



trustis

Trust in the Information Society

10-11 of February, 2010

León, Spain

Conference Report

Rapporteur: José A. Mañas

18.6.2010

1 Index

1	Index.....	1
2	Objectives of the conference.....	3
3	Conclusions and Recommendations	3
3.1	Conclusion #1.....	3
3.2	Conclusion #2.....	4
3.3	Conclusion #3.....	4
3.4	Conclusion #4.....	4
3.5	Conclusion #5.....	4
3.6	Conclusion #6.....	4
3.7	Conclusion #7.....	5
3.8	Conclusion #8.....	5
3.9	Conclusion #9 - e-identity.....	5
4	Summary of the sessions on February 10th.....	6
4.1	Opening Session.....	6
4.2	RISEPTIS report (“Trust in the Information Society”).....	8
4.3	Trust in Digital Life – an Industry View	9
4.4	Trustworthy Networked Service & Computing Environments	13



4.5	An European Framework for e-Identity Management	16
5	Summary of the sessions on February 11th	19
5.1	Technology Development and the EU Legal Framework of Data Protection and Privacy.....	19
5.2	International Cooperation on Trust and Security Research	22
6	Annex A – Agenda.....	27
6.1	February 10th.....	27
6.2	February 11th.....	28
7	Annex B – Background: The recommendations of the RISEPTIS report on Trust in the Information Society.....	30
7.1	Recommendation 1:.....	30
7.2	Recommendation 2:.....	30
7.3	Recommendation 3:.....	30
7.4	Recommendation 4:.....	30
7.5	Recommendation 5:.....	31
7.6	Recommendation 6:.....	31
8	Annex C - Conclusions of Leon.....	32



2 Objectives of the conference

Internet is a fact, but unfortunately it was not designed with trust in mind. If in Europe we want to benefit from the opportunities of a digital world, we have to use the network according to our values, and respecting our laws. We need a net we may trust. The RISEPTIS¹ report is the key background material for the topics to be addressed (its final recommendations are given in annex).

The open issues addressed in this conference may be summarized into:

- how, and how much collaboration we need between private and public actors
- what may be left to the market and where is regulation needed
- how can we balance the different requirements of privacy, accountability and reliability
- how can Europe collaborate with other actors

3 Conclusions and Recommendations

Overall considerations that arose in the discussions:

1. Currently we have a lot of technology. It may be we have technology enough, and even too much technology; but it may also be that we lack some technology. In any case we have technology deployed without built-in security, privacy and trust. There is a question whether we should redesign the architecture from the beginning.
2. We have an obscure understanding of use cases. We are still discovering new things we can do, or we want to do, and then try to do it with deployed technological solutions that were never designed for it. On the other side, users have little experience, training, and informal education on how to live in a digital world.
3. We have a legal framework without built-in coverage of the new scenarios of use. There is a question on how to keep legacy and provide a sound basis for new approaches. For an effective digital world, we need to align technology and legal frameworks to fulfil the intended scenarios of use.

3.1 Conclusion #1

We need secure systems. Security must lead to predictable systems, which are the basis for trustable services.

¹ <http://www.think-trust.eu/>



3.2 Conclusion #2

We need a clear understanding of use scenarios and understand the expectations of the different parties involved: citizens, industry and governments.

There is an urgent need to understand and tame the complexity of the borderless services and the interactions between services.

3.3 Conclusion #3

We need to define metrics, and instruments to measure the success of implementations in order to know whether the objectives are reached, or how far they are.

3.4 Conclusion #4

Users must have effective control:

- clear options to choose from
- smart transparency: where 'transparency' stands for access to the information that is associated to it, and 'smart' stands for avoidance of tricks, half-truth, and partial information of data or consequences of the data collected

3.5 Conclusion #5

We need a regulatory framework and policies that establish the rules for every party

- clear statements of compliance for providers
- awareness of the rights and duties of the parties
- accountability, and allocation of liability
- protection of users with low education
- effective power to authorities to enforce compliance and investigate both preventively and reactively

We need regulation that is abstract enough to establish the rules for current and new services that may arise in the future. That is, we need to tame current technology and future technology such as the Internet of Things.

3.6 Conclusion #6

We need regulation on the minimal information needed for a transaction. And users need technological support to control the disclosure of information, being aware of the information that is disclosed, the association to their e-identity, the accountability of the disclosure and the liabilities of the actors, especially with respect to privacy.



3.7 Conclusion #7

Providers should incorporate security and trust into the design. In order to achieve this objective we need clear incentives for the market to avoid surprises and patching.

We need means to require providers to demonstrate their trustworthiness by objective means, showing assurance that they comply. This must be done in a transparent and non-arbitrary manner.

Minimal disclosure should be built into the design.

