concepts and agreements across Europe on how to manage these networks. Technological interoperability will also be important in the European context.

All this will help lead to "a European security culture" Dr. Lechner argued. "If we can set our mind towards it and have the right attitude we will succeed."

Challenge with Security and Regulation

Mr. Mika Lauhde, Director, Nokia, Technology Management, Customer and Market Operations

Mr. Lauhde’s presentation explored the uneasy relationship between security and regulation. The latter can change very quickly, he explained, and undermine years of technical work.

Regulators are getting alarming messages about security. Yet security is already serious business, with the US and Asia big players as well as Europe. The challenge for Industry is to convince decision makers of the progress that has been achieved. In today’s world, propriety systems are not an effective solution.

Governments’ interests in security come from two directions: protecting national security and protecting citizens’ privacy. Approaches to and balance between these issues tend to differ between countries, making it difficult to develop common products for all markets.

Turning to security technologies, Mr. Lauhde noted that the problems lie not with the technologies themselves but in how they are used. We need to ensure legislation evolves at the same rate as the technology and also to accept that requirements will vary between different jurisdictions. De facto standards play a key role in determining market growth and can be difficult to overturn once established. In Europe we have to be early birds in standards and guide decision making in the right way.

Mr. Lauhde saw optimisation of security as another key issue. We have to balance the level of investment against the benefits achieved: in most applications military-level security will not be necessary. User requirements is a good place to start so as to achieve the most appropriate approach. We should also pay attention to usability and look at the costs and benefits of alternatives.

In conclusion, Mr. Lauhde noted that rules and regulations are essential for unleashing wider use of security technologies across society. In addition, we have to sell the benefits to the public and make provision for ‘fallback’. An example of the latter is the SafetyNet system in Austria, which provides support for people suffering lost or stolen identities.

Security and Trust in Ubiquitous Information Society

Mr. Mitsuo Yamaguchi, Chief Operating Officer, Hitachi Ltd., Information & Telecommunication Systems

Hitachi’s vision for the future was to promote ‘uValue’, Mr. Yamaguchi explained. ‘u’ has several meanings here: ‘ubiquitous’, ‘user-friendly’ or ‘universal’. In essence, uValue means working with customers to create innovative forms of value whatever the application. Hitachi is not a pure IT company and operates in very different ways, giving it a unique strength in the complex world of security solutions.

Turning to changes in society, Mr. Yamaguchi noted that Hitachi was playing a major role in the e-Japan strategy, the latest version of which was published in January 2006. This aims to solve problems in Japanese society through capturing the "reformation capability" of IT in a number of socio-economic areas.

As the information society becomes ubiquitous, so does the need for safety and security. This is particularly so in business, where information leakage and other security concerns can have a critical impact. Falls in share price and revenues, damage to brands and reputation, and even bankruptcy are just some of the possible effects. Thus, it is essential that firms take effective countermeasures.

To be an excellent provider of security solutions Hitachi must also be an excellent user, Mr. Yamaguchi explained. Hitachi’s Internal Security Committee (ISC) has been set up to oversee all areas of security management. Aspects include secure PCs and cell phones for Hitachi employees, and a unified approach to business continuity planning across the Hitachi Group.

Mr. Yamaguchi concluded with some examples of

Hitachi's technologies in ID and security solutions. These cut across five application areas: networks, terminals, users, content, and goods. In the area of terminals, for instance, Hitachi has developed a Trusted Platform Module (TPM), a standardised chip that fits inside a PC and allows both to execute security functions and to protect data independently from the operating system or hardware. For users, finger vein authentication – based on internal vein patterns within the finger - offers a biometric solution that is difficult to copy. And for content, the company's iVDR system is an access-protected removable disk storage that provides a bridge between different media applications, such as in-home and in-car entertainment.

INDUSTRY Q&A SESSION

This part of the proceedings concluded with a panel session at which participants were invited to submit their questions to the industry speakers.

Tony Morton-Blake asked: "In a society in which decision-makers are directly answerable to the people, what problems do you foresee with privacy? Must we insist on personal privacy? Is it a right?" Dr. Bus replied that privacy is not a fixed concept, nor even a well defined one. We live in an evolutionary environment and will have to deal with a moving target. People do care about their data and they will expect controls to guard against 'function creep' (e.g. to prevent abuse for commercial purposes). We will need rules which allow people to live in different spheres – home, work, holiday, etc.

Daphne Steegh noted that the panel had talked about changing the mindset when it came to 'European' security, but how would this come about practically? "Where is the European value?", she asked. Dr. Lechner replied that the European mindset could not be regulated or changed easily. To create a security mindset and attitude we would need to build alliances between the players and stakeholders at many different levels: industry, government, human rights bodies, and consumers.

"In New Orleans the world witnessed the collapse of civil society due to a hurricane", observed Rolef de Weijs. "With the growing dependency on ICT, the same could happen in case of a breakdown of the internet. Should companies be obliged to have a non-ICT back-up system?", he asked. Martin Sadler said many companies already had them, as part of their business continuity plans. Companies and regions could help each other more, for instance by sharing facilities to guard against a major internet outage.

Mike Parr asked: "How can we take account of human factors in the technology? Human factors have been key in breaching US military systems over the years but still we don't learn the lessons." Dr. Lechner agreed that human factors were essential. They had been weak points in the past, for instance people's use of passwords. Interfaces needed to be more transparent with security integrated into the technology. Lord Erroll agreed that we had to build security into systems, but also noted that "plain-old corruption" could be a factor too. Mr. Laudhe noted that centralised security systems were on the way out and that future systems would deal

EU Hitachi
Science & Technology
forum
ICT for safety, trust and security:
its impact on European citizens
HITACHI

New Forum Fellows: Mr. Antoine Ripoll and Mr. Didier Gambier,
Dr. Stephan Lechner,
Members of the audience,
Dr. Jean F. Freymond

with security in a more distributed way.