3.8 Conclusion #8

We need international cooperation, and inter-sector cooperation for a seamless network where user rights may be protected everywhere.

3.9 Conclusion #9 - e-identity

Due to its importance e-identity deserves a section by itself.

On one hand, we need to align the electronic identity with the physical identity, in particular in the enrolment phase so that there is a legal basis for identity.

Then, we need to define rules of minimal disclosure to avoid abuse of identity to profile users without their consent, or taking advantage of their inability to understand the consequences of identifying themselves in the network.

We need as well an effort to align country-specific legal framework into a global framework that makes a clear statement of liabilities of the parties, especially of those issuing attributes bound to e-identities.



4 Summary of the sessions on February 10th

4.1 Opening Session

Formal opening by Victor Izquierdo, Director General of INTECO (The National Institute of Communication Technologies), Ministry of Industry, Government of Spain.

Formal welcome by the Major of León, D. Francisco Fernández.

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

4.1.1 Mario Campolargo

Director of the "Emerging Technologies and Infrastructures" Directorate of DG-INFISO.

Summary

Internet is a fact, an opportunity and a risk, affecting our private life and commercial activities. Europe has an opportunity if due attention is paid. This conference is expected to discover areas where research and regulation are needed.

Key points from the presentation:

- **Internet:** it is a fact, it is everywhere, and it is The Way for new generations (digital natives); Internet is connecting web, mobiles, things, and computing into a single big and pervasive thing (about 70% of Europeans use Internet daily)
- **Vulnerable:** current society depends on massive data collection and information, but it has not been designed with security in mind, so we are vulnerable: people, industry and governments are concerned about the trust it deserves
- **Open issues:** a number of issues lack a clean answer: protection of privacy, management of identity, and liability
- **Single Online Market:** the Digital Agenda is at the core of the new policy framework, and we regard trust as a key enabler
- **Needs:** to keep the Internet free and neutral, stimulating industrial inversion
- **EU response:**
 - R&D – securing the architecture; protecting against threats; enabling the management of privacy, identity, and trust; with sound engineering principles and technologies
 - innovation and industrial agenda



- policy + standardisation + regulation

4.1.2 Francisco Ros

State Secretary of Telecommunications and for the Information Society, Spanish Government.

Summary

In Spain there is a large number of activities promoting the usage of Internet services and paving the way for a secure usage by every citizen. Special mention to INTECO, promoting a secure use of the network, and the e-ID (DNI electrónico) that allows every citizen to login and sign using secure means of authentication. However, there are problems to get everybody online, especially elderly people that do not feel confident with the new technologies.

Key points from the presentation:

- **Spanish presidency:** very strong interest to promote the digital agenda for 2010-2015, now we start a new mandate
- **Education:** it is essential to educate people on responsible and secure use of information and communications technologies (ICT)
- **Internet,** the network of networks is a major engineering achievement that is a fact, and an opportunity for productivity
- **Security** is a need, but must live together with privacy
- **INTECO,** an European reference on security on Internet
- **DNIE** (Spanish e-ID): a device we must exploit: i.e. personalised services with legal value to establish binding contracts on the net
- **electronic signature,** Spain has a large number of users: this must be the basis for the development of new services
- **Asymmetric penetration:** high number of young people, but a deficit on elderly people
- **USA:** we must align efforts and unify criteria with other regions, although we first need a unified position in Europe

4.1.3 Partial conclusions

- the **Digital Agenda** is an opportunity for Europe to benefit and drive the Information Society into a Single Digital Market
- **Concrete resolutions:** we expect from this congress recommendations on the actions to take



4.2 RISEPTIS report (“Trust in the Information Society”)

4.2.1 George Metakides

Chairman RISEPTIS, University Patras

The RISEPTIS² report itself is not presented, since it is widely known.

Summary

Internet is the technology that quickly has become a common place in our life. Unfortunately, security was not part of the design, and we are trying to patch it afterwards. In fact, initial designers did not forecast the possible uses of the net, and there is a serious problem to keep the network well organized in a number of quickly changing scenarios, that intermix in a new way of performing private and commercial relations. Current situation is that trust is not guaranteed, but a number of activities, like this conference, are being carried out to find out what has to be done in order to establish the grounds for a trustable Internet, combining both technology, and overall governance.

Key points from the presentation:

Mr. Metakides focuses on its evolutionary experience on trust, from old days where trust was measured in terms of bits in cryptographic keys into the current holistic approach to understand processes.

Currently, the complexity of Internet is similar to the complexity of one human brain, and the network is growing, while the brain is stable.