Janne Uusilehto asked how the European Commission will ensure the right approach for information society development in Europe. By ‘right’ he meant "an awareness- and human-driven approach, instead of the technology and corporate-driven approach we see in many areas today." Dr. Bus replied that there was no right approach. The Commission was trying to follow what is going on in society and to react accordingly. Policy goes hand-in-hand with research, for instance in the area of critical infrastructure protection. "It is a matter of bringing together diverse requests and demands", Dr. Bus commented.

David Sporn was concerned with e-crime. "What would be the effect on crime over the internet of widespread take-up of open source software?", he asked. "Should we provide citizens with a kind of ‘how to use the internet safely’ guide?" was his supplementary. Martin Sadler commented that the Commission had done a lot to promote security in open source software (OSS). For instance, HP was involved in a new project looking at trusted computing based on OSS within a multi-platform environment. This diversity is not there today but it will be in the future so we have to prepare for it. Dr. Bus noted there was a high correlation between cybercrime and the uniformity in today’s systems (dominance of Microsoft and Intel). Through its research programmes, the EC was promoting interoperable, standardised solutions in all sorts of environments. Finally, Mr. Laudhe commented that OSS approaches had major security advantages: with more resources – ‘pairs of eyes’ – to look at problems developers were able to respond to issues faster.

PERSPECTIVE IV: ICT SYSTEM USERS

User’ Viewpoints and Expectations: Healthcare as a Showcase

Mr. Vincent Bousquet, VP & GM, Medasys, Healthcare Operations

Mr. Bousquet considered health an ideal showcase for ICT security applications, for a number of reasons. Firstly, health is an important concern for individuals and deals with our most private data – aspects which we may not even wish to share with our families. For governments, health is a major determinant of well-being and also a major area of public expenditure. An ageing population and continuing progress in drugs and medical technologies will increase these pressures even further.

Medical practice is changing rapidly, too. Modern medicine requires cooperation between a vast network of specialists. Patients are now keen to be part of the decision process and there are trends towards managed care. Meanwhile, local, regional and national authorities are in need of real time business intelligence tools to monitor healthcare quality and productivity.

Mr. Bousquet then presented a detailed case study provided by Hopital Européen Georges Pompidou in Paris. In the example an integrated solution tracked all aspects of a patient’s treatment at the hospital, from admission in the emergency room, through examination by a physician, to lab tests, x-rays in the radiology department, discharge and after-care follow-up. Over 100 hospitals in France already have this system and there are now plans for a national database.

Mr. Bousquet saw a number of consequences from such developments. A mass of information is created for each patient and ICT, combined with emerging standards, allows this information to be made accessible online. This brings benefits in terms of increased quality, productivity, and traceability. But privacy and accountability are key challenges.

The various user groups have widely differing viewpoints and requirements. Patients will wish to ensure such developments allow them online access to information contained in their personal medical folder at anytime and to control who has access to that information. They will also need to trust that the information is being stored safely and is not being accessed by unauthorised parties. Professionals need to be able to trust medical information about the patient – their life could depend on it. In a paperless/filmless environment, this means having absolute trust in the system availability.

Professionals will wish to safeguard their accountability and independence in making decisions, and to accept that the information might be used to assess their own performance. Finally, administrations will wish to gather on a real-time basis information required to manage the healthcare system locally, regionally and nationally. Increasing quality and productivity and tracking malpractice will also be key concerns.

In conclusion, Mr. Bousquet noted that use of ICT in healthcare is not mature, but nevertheless it is becoming the daily tool for modern "care production". ICT will provide governments with necessary tools to manage their healthcare system better. However, safety, trust and security are major concerns for patients (i.e. citizens) and professionals.

How to Interact with the EU Institutions and Participate to the EU Decision Making Process

Mr. Pierre Longin, Director, Longin Conseil

The presentation was made at the request of Forum members, through the Working Group, so as to broaden the discussion of Hitachi and the EU within the Forum. Progressive enlargement has had huge benefits for the European Union, Mr. Longin explained, most recently through the accession of the ten new member states. "Its founders could not have anticipated what Europe is today".

At the heart of the EU is the European Commission comprising 25 commissioners and 22000 civil servants, and the European Parliament comprising 732 MEPs split into 8 political groups. The Parliament is a key part of the EU’s legislative process and has ‘co-decision’ on EU legislation with the European Council, representing the 25 national governments. Around 50% of amendments to legislation made in the Parliament and its 20 committees are incorporated into the final legal text.

Around 70% of national legislation now comes from

left to right
Mr. Mika Lauhde, Mr. Vincent Bousquet, Prof. Krzysztof Kurzydlowski,
Parallel working session, Mr. Mark Cantley and Dr. Michiharu Nakamura,
Mr. Mitsuo Yamaguchi, the Forum moderaotrs

Brussels. Hence, companies need to be well equipped to work with the EU institutions. Firstly, they must monitor what is going on, which most can do. But to be successful, companies have to move beyond this to issue management – measuring the impact of legislation on their business.

Early action is essential here: the earlier you get into the game, the earlier you can influence the process. Firms must mobilise collectively, within networks. "But remember a network is not the same as an address book", Mr. Longin observed. "Relationships have to be built on trust, which is built over years." "You inform for as long as you are not understood", Mr. Longin explained, "and until you are understood you cannot expect support." Industry should also lobby at national level and tell a consistent story.