1. **1993:** EU delegation to the States: a conference about “security and privacy”: the subject was “the number of bits needed in cryptographic keys”
2. **Explosion of Internet:** currently the number of sites is similar to the number of neurons in a human brain; and the net is growing
3. **Transformational effect of Internet:** qualitative change
e.g. social networks: a new phenomenon, and new dimensions are to appear
4. **History:** in the past we have had centuries to adapt society to technological evolution; now technology changes faster than persons and
Electricity is similar to web:
 - it started slowly in industry
 - households were afraid; it took more than 40 years to become ubiquitous
 - now: pervasive

² <http://www.think-trust.eu/riseptis.html>



5. **Trust:** a [new] political priority – less than 5 years ago
now: an increasing number of political statements around trust in Europe and everywhere
 - Malmoe, León, Barcelona, Commissioner Reding, ...
 - H. Clinton: “we should synchronise technological progress with our principles” (e.g. anonymity has pros and cons)
6. **RISEPTIS:** a decision to focus on some issues to recommend on
 - network security: when created, security was not in mind; now we patch reactively
 - system safety: we need system metrics, and safety economic models
 - privacy : security was not in the design
 - governance: need for legislation that does not cripples the system
 - e-ID: is not the mere translation of traditional identity into bits; the issue is to introduce sufficient flexibility, so that minimal disclosure can be implemented
 - trust, security and privacy are no longer of marginal importance

4.2.2 Partial conclusions

- currently, we suffer from a lack of concepts in design: security, privacy, ...
- technology and innovation: security and privacy should be taken into account from early research and design stages
- lack of metrics
- end user: enable informed decisions
- policy and regulation: useful balance between protection, accountability and liability

4.3 Trust in Digital Life – an Industry View

Chair: Van Rijnsoever (Philips)

www.trustindigitallife.eu

An open initiative to work with society and industry, public policy makers, and academia

Currently, there are 3 working groups

- use cases
- requirements on technology
- law and technology



4.3.1 Ksheerabdhi Krishna (Gemalto)

Summary

The opportunities that the net opens will only succeed if the focus is placed on the user. The end user needs to trust on what he is doing, and that will only happen if events are under his control. That requires visible security and that he feels that the management of his e-identity is under his control. Education on how to live in the digital world must start moving current elements of trust from physical to digital.

Key points from the presentation:

- Internet opens an option to exploit
- trust is a need
- need: security + privacy + trust + convenience
- citizen-centric: the challenge is to translate into digital context tangible facts that people trust
- the user must be always in control: expert users, and those with lower education
- 3 pillars:
 - identity management: creation, storage, usage
 - data protection: storage of data
 - security in the transaction:
- strong authentication
- minimal disclosure

4.3.2 Luis Fernando Álvarez-Gascón (GMV)

Summary

The key for the success of the net is that users recover the control. We need to avoid both a world ruled by technology push and by market ambitions, and place the net under the rule of law. There is a concern with the economics of transactions; the idea of free contents is corrupting the perception and hiding the fact that very often you are paying with your personal data. The perception of free contents as a right is destroying the right to privacy. Privacy should be built into the design, and we should work to make the net conform to our views of rights and values so the net is trustworthy in the first place.

Key points from the presentation:

- never forget that we are dealing with people



- revolution does not happen when society adopts new technology, but when society adopts new behaviours
- trust is about the ability to deal with an scenario of risk: education is needed
- Internet - shift in power
 - early days: architecture drives the net: “the code is the law”
 - currently: market drives the net
 - the future: law drives the net
- we need a more regulated Internet to protect privacy
- we need incentives to adopt new technologies e.g. electronic identity cards
- issues
 - privacy by design
 - too much focus on data transmission, forgetting data protection
 - users are losing effective control of their data
 - identity management
 - free is a buzz word, what does it mean?
 - minimal marginal cost is a fact
 - digital property problems
 - perception of free as a right
 - data is the currency
- Trustworthiness
 - the weakest point is the user equipment
 - critical infrastructures
 - certification schemes
- Europe has an opportunity, and an obligation, to shape cyberspaces to conform to their views on rights and values

4.3.3 Laila Gide (THALES)

Summary

Security is something we are used to build into the products, but trust is a new dimension that comes into scene as soon as there are humans in the loop. For systems to be trustworthy we need to add new actors into transactions: trusted advisors that are informed agents which the users may trust in order to work with distant service providers. Nevertheless,



research is needed to measure trust, and manage e-identities when different domains are involved in a transaction.

Key points from the presentation:

- security: problems in products
- safety: problems from the environment
- trust is a new concern because the human is moving more and more into the loop: failures are coming from humans: thanks to product certification
- research domains:
 - trust evaluation
 - trust is not controlled by technology, but a social contract between society and technology
 - we need context-adaptive security, and policies
- new needs
 - inter-domain identity management
 - formal methods
- security by design is not enough: systems are too complex, dynamic and multi-layer service providers with interfaces
- we need metrics and continuous measurement
- proposal: add TTP: trusted advisors between service providers and service users

4.3.4 Craig Wittenberg (Microsoft)

Summary

Craig presents the evolving approach of Microsoft to engage in the community through his long personal and first-hand experience working for Microsoft.