Completing his tour of the EU institutions, Mr. Longin noted that "the tough nut" is the Council of Ministers. The best approach here is to develop close contacts with the Brussels-based permanent representatives in the Council.
Thus, dealing with Brussels involves passing over huge amounts of information and building many relationships. Good contacts and networks are key, Mr. Longin concluded.

PARALLEL WORKING SESSIONS

Working Session I: Safety, Trust and Security Threats

Contribution by Session Moderator: Mr. Marc Besson, Director of Professional Services, WISeKey

Threats are numerous in the fast developing world we are living in and represent a very broad subject to cover in a limited amount of time. Threats we are facing can be analysed in a societal, corporate or individual perspective. An initial brainstorming led to the identification of various threats among which terrorism and cyber-terrorism, pandemics, domestic accidents, medical error or population aging where reported with more emphasis.
ICT responses to those threats highly depend on the actors who formed them. As an illustration, ICT have been used in different ways to build a response to the potential human flu pandemic resulting from the evolution of the current avian flu crisis:

- At the international level, WHO is using blogs to collect information on suspect cases as an alternative information source.
- At the corporate level, enterprises are deploying virtual private networks to enable their employees to securely work from home as part of their contingency plan.
- At the individual level, persons are connecting to websites to collect information and to purchase Tamiflu© .

This example highlighted the role played by the Internet as a key vector in forming adequate responses to threats by becoming essential to the basic functioning of interconnected society.
Unfortunately, the Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing threats. If no measures are undertaken, we will rapidly face proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet.
The key component in managing this new form of relationship will be ensured by a major shift in the identity model. Identity tokens are not a new concept. In ancient Egypt, pharaohs used cartouches as their insignia, and for centuries royal seals have been used to authenticate royal charters and decrees. During the 20th century, an increasing set of identity tokens were needed not just for high ranking people but for all citizens, for example, passports and driving licenses.

The creation of a digital identity layer that could be used in digital interaction and transaction is now becoming an urgent need to cope with safety, trust and security threats.
In order to succeed and to be commonly accepted, preventing as such a "Big Brother" effect, digital identities should meet specific criteria. The group identified and agreed on a set of minimal rules:

- Respect of privacy supported by the diversity of identities providers.
- Low cost enabled by the use of open standards and interoperability and by a mass distribution of digital identities in a transparent and competitive market.
- General acceptation by keeping the user experience as simple as possible and by supporting the end-user with training and awareness.
- Trust provided by diversity in trust mechanisms and supported by strong authentication mechanisms such as biometrics systems.

These four sets of rules are in line with the latest research on digital identities, in particular with the research conducted by Kim Cameron and published in "The Laws of Identity ".

Among digital identity models, trust is the central component. In an analogue world, we trust an identity card because it was issued by a government and the physical document seems real, or because the person we are interacting with has been endorsed by somebody we already know and trust. How could this trust notion be transposed in a dematerialized interaction? In practice, two trust models have been, to some extent, replicated in the digital world.
The first one, designated as centralised trust model, relies on a trusted issuer who could be a government or a private entity, which has demonstrated strong capacity in validating the identity of a physical person before issuing his/her digital identity.
The second model consists of identity endorsed by another community member and can be assimilated to a kind of peer-to-peer trust model. It is commonly used in social network websites such as LinkedIn or OpenBC. In these systems, your identity is ensured through the network of contacts you build, inspired by the "friend-of-a-friend" concept.
A second implementation of the peer-to-peer model may be found in the eBay community. Each actor in this online auction receives an identity which enables him/her

to transact. The quality and the reliability of a seller are based on ratings granted by other users. Good ratings increase the chance of a seller to conclude a transaction. Trust in this case is derived from reputation.

Many of the dangers, complications, annoyances, and uncertainties of today's online experiences could now be over. The group strongly believed that a widespread deployment of digital identities has the potential to solve many of these issues, benefiting everyone and accelerating the long-term growth of connectivity by making the online world safer, more trustworthy, and easier to use.

Working Session II: Citizens Daily Life

Contribution by Session Moderator: Mr. Stephen White, Directorate Manager, Publications & Communications, The British Psychological Society

The group agreed to consider the questions posed as 'ordinary citizens' rather than experts in ICT, so that we could bring a lay, user perspective to our discussions

Our first question was:

" Which technology should be promoted to enhance safety and trust in citizens' daily use of ICT?"

First, we made two general points: we accepted that no technology could ever be 100 per cent safe; and secondly, we felt that the ordinary user probably did not care or even think very much about safety and trust issues. Furthermore, they often ignored the advice on such matters provided by ISPs and retailers who have many products available to ensure safe use. We also believed that most users had little interest in 'which technology' to use. Indeed, as technology is advancing so quickly and each advance increases the complexity, we felt it was impossible to give a direct answer to the question about 'which technology should be promoted' as the technology is likely to change radically and rapidly.

However, we believed that despite the many negatives citizens did want to use ICT and that some simple principles described their needs – ICT had to be 'reliable, fit for purpose and easily available'.

Another aspect of the discussion concerned whether there should be rules for ICT in the same way as there are rules for cars – i.e. rules for both manufacturers and rules for drivers? However, we accepted that 'driving ICT', as opposed to 'driving a car' was unlikely to kill anyone. But the car theme ran through our consideration and we agreed that, like a car, ICT equipment should be given a regular health check, or service to ensure safety. We believed that manufacturers, retailers, ISPs and even local government had a role to play in providing such a service either free, or at affordable prices.