He presents the evolution from designing, developing and making secure its own protocols, to adopt open protocols and try to reduce the gap between what users perceive as their needs, and the solutions provided in products. He expresses a strong commitment of Microsoft to hear and participate in open specification scenarios, and presents some examples such as OpenID, and minimal disclosure. The final aim is to offer products that are trustable and usable, responding to the scenarios identified.

4.3.5 Partial conclusions

- there is a need to educate users to live in the digital world
- we should emphasize usability or convenience as driving factors



- we should enforce privacy by design
- it is necessary to analyse the role of certification
- we need to measure, evaluate and certificate trust

4.4 Trustworthy Networked Service & Computing Environments

Chair: Willie Donnelly (WIT, THINK-Trust)

4.4.1 Francisco García Morán (CE)

Director General – DIGIT Directorate-General for Informatics

Summary

In the EC we have a huge network than spans a large community of internal and external users. In order to enable trust on this network, we invest on security. Information is classified, and systems are segregated and protected according to the information they hold, and in proportion to the risk they are exposed to.

Key points from the presentation

- The speaker presents the commitment of the EC on security and trust:
 - Internal e-Governing Initiative
 - Barroso II: transformational agenda for Europe
 - the Digital Agenda is in the core of the near future plans
- Then, he presents the requirements of networking for internal and external users, and the approach followed to meet them. In summary, no trust is feasible without security.
- He presents the kinds of information managed, and the problems to manage classified information that is a small quantity, but is scattered over the systems.
- After describing the organisation for security, and the technical solutions in place, the speaker concludes that security must be based on risk, to focus on highest risks and react proportionally.

4.4.2 Michel Riguidel (ENST)

Summary

Internet has grown out of control of the users. Currently we are unable to model it thoroughly, because it is more than a bunch of technologies. Technology is only an enabler for new paradigms of behaviour that cannot be grasped digging into the details. For instance, trust is something more than security; we need to trust on Internet as a living subject, far beyond the security of its digital elements. The challenge is not perfection on security, but excellence in trust. We must start thinking on an Internet without a



clear border between living beings and technological artefacts. The Internet of things is blurring the border and it is foreseeable that our biological parts become parts of Internet with inter-domain threats and risks. It is mandatory to learn how we can measure actual trust, and live with it according to our understandings and expectations.

Key points from the presentation:

The speaker performs a heterodox presentation about network complexity and evolution. To secure something you need to know what it is. But Internet is polymorphic, and needs several models for communication, storage, and computation. Engineers are patching the old Internet rather than researching on the new Internet. But currently we, the users, lack the tools to effectively manage Internet.

For the future of Internet, we have to abstract more effectively. The net is no longer a graph of interconnected nodes. IP addressing is confusing all of us.

Thinking differently. The Internet needs to be porous, viscous, ...

Chopin was investigating excellence to play classic piano. Fingers are like atomic IP packets. The future is more like Debussy that makes piano a flowing working play. We need a continuous flow.

Like programming languages, old Internet was like FORTRAN, with fixed structures. Today it is like LISP with flexible lists (see google, googling everything). The future will be like objects where everything is programmable, and moves on its own, not necessarily based on IP routing.

Current and future threats and vulnerabilities:

- it will not be limited to computers talking to computers, but could involve anything. For instance, it might be possible for viruses to kill people on the Internet.
- we have currently illicit content, in the future we will have illicit computation
- ddos (distributed denial of service) may turn into domino effect

In summary, Michel foresees an Internet that is living organism.

The big challenge for security is that we have to detach security from trust; we need measures for trust creation and sharing: recommendations, votes, confidence, ...

4.4.3 Volkmar Lotz (SAP)

Summary

Absolute security is not an option. Security has to balance convenience and economics, while it is definitely driven by economics. To build an Internet that is usable. We need to create elements of service that may be used to



construct services that deserve trust, guiding users in real time through understandable and reliable options tailored for each transaction so that users' expectations are met without surprises.

Key points from the presentation:

- The speaker addresses security and trust in the Internet of Services from an architectural point of view.
- We need usable security. Security is not perfect. Security implies some inconvenience. Security is driven by economics.
- Security of Services puts together many actors with many technologies, interests ... Actual protection may be very different at different layers. The IofS (Internet of Services) will not be generally secure and trustable. We have to face new threats: malicious providers and consumers.
- Trustable environment should be built on demand. We need a menu of services, and guide users to come up with the best balance for their context-specific needs.

4.4.4 José M. Cabanillas (Atos Origin)

Summary

Security is like water: extremely powerful because it is able to adapt to circumstances with its always-moving characteristics. We need to build trustable services over troubled waters. For instance, atop e-identity that is also an always-moving object. Trust is not black or white, but a scale of greys, slow to grow, but subject to quick destruction by failures. Establishing bridges enables trustable collaboration between agents in Internet.

Key points from the presentation:

- The speaker devotes some time to present its company, and the projects they are involved related to security.
- The speaker makes a distinction between trust that is a binary property (I trust you) and trustworthiness that is an individual property (this thing is trustworthy).
- The speaker will use water as a metaphor for security. Fish is Atos. The water is the moving target of information security.
- About identity, he recovers old Greek philosophers to state that “you cannot step twice in the same river”, because it is continuously moving, and the second time it is different water. Identity is similar for humans we are always changing. Threats to information security are continuously changing, and require security that adapts dynamically.



- We are building bridges over troubled waters. We have shades of trust (greys). We need metrics, or at least indicators to measure where we are at every moment. We build bridges to catalyze the future trust.
- In the future Internet, collaboration is compulsory.

4.4.5 Simon Foley (University College Cork)

Summary

Security is not any longer a property of technology, but it must move into a response to requirements established by federations of consumers and providers, context-specific. Research is ongoing on the behaviour of centralized and distributed coalitions.

Key points from the presentation:

- Simon addresses “requirements based security”.
- We need to move from technology-focussed security into user-focus and into federation of consumers and providers.
- The speaker goes over understanding context-specific needs, and concludes mentioning research on understanding coalitions (centralized and distributed) to make them secure.

4.4.6 Partial conclusions

- security is required as a basis for trust
- we need to open our mind to the future of internet, and understand actual use, rather than looking at the technological infrastructure: build use cases
- we need instruments to measure trust
- we need to transfer control to users

4.5 An European Framework for e-Identity Management

Chair: Kal Rannenber (Goethe Universität Frankfurt)

Identity management is like a business deal because we have a number of parties involved in transactions that need to trust in identity: the identified parties, the relying parties, and the service providers. So we need trust relations.

4.5.1 Reinhard Posch (CIO Austria)

Summary

Identity is an old service provided by governments. Moving the concept into the electronic world raises a number of complex issues, technological and legal. There appear new actors between identity issuers and identity consumers. It looks unfeasible to reach a uniform global e-identity, with uniform liability and uniform respect for privacy. Currently we need



research projects, like STORK to learn on realistic scenarios, which are the issues, and the adequacy of proposed solutions.

Key points from the presentation:

- Needs and conditions for a European eID.
- The big picture includes subjects, technology, and the demand for interoperability (e.g. standards). The problem is to make it usable between countries, and domains.
- We need to address people, things, and services.
- Pairing, enrolment: to map e-Id, and ID for recognition.
- The data in the e-ID must be aligned with privacy requirements. Minimum collection of data, minimum disclosure, and re-use of identifiers to control traceability.
- Do we transfer management to the grey cloud of the applications?
- Do we need intermediate agents? What is the legal situation of this middleware. Who is accountable for failures? Who pays?
- We need an inventory of technology, and legal frameworks. We cannot regulate the technology cutting edge; but we need a regulatory framework.
- In project STORK we have a number of pilot scenarios to learn the issues of actual use. Currently the experiments are between two countries. In the future we shall address Europe-wide identity management.
- How to make use of electronic signature on electronic documents?

4.5.2 Jorge López Hernández (Indra)

Summary

Project STORK (Secure Identity Across Borders Linked) is a research project to experiment with scenarios of inter-domain usage of e-identity. We are currently analysing the issues raised by different technologies in different countries with different legal frameworks and involving both public and private sectors.

Key points from the presentation:

- More detail on project STORK.
- The aim is to test recognition of existing eIDs in other countries.
- Problems addressed:
 - different countries
 - different technologies (already deployed in different countries)
 - different legal frameworks



- public and private actors
- Duties and rights are part of digital life.
- The user can not be isolated from risk: providing control is a step forward

4.5.3 Jan Camendisch (IBM Research)

Summary

E-identity must take privacy into consideration. We have technology, cryptography, able to respect privacy by means of providing as much information is needed for a transaction, and no more, so the privacy is always under control of the subject of the e-identity. So emphasis moves from core private information onto credentials that may combine different sources of information into what is needed for a single transaction.

Key points from the presentation:

- Any eID framework needs privacy built-in. Otherwise it is not trustworthy.
- Users leave digital traces everywhere, forever.
- We need multiple e-identities to keep our spheres private and apart.
- There is technology available, but we have to put it to work.
- The key idea is that the identity is kept secret, and generates as many ephemeral identities as needed, and keep them unrelated. You get ad-hoc credentials. The credentials say as little as needed, and still are cryptographically protected.
- Even there are ways to mix several credentials into a new aggregated credential.