A further consideration concerned the 'promotion' aspect of the question. We quickly formed the view that government probably had little or no role to play as such activity could potentially curtail individual choice and freedom. But we did feel that some commercial concerns may have a role – i.e. we felt that banks could insist on some basic rules/safety measures before individuals were allowed to use 'e' banking services.

Our second question was:

" How to educate citizens on best practice regarding safety and use?"

Whilst we accepted that the younger generation were the best educated on ICT use and therefore had the most (potential) knowledge of safe use, we also agreed that they were the worst abusers of systems and appeared to care very little about safety issues. Concern was expressed about how ICT use had enabled 'e' bullying and we noted the rare cases where, allegedly, children had been driven to suicide by 'e' messages. We felt that the moral and ethical dimension of ICT use should be taught within the formal education system.

For the older generation our view was quite different. As their use was lower, then their knowledge of safety issues would inevitably be lower. However, we were aware of the growing 'silver surfer' generation that is increasingly turning to ICT for leisure and to keep in touch with increasingly dispersed families. We were also aware that government, both local and national, is pushing the 'e' government agenda and providing services via ICT. Given this specific push, we felt that government had a significant responsibility to provide education – this must be free at the point of access and provided locally. Our argument was that as 'e' government is supposed to reduce costs, then some of these savings should be returned via the provision of free ICT education to help with the uptake of those 'e' services.

Our view was that manufacturers, retailers, ISPs and software developers should want to be seen to sponsor or even supply these educational opportunities in partnership with local government. This would allow these companies to get closer to their customers and, therefore, potentially the customers' trust in those companies and their products would increase.

A final point in terms of this question was the increasing number of immigrants coming into the developed world from countries where ICT use and availability was much more limited. Our concern was that for these individuals to fully participate in a modern democracy then ICT education was necessary and again should be available free of charge and locally.

Our third question was:

"How to protect citizens from data mishandling and more particularly how to protect weaker users e.g. children?"

Our basic analysis was that increasing amounts of data was being held on every citizen by both public and private organisations. It was hard, if not impossible, for the ordinary citizen to find out what data was held; who held the data; whether the data was correct; and, how to correct the data if it was wrong. Our solution was that each year every organisation that held data should send a copy to the individual so that it could be checked and if necessary corrected.

We were aware that within the EU laws existed on data handling, use and misuse and we supported the use of prosecutions to protect the individual. However, we were also aware that prosecutions happened after the event and often after damage had been done to the individual, so better monitoring of data use may mitigate the need for prosecutions and damage to the citizen. On the specific issue of ‘weaker users’, we were aware that software was available to provide protection. However, our view was that the control over the use of such measures must be in the hands of parents and carers; as such choices would inevitably vary from household to household. But again on the issue of data held on ‘children’, our view was that such data should be provided annually to parents/carers for checking and correcting.

Our fourth and last question was:
"How to protect citizens from external attacks e.g. spam, spyware and cookies?"
Although we were aware that many products are available from ISPs and retailers to offer protection, this could never be 100 per cent effective and the key responsibility in this area must lie with the individual user and the ISP to provide high quality protection on resident servers. Further, we believed that ISPs should provide an agreed pan-national level of protection against attack and that there should be stringent penalties for any ISP failing to provide this level.
A further recommendation was that a simple ‘code of practice’ should be developed for users. This could be displayed on the first logon page of every computer and include such advice as: not leaving your computer on all the time; and, keeping anti-virus software up to date.

Working Session III: Privacy Issues
Contribution by Session Moderator: Prof. Jos Dumortier, Director, Interdisciplinary Centre for Law and ICT (ICRI), K.U.Leuven

Privacy is a very large concept. It can be defined as the ability of an individual or group to keep their lives and personal affairs out of public view or free from intrusion by other persons ("the right to be let alone"). One aspect of privacy is what is commonly called "informational" privacy, which can be defined as the ability for a person to determine which information related to him may be communicated to which other persons ("informational self-determination").

The discussion in the parallel working session focused exclusively on this last aspect of privacy and in particular on the protection of individuals in the context of processing of personal data ("personal data protection"). In Europe the respect for privacy is a fundamental right of every citizen. It has received protection in the constitutions of most of the European countries and also in the European Convention on the Protection of Human Rights and Fundamental Liberties. In this last Convention the European citizens also received protection of their personal privacy against their own state. This right is sanctioned by the European Court for Human Rights in Strasbourg. After the European experience before and during World War II, the protection of individual privacy is being considered as a necessary condition for democracy. Without respect for privacy, citizens don’t have the possibility to behave freely and express themselves. Such a situation can very rapidly degenerate into a totalitarian society. The protection of privacy is therefore primarily a political and societal necessity in the context of a democratic state.
The discussion in the parallel working session has been based on this European understanding of privacy rights. This understanding may be different in other regions of the globe, in particular in the USA.
With regard to the protection of privacy restricted to personal data protection, four essential principles have been put forward during the whole discussion:

- The finality principle: personal data should only be processed for specific legitimate objectives and not be used further for other purposes which are not compatible to the ones for which these data have been obtained.
- The proportionality principle: because processing of personal data is "by definition" considered as a privacy intrusion, it should be restricted as far as possible. Only personal data that are necessary for the legitimate objective should be processed and they should not be kept longer than necessary for this objective.
- The transparency principle: personal data should, as a rule, never be processed without the person concerned having been informed correctly. Every individual should have the right to get access to personal data related to him.
- The security principle: controllers of personal data should take adequate measures to protect personal data against unlawful access.