4.5.4 Kim Cameron (Microsoft Research & Development France)

Summary

Internet was not designed to guarantee authenticity, neither to protect privacy. These are afterthoughts we are trying to repair by means of kludges. The current standard is to translate long-term identity numbers into Internet opening many concerns as described in the RISEPTIS report. We should rather embrace the concept of 'minimal disclosure', where private information is under the sole control of the subject, and it is only disclosed to the extent that is needed by a single transaction, and accepted by the subject.

Key points from the presentation:

- Identity is needed for personalization.
- Internet was not designed to know who you are talking to. Today we have a lot of patches (i.e. kludges) to try to survive. We need a layer for identity on Internet. Something for the whole Internet.



- Instead of eternal identity numbers, let's provide the minimal information that is needed for a transaction. That is minimal disclosure.
- There are solutions working in enterprises, at the application level, using limited credential servers.
- There are problems for individuals. There are solutions such as OpenID, but it has security problems: difficult to use and understand, and susceptible to phishing. It is "naïve federation" where the provider knows everything.
- Minimal disclosure. Alice receives a set of assertions, but she controls the part that is disclosed to the relying party.
- I do not want to infantilize the user, but we cannot educate everyone into the details. We need to understand the users and speak the language they speak.

4.5.5 Partial Conclusions

- technology is not the biggest problem: there are cryptographic algorithms, and working solutions (e.g. e-cards)
- the biggest problem is interoperability with respect to accountability and liability
- minimal disclosure reduces the amount of information to what is strictly needed for the transaction; but it may be difficult to put into legacy systems
- policy is needed to protect users from exaggerated claims
- universal identifier are a fact in legal frameworks, and a risk for profiling and tracing

5 Summary of the sessions on February 11th

5.1 [Technology Development and the EU Legal Framework of Data Protection and Privacy](#)

Chair: Ugo Helmbrecht (ENISA)

5.1.1 Peter Hustinx (EDPS)

European Data Protection Supervisor.

Summary

Trust is essential for a useful information society, and trust depends on authenticity, accountability and liability, requirements that may collide with privacy and regulation on personal data protection. We cannot regulate technology, but we must regulate the requirements that must be met by working solutions, and allocate incentives for technology to devise solutions. Privacy awareness must be provable with enough evidence that



permits supervisors to assess that the service meets the requirements stated by regulation. Respect of privacy must be present from the initial conception, rather than added later to a poor design.

Key points from the presentation:

- Trust is essential for the information society. The society increasingly depends on ICT (information and communication technologies), which are becoming pervasive, and causing an increasing concern with privacy and data protection. We must align internet with the values of our society.
- Roles of my position:
 - European institutions comply with data protection rules
 - advise parliament on new policies and legislation
 - work with national authorities for a consistent approach
- Privacy and data protection is becoming a horizontal, holistic approach.
- Implement principles in a more intelligent and effective way.
- Innovation on principles:
 - privacy by design
 - accountability
- The question is allocation of incentives to get it done.
- Diversity in legislation is here to stay. We cannot legislate on technology. But privacy must be embedded into the design from the initial conception. We can expect incentives for industry to design with privacy in mind.
- Privacy by default settings.
- A need for evidence to demonstrate controllers that technology is under control, and that all the measures have been taken to ensure the desired outcome.
- Proactive and reactive mechanisms.

5.1.2 Alma Whitten (Google)

Lead engineer for privacy.

Summary

Google's approach to privacy is by means of transparency. That means that users of Google get access to the information collected about them, and are enabled to edit it. Obscurity does not help: it must be clear to the user that they have full control through meaningful options.

Key points from the presentation:



- The approach of Google to protect privacy is to pass control to users, so users know what Google knows about them, and may tune it to their will.
- The emphasis is on transparency and choice of meaningful options to users.
- The incentive for Google is to get aligned with user concerns. We ask users which are their wishes about control of their information, and try to align to expectations.

5.1.3 Mireille Hildebrandt (Vrije Universiteit Brussels)

Senior researcher.

Summary

The problem of privacy in the net is more than controlling what data is released to another party; we need to control what information the net can infer about us. Legal protection of privacy should require smart transparency so that service providers are required to provide smart tools to access the retained data and understand the knowledge inferred from it.