Proposed Recommendations
The participants of the parallel working session reached a consensus on four types of recommendations related to the protection of privacy. The recommendations relate to a) education, b) technology, c) standardisation and d) regulation.

Education
Privacy may be an essential condition for individual freedom and therefore also a conditio sine qua non for a democratic society. Nevertheless, privacy values are unfortunately not sufficiently rooted in the contemporary public opinion. Privacy is therefore seldom considered as a political and societal priority. This is the reason why privacy is often too easily sacrificed in exchange for more security and efficiency.
Efforts are thus needed to give privacy values stronger roots in the public mind. This is a task for our educational system. Privacy should be included into the agenda of our school programmes. School teachers and other educators should be stimulated to put more emphasis on privacy values in their classes.
Other initiatives can be taken to increase privacy awareness. One possibility is to subsidize privacy-promoting associations or awards for specific privacy-enhancing initiatives.
Participants in the working session agreed on the fact that privacy laws contain a series of very useful rights for users in the area of personal data protection, such as the rights of access and correction. Unfortunately, these rights are very rarely used in practice, partly because few people are aware that these rights exist and how they have to be put in practice. Therefore it was suggested to stimulate and actively support initiatives to

assist users in exercising their privacy rights (following the example of consumers' associations).

Technology

In recent years efforts have been made to develop privacy-enhancing technologies. One example is the possibility to block calling line identification on mobile phones. It is necessary to further invest in such privacy-enhancing technologies but at the same time efforts are needed to make them more user-friendly and easy to use. Users should be able to express their privacy preferences as much as possible in an intuitive manner, within any application or technological solution and without loosing comfort, speed and easiness.

Standardization

Personal data protection legislation is very complex and not easy to implement for companies and individuals. Therefore it is necessary to translate the legal principles into practical guidelines and standards which can be more easily implemented. At the same time privacy compliance can become something which is auditable. This would permit the establishment of conformity assessment schemes. Companies could receive privacy "quality labels" for products, applications or services before introducing them on the market.

Regulation

The preceding recommendations should not lead to the conclusion that nothing needs to be done on the level of privacy regulation. More effective regulation is certainly needed. Privacy compliance should be more systematically monitored and enforced. Regulation should avoid complexity and remain generic in order to keep sufficient flexibility.

In the context of the European Union, divergences between national laws and policies in the area of personal data protection should be progressively eliminated. The 1995 European data protection directive has harmonized the regulatory framework in Europe to a large extent, but there still remain many differences in the practical implementation of the rules. Moreover, the large number of small detail differences between national laws result in a fragmented regulatory landscape. This increases the complexity for companies and organisations and is therefore an obstacle for privacy compliance.

Besides the European harmonisation, it is also necessary to strive towards a global consensus on a series of basic data protection principles. This should avoid the emergence of privacy "havens" and distortion of international competition.

General comments

During the discussion in the parallel session many participants highlighted the relationship between privacy and trust. Privacy is seen as the ability for everyone to determine in which circle of trust personal data will be shared.

Sometimes privacy can be enhanced by introducing trusted third parties. The services of these trusted third parties should be used wherever they can contribute to more privacy for citizens, subscribers, users or other individuals. Many applications in the public and private sector can function perfectly well without a need to collect identification data. It is frequently sufficient to collect credentials (for example: controlling the age of a person before permission to access).

Last but not least it should be mentioned that privacy values are closely linked to culture and tradition. Privacy values are not universal.

Working Session IV: Digital Divide

Contribution by Session Moderator: Dr. Ilkka Tuomi, Chief Scientist, Oy Meaning Processing Ltd

The Working Group defined the digital divide as "economic, social or cultural deprivation generated by missing ICT access and skills."

This definition goes beyond conventional definitions and has a number of practically important characteristics. It explicitly spells out the three dimensions where digital divides are important and where ICTs make a difference. Firstly, in the modern knowledge- and information-based world, economic opportunities, such as employability, depend on ICT access and skills. Secondly, ICTs play an increasingly important role in all social relationships, ranging from political participation to connecting local communities, friends and the family. Thirdly, in the global and culturally diversified world, ICTs are increasingly important for access to cultural resources and expression. These three dimensions generate different types of challenges, and different policy domains and actors are involved in each.

Lack of technology, per se, is not always a problem. It is clear that technology remains inert and useless without necessary human skills and competences. Technologies become real when they are combined with knowledge and capabilities to use them, and when they are embedded in social practices. In discussing digital divides, therefore, we have to reject purely technological characterisations, and discuss appropriate combinations of technological and human capabilities.

Technology-focused measures of digital divide are also inaccurate measures of deprivation, as people often prefer to use complementary technologies and social resources. The fact that until a couple of years ago, many CEOs of big corporations did not use a PC, and asked their secretaries to read their email, would not push these CEOs to the other side of the digital divide. To the extent that the lack of access to ICTs does not generate deprivation, there is little point in talking about a "digital divide."

Conventional views of the digital divide, therefore, are rather misleading. Instead of asking: "Do you have access to a computer with a modem?" we should focus on the real impact. Furthermore, the focus should be on actual deprivation generated by the lack of competent access to ICTs. For example, we should ask: "Are you unable to find a job because you don't have necessary competences and access to ICTs?" Similarly, we can ask whether the lack of access to ICT and ICT skills is, in practice, making it difficult for someone to participate in decision-making, act as a citizen in society, or learn new useful skills and educate oneself.

As new technologies emerge and diffuse in society, there are always early adopters and later-comers. When measured by technology use, user and non-user gaps always exist. This has been the case for the steam engine, the railway, the radio, the car, the telephone, and the computer. From the policy point of view, some of these technologies have been considered so important that they have been provided fully or partially as public services and public goods. This was the case, for example, in public broadcasting. Many innovations, however, have diffused in society without policy intervention and promotion. The interesting question is whether ICTs are somehow different than earlier technologies, and whether special policies are justified.

It is possible to argue that ICTs, indeed, are historically special and unique. Access to global knowledge and communication networks may well become a pre-condition for effective operation in the knowledge society, and it is possible that ICT becomes the entry point for economic, social and developmental opportunities. "Equal opportunities," therefore, could in practice mean access to ICT.

Furthermore, ICTs provide access to resources such as knowledge, which accumulate. It is therefore possible that early adopters move fast, and laggards become increasingly disadvantaged. Such a "trickle-up" developmental dynamic could be socially and economically highly problematic. The modern innovation economy presents qualitatively new challenges for advancing broad social prosperity.

The Working Group therefore concluded that beyond all the hype and limitations of early conceptualizations of the digital divide, there is a proper argument for highlighting its importance. We assume that in the future lack of access to ICTs and related skills will generate deprivation, and this will have a profound socio-economic impact. Policy is therefore relevant, and it can be most efficient when problems are still limited. Even when it is clear that, on average, access to ICT is increasing, policy is needed to address emerging challenges.

Specifically, new technologies can both create new divides and reduce existing ones. Policies should, therefore, aim at: 1) avoiding the creation of new divides; 2) shrinking the existing divides by actively using ICT for development; and 3) eliminating already generated ICT-related divides, for example, by designing for usability.

An important design principle - both for policies and technologies - is to start from the fact that information and communication technologies are essentially social technologies. ICTs mediate social, economic, and cultural interactions, and ICTs become meaningful only in a social context. The importance of social and cultural dimensions of ICTs is now rapidly becoming visible, and many of the fastest-growing uses of ICTs are explicitly social. This shifts the balance from the purely functional aspects of ICTs towards the way technology is integrated into social processes. Thus, technologists will need to give even greater attention to users' needs and requirements and to understand users as social and cultural actors.

The basic starting point for designing future policies and technologies, therefore, should be to respect social and cultural diversity. For example, in the area of security and safety, populations have different expectations concerning the trustworthiness of governments, policymakers, public servants, and economic and cultural institutions. The concept of privacy is fundamentally different in Japan, where dense cities and paper walls have existed for centuries, from what it is, for example, in Finland, where 11 persons live per square kilometre, on average, and where the number of lakes roughly equals the number of inhabitants.

The digital divide, therefore, can not be understood as simply "being in or being out." ICTs generate the infrastructure for complex social interactions where multiple perspectives are represented and expressed. Modern societies are based on a complex division of labour and diversified social practices. The 'digital divide' therefore does not consist of or align with a single boundary. Instead, ICTs restructure existing boundaries, erode traditional boundaries and make them visible in new ways. This increasing visibility of social and cultural factors means that in the future we have to better understand the "soft" dimensions of design. For example, designers will have to understand culturally and historically embedded value systems and how these are expressed in political debates on privacy, access to knowledge, and rights and responsibilities. In general, this means that both policy and technology designers need increasingly sophisticated skills and concepts that facilitate meaningful and productive discussion on ethical and political aspects of ICTs.

The main conclusion of the Working Group is, therefore, that ICTs are fundamentally social technologies, which have a broad impact on social participation, human development, and economic opportunities. Digital divides are of critical importance for policymakers, citizens, and industry. To address the emerging challenges, Europe's ICT industry needs to strive to shrink existing divides, to avoid creating new ones, and to eliminate already generated ICT-related divides. This will open major opportunities for new products and services for companies that truly combine social and technical development.

Working Session V: Business Impact / Business Model

Contribution by Session Moderator: Dr. Pierre Beuzit, Vice President, Renault SA

I – Business impact

It is obvious that ICT drastically change business.

If we consider research and development activity as an example; major changes are permitted by the usage of ICT:

- the possibility to externalize part of it without loosing any agility and flexibility, in order to use the best expertise across the world.
- to work 24 hours a day (speeding up by factor 3 without any discontinuity)
- and by the way to shorten significantly the development phase
- and finally to increase the competitiveness of the industry

But we are conscious that this new way of working creates new problems in terms of safety and security. In fact, it induces a new type of relationship between the partners of the business.

The first impact concerns the responsibility of each. In order to guarantee the safety aspects, it is necessary to define precisely who is responsible of what, and of course to cover the complete field of activity.

The second impact, which is related with the first one, concerns the confidentiality and the reliability of the exchanged information. Some techniques exist to "guarantee" more or less this type of confidentiality, but that is important from legal point of view.

These problems can be solved by complete and detailed contracts between partners.

II – Citizen Concerns

One question is: how might citizens' concerns slow down technological deployment? Of course citizens often feel worried about new technologies, by the effects they could have on their own "comfort". One example was given by the attitude to genetically modified food.

In fact we consider that the behaviour of people is the result of the evaluation of two aspects of the problem. On one side, they consider the benefits given by the usage of the new technology (not only for the company but also for themselves); on the other side there are the risks as the impact on the private life and the constraints induced.

We consider that two rules must be followed: each person has the freedom to accept the conditions of using the technology; and has the assurance that he will not be tracked by the system.