Key points from the presentation:

- The speaker wants more than user control of options. She wants full understanding of the semantic consequences of the retained information and its processing. It is not only the amount of data, but also the computation you may derive on it.
- Trustworthiness cannot be market driven.
- User-centric European platform does not suffice because there are Knowledge Discovery Databases.
- We need that data minimization is smart, and we need transparency of knowledge that applies to me, not only the data others have about me.
- Legal protection must be built into the ICT infrastructure, and that's legislator domain, not to be left to the market.
- Patching a poorly designed infrastructure lacks incentives for companies and users to use the patches with extra cost.
- The problem with Google is not [only] my personal data, but the digital leak of information I leave behind. E.g. keyboard typing may be analysed to derive sickness. In Internet of things, a lot of knowledge can be inferred by correlation.
- The autonomy trap: if the software discovers my wishes, I may be subject to commercial ads that change my wills, and still it is too obscure to understand that I am becoming a puppet of the net.
- Social sorting of citizens. I may be categorized without understanding why.



- Smart data minimization is about controlling what knowledge you want to hide/expose in a certain context. I need enhanced transparency tools to understand the whole picture.
- My interest is not on MY data, but on the data that may impact my life.

5.1.4 Michelle Chibba (Director Policy, IPC Toronto, CDN)

Director policy.

Summary

In Toronto we have some successful experience in addressing privacy from the design by making it clear to the providers that there is an incentive for being compliant with clear requirements that services and products must fulfil. The rule is to look for positive sum relations. Further research is needed to attach behaviour to information into smart data agents that are able to think by themselves.

Key points from the presentation:

- The speaker presents the work done in Ontario (CA) in preventive approach to privacy: to build privacy into the design.
- Our approach is to look for positive sum relations, and extend it over the whole life-cycle.
- Legislation alone is not sustainable. We must be proactive, and understand the market.
- Research: SmartData make the data think for itself. No raw data in the open, but data is housed within a SmartData Agent. Sounds similar to object oriented paradigm.

5.1.5 Partial conclusions

- a legal framework is needed to harmonise and support technology and user requirements
- transparency and user control are essential
- problems with aggregation of information: inferences are more than personal raw data
- privacy by design is proposed, with incentives that drives the market in the intended direction

5.2 International Cooperation on Trust and Security Research

Chair: Neeraj Suri (Technische Universität Darmstadt)

Trust is an end-to-end attribute

Project INCO-TRUST (International Co-operation in Trustworthiness Systems) looks at security privacy and trust in large-scale global networks and services.



Do we have the technologies, and the mechanisms to have an effective cooperation?

What are the national agendas on security and trust?

5.2.1 Malcolm Crompton (IIS Partners, AU)

Summary

When providing services it is necessary to take governance into account, and to identify where the economical incentive to enable trust in the service is. The key for trustworthy services is that the risks are adequately identified and allocated. Then, risks can be controlled. That is a universal rule, and in order to apply it to global services, we need standards for security and trust, including metrics on service trustworthiness. In that aspect, we should cooperate and produce agreed APIs.

Key points from the presentation:

- Security is not about perfection. It is about economics.
- Accountability, liability: it is not what I say, it is what I do
- I can show trustworthiness evidences, but it is you to decide whether I deserve trust.
- Risk management
- We need metrics
- Personal experience with privacy impact statements: usually we do not talk about privacy, but rather ask whether “is my life under my control?” Then I want to have under control the world around me. Then we run a risk analysis, and decide whether the system is under the desired control. If not, the privacy is under risk.
- There are two missing links: risk allocation and governance
 - trust drives the decision to run some risk, so risk analysis and risk allocation is a fundamental step to take go / not go decisions
 - nevertheless, risk allocation comes before risk management: who pays the bill?
 - we need governance: measures and the capacity to act on measured
 - safety net: what happens when things go wrong; if we can manage failure, we can take more risk
- We need to abstract requirements into an API for privacy and security so we can interoperate.



5.2.2 Priscila Solis Barreto (University of Brasilia)

Summary

Brazil is currently involved in a major technological effort to bring broadband communications to every citizen. This effort must be topped with effective services that everybody can trust. In that respect, we are open to, and willing to cooperate with EC on secure communication infrastructures, and environments to develop trustworthy services that are useful regardless the technical expertise of the users.

Key points from the presentation:

The speaker presents the figures of present and near future of networking in Brazil. The final objective is to provide services for collective access and reduction of regional and social disparities. These services must be usable, secure and trustable. The network shall encompass both public and private institutions.

There are some subjects for research and cooperation with European Union.

- defining guidelines for ICT market
- trustworthy ICT

In September 2009, we ran a workshop in Sao Paulo to promote collaboration with European Community. One of the topics of common interest is “Security, Privacy and Trust” covering

- trusted communication infrastructures
- application service environments providing secure and consistent access
- usability regardless technical expertise

5.2.3 Barend Taute (CSIR Meraka Institute)

Summary

In South Africa there is an ongoing effort to expand digital services to every citizen. The main concern is that security is usable, and does not depend on the ability and quick reaction of the user. We would like to cooperate with the EC on several frameworks: trust, privacy, identity management, net governance, and forensics. On this subject we need common elements for interoperability.