We understand that it could result in discrepancies between the orientations of the company and the individual tendency. There is no easy solution to conciliate these two positions; the only way is based on the education of the employees and the customers involved in the usage of ICT. In fact the problem to solve by education is to conciliate the fundamental rules of the democracy with an easy and flexible use of the new technologies.

III – New Business Models

To assure the efficiency and the safety of the business and to protect the citizens, it is necessary to create a new type of relationship between the partner companies, between the company and its employees, and between the company and its customers. That means that all the relations are modified.

As mentioned above, ICT allows working simultaneously with people anywhere in the world, from different native languages, different working habits, etc. On another point of view, if we consider the supply chain, in the past the deal was bilateral between the levels N and N+1, that means between people who used to work together. Now the technologies allow all the levels to be involved at the same time in order to accelerate the process and to find a better optimum.

The business model must guarantee that all the actors are winners; that means:

- to guarantee the confidentiality of the information and the rights related to the intellectual property (very important to work with SMEs')
- to assure there is no impact on individual freedom.
- and for the principal: to keep the control of the databases

The risk is that some companies will not be able to comply with the requirements and would no longer be accredited.

IV – Impact on Employment

Some aspects could have a negative impact, such as the possibility to outsource a part of the business and changes to working practices from some evolutions of the jobs and the usage of new technologies.

Other aspects have clearly positive impact: the first of them is to improve the competitiveness of the industry, with the consequence of maintaining or even development of employment. New business can be permitted by the development of new activities. More freedom for the employees by allowing to work anywhere at any time (of course it is a new way of working).

Finally, we consider that if people are educated correctly to use in a good way these technologies the benefits for the citizens and the company would be superior to the risks.

Panel Discussion

The Forum concluded with a panel debate involving the speakers and session moderators, at which participants were invited to raise questions on all they had heard. The participants used the opportunity to home in on the key issues that had arisen during the meeting.

"The Forum had identified that education was key. What tools are to be used? How would it be differentiated? And who would pay for it?" one Forum member asked. Lord Erroll thought there was a risk of people reacting too late. People only learn when they are interested – the European Computer Driving Licence (ECDL) was a valuable example.

Forum member Mike Parr commented that: "Who pays is linked to who benefits. How do you sell the idea of ICT to over 30s?" Local government, as a deliver of services, rather than central government was probably one of the best ways of pushing ICT out into the community. Lord Erroll agreed that central government would not move fast enough. Prof. Dumotier's group had looked at education in citizenship, values and fundamental rights, rather than technology. The group thought this needed to be made an elementary part of the education system.

Following on from this question, Eckhard Kroll asked the panel: "What are your recommendations for keeping knowledge up to date throughout life?" Dr. Tuomi commented that the impact of informal learning is clearly increasing and in many areas formal learning is becoming irrelevant. Dr. Bus said much of education is 'learning-by-doing'. With privacy-enhancing technologies, devices must be intuitive enough to stimulate people to use them in an optimal way. Thus, the main contribution of technologists is in designing systems that people want to use.

Fabrice Axisa queried Working Group I's reliance on the peer-to-peer trust model. "Didn't this violate personal

left to right
H.E.M. Ikuo Mizuki,
Mr. Simon Davies

privacy?" Mr. Besson replied that the model was valid where low-level identity was required but was not suitable for exchange of sensitive information. LinkedIn was quoted as an example of this type of model only. Lord Erroll noted that LinkedIn mirrored a traditional way of behaving – an introduction through a mutual contact – and hence had a good chance of success.

Mark Cantley was concerned with diffusion of ICT. "What proportion of the world's 6 billion population has access to the internet now, and will have access in 10, 20, or 30 year's time?" he asked. Dr. Tuomi agreed it was an important question. He didn't have the figures. But the issue was whether we create content for everyone? Prices are falling rapidly and will continue to do, so in the future computing and communications will be almost free, even in developing countries. But as these traditional barriers fall, it will push privacy issues into a new dimension. Prof. Muraskiewicz agreed that we had arrived at the real philosophical problem: trust and security in a truly global interconnected world. Living in this new universe of cyberspace will force us to look for new approaches to human sociology and psychology, he believed.

Hitachi in Europe: A Corporate Presentation

Sir Stephen Gomersall, CEO, Hitachi Ltd.

The presentation provided a short profile of the Hitachi Group, an overview of its presence in Europe, and the key messages to European stakeholders.

Hitachi is one of the largest and most innovative technology firms in the world. It ranks third in the Fortune 500 for global sales in electronics, electrical equipment and computer industries, and is number two in patent applications at the US Patent & Trademark Office. Hitachi's mission is to provide value for customers and to society at large, and the senior leadership is committed to making the business more global and competitive.

The Hitachi Group now operates in seven industry segments: information & telecommunications; electronic devices; power & industrial systems; digital media & consumer products; high functional materials; financial services; and logistics, services & others. Consolidated turnover in FY2005 was US$80.9 billion from over 40,000 products and services. There are approximately 355,000 employees worldwide, split across over 900 subsidiaries.

In Europe, Hitachi has 24 operating companies, 5,300 employees and total revenues of US$6.3 billion. The company's strength is in technologies and systems supporting social infrastructure and information systems, with a focus on seven key growth sectors: power generation, transportation systems, construction machinery, air-conditioning, storage systems, digital consumer, and automotive systems. The European Headquarters, headed by Sir Stephen, provides coordination, brand development, business development and public affairs. The Mediterranean and Central & Eastern Europe are being targeted as the main growth markets.

Research is the essence of Hitachi. Its R&D laboratories form a global network working on a wide range of cutting-edge topics. Worldwide, the Hitachi Group employs 4,500 researchers and spends around US$3.7bn per annum on research. Hitachi innovation enables its customers to innovate in their markets: through technologies such as finger vein recognition. Research activities in Europe are distributed across seven main locations: Dublin, Cambridge, Munich, Paris, Milan and Sophia Antipolis.

For stakeholders, the key message is "Hitachi creates first class technology which improves your life". This is portrayed through a variety of marketing campaigns.

Closing of the Forum

Dr. Michiharu Nakamura, Executive Vice President, Hitachi Ltd

Dr. Nakamura thanked all participants for attending this year's Forum, including speakers, group moderators, Forum members, and distinguished guests. Special thanks were due to Dr. Freymond, who had dedicated himself to the Forum's success.

Mr. Nakamura had found the discussions exciting and fruitful. Safety, security and trust are major concerns in our daily lives, he observed, and the Forum had discussed many aspects, including business impacts and the contribution of ICT.

"We can't go back to the previous era before ICT", Mr. Nakamura noted. "We believe in ICT and its optimal deployment for society". The Forum had provided a great opportunity for scientists and non-specialists to get together as part of a deeper and interdisciplinary discussion. The Forum was both informative and successful, and he looked forward to continued efforts to contribute to the development of European society.

A presentation was made to Mr. Mark Cantley, on his retirement from the European Commission, in recognition of his help and support for the Forum over the years.

Speakers

Mr. Marc Besson	Director of Professional Services, WISeKey
Dr. Pierre Beuzit	Vice President for Research, Renault S.A.
Dr. Ian Brown	Senior Research Manager, the Cambridge-MIT Institute, & Board Member of European Digital Rights (EDRi)
Mr. Vincent Bousquet	V.P. & G.M. Medasys, Healthcare Operations
Dr. Jacques Bus	DG Information Society and Media, Head of Unit, ICT for Trust and Security, European Commission
Mr. Simon Davies	Visiting Fellow, London School of Economics & Director, Privacy International
Prof. Jos Dumortier	Director, Interdisciplinary Centre for Law and ICT (ICRI), K.U.Leuven
Lord Merlin Hay, The Earl of Erroll	The House of Lords, UK
Sir Stephen Gomersall	Hitachi Group Chief Executive for Europe
Mr. Mika Lauhde	Director, Nokia, Technology Management, Customer and Market Operations
Dr. Stephan Lechner	Head of Security Research, Siemens AG Corporate Technology
Mr. Pierre E. Longin	Director, Longin Conseil
Prof. Mieczyslaw Muraszkiewicz	Deputy Director, Institute for Computer & Information Engineering, Warsaw University of Technology
Mr. Bart Van Rijnsoever	Department Head, Information & Security Systems, Philips Research
Mr. Martin Sadler	Director, HP Security Laboratory, Hewlett Packard
Dr. Ilkka Tuomi	Chief Scientist, Oy Meaning Processing Ltd
Mr. Stephen White	Directorate Manager, Publications & Communications, The British Psychological Society
Mr. Mitsuo Yamaguchi	Chief Operating Officer, Hitachi Ltd., Information & Telecommunication Systems

Forum General Moderator:	Dr. Jean F. Freymond, Director of the Centre for Applied Studies in International Negotiations (CASIN), Geneva, CH
Report Prepared by:	Michael Sharpe, MS Consulting & Research Ltd, Birmingham, UK

Working Group 2007

The working group was set up in 1999 to give the Forum members the opportunity to become more personally involved in the selection of the Forum topics, and subsequently in shaping the Forum agenda. The current working group consists of the following members:

Cécile Cappeau	Andorra
Reto Grob	Switzerland
Sander Hansen	The Netherlands
Olivier Pech	France
Geert Somers	Belgium
David Sporn	France

Acknowledgement

It gives me great pleasure to extend my thanks to the distinguished speakers and moderators who contributed to this year's Forum. I would also like to thank all of this year's Forum attendees whose active participation and enthusiasm lead to very vibrant and constructive discussions.

I would like to express my deepest gratitude to Mr. Jean Freymond (CASIN) who kindly accepted to be this year's Forum general moderator and who performed his task with the utmost professionalism.

My sincere appreciation also goes out to the Working Group members who kindly gave up some of their free time to help us shape the agenda for this year's Forum and to discuss and propose possible changes in order to continuously strive to improve the Forum. I would also like to sincerely thank the Forum Fellows, whose contributions have proven to be a key asset for the Forum and, particularly, I would like to congratulate Mr. Didier Gambier (EU Commission) and Mr. Antoine Ripoll (EU Parliament) who have kindly accepted to become Forum Fellows.

Finally, I would like to address a special thank you to Mr. Mark Cantley, who as Forum Fellow, has been a great supporter of the Forum for many years and who will soon retire from the European Commission. I am sure all Forum members join me in wishing him a very pleasant and active retirement.

Ko Takahashi
General Manager
Hitachi Corporate Office, Europe

For more information about the EU Hitachi Science & Technology Forum, please contact

Hitachi Corporate Office, Europe
Avenue Louise, 326, box 11
1050 Brussels
Belgium

Tel: +32 2 643 48 88
Fax: +32 2 640 08 98

Forum Homepage: www.hitachiforum.com

9th EU Hitachi Science & Technology *forum* 2006

EU Hitachi
Science & Technology
forum
ICT for safety, trust and security:
its impact on European citizens
19-21 May 2006
HITACHI

HITACHI
Inspire the Next

Designed by Challans & Faber bvba, Printed in Belgium, June 2006