Key points from the presentation:

We perceive a need for ‘usable security’, as well as ‘awareness and access to good advice’. Legislation is slower than technology and mischievous use. We do not want to wait for a crisis, because incidents happen just too fast for human reaction.

Some facts about South Africa

- < 10% penetration



- privacy is not a big political issue
- we lack tools to implement, monitor, investigate, ...
- lack of trust does not stop online transactions

Research agenda for trustworthy ICT

- pervasive security
- trust, privacy, and identity management frameworks
- engineering principles & architectures for trust, privacy, transparency and accountability
- data and policy governance

E-Identity:

- by design: privacy, minimal disclosure, proportionality and legal
- instruments for forensics

We are willing to cooperate and benefit from already done work.

5.2.4 Daniel Brett (S21sec)

Summary

In S21sec we are investing heavily on security because we think it is a key subject involving private and public sectors. Improve collaboration is needed as well as an international legal framework.

Key points from the presentation:

- The speaker presents the activities of S21sec in several sectors related to security.
- S21sec invests heavily in research because threats are global and require international cooperation.
- Trust and security are global and challenging problems that impact citizens, companies, and governments.
- We would like more of
 - public-private collaborations with a global scope
 - international legal agreements
 - care to maintain the complex ecosystem

5.2.5 Ty Znati (Director NSF, US-TBC)

Summary

In the US the NSF is about to start an ambitious program towards a science of security. That implies theoretical models and engineering solutions. The



plan is open to international collaboration, mainly in experimentation with real scenarios.

Key points from the presentation:

- Towards a science of security. We have a successful network, but we do not understand it, and we are unable to predict the behaviour of the system. We need a science, a model to reason on it, and tame complexity.
- NSF (National Science Foundation) has a mission to support research on information systems that
 - functions as intended, specially under incidents
 - complies to policies
 - addresses individual and societal concerns on privacy and usability
 - educates workforce and inform the public
- Trustworthiness = reliability + security + privacy + usability. All these subjects need research, and experimental evaluation of designs.
- CNCI – Comprehensive National Cyber Security Initiative. Towards securing critical infrastructures.
- There are a number of options to collaborate, and the will to do so.
- To sum up:
 - we need sound theoretical foundation
 - we need true experimentation
 - we need international collaboration

5.2.6 Partial conclusions

- International cooperation is a must and already a fact. International workshop in May co-sponsored European Commission and NSF.
- There is an amazing similarity of the issues in every country.
- The size of the population in the countries of the speakers is a large piece of world population. We may observe common goals and opportunities for cooperation and alignment for secure and trustable interoperability.
- There is still a lot of work to be done.



6 Annex A – Agenda

6.1 February 10th

09h00 - 09h30	Welcome
09h30 - 10h30	<p>Opening Session</p> <ul style="list-style-type: none"> • Francisco Ros Perán State Secretary of Telecommunications and for the Information Society Spanish Government • Mario Campolargo. Director of Emerging Technologies and Infrastructures European Commission • Víctor Manuel Izquierdo General Manager Inteco • Francisco Fernández Mayor of León
10h30 - 11h15	<p>RISEPTIS report “Trust in the Information Society”</p> <ul style="list-style-type: none"> • George Metakides Chairman RISEPTIS, Uni. Patras
11h15 - 11h45	Coffee Break
11h45 - 13h15	<p>Trust Digital Life - an Industry View</p> <ul style="list-style-type: none"> • Willem Jonker Philips • Krishna Ksheerabdhi Gemalto • Luis Fernando Álvarez-Gascón GMV • Laila Gide THALES • Jerry Fishenden Centre for Technology Policy Research (CTPR)
13h15 - 14h15	Lunch
14h15 - 16h00	<p>Trustworthy Networked Service & Computing environments</p> <ul style="list-style-type: none"> • Willie Donnelly WIT, THINK-Trust

	<ul style="list-style-type: none"> • Michel Riguidel ENST • Volkmar Lotz SAP • José María Cabanillas Atos Origin • Simon Foley University College Cork • Francisco García Morán Director General Informatics European Commission
16h00 - 16h30	Coffee Break
16h30 - 18h15	<p>An European Framework for e-Identity management</p> <ul style="list-style-type: none"> • Kai Rannenber Goethe Universität Frankfurt • Reinhard Posch CIO Austria • Kim Cameron Microsoft • Jan Camenisch IBM • John Heppe Indra
20h30	Official Dinner

6.2 February 11th

09h00 - 10h30	<p>Technology development and the EU Legal framework of Data Protection and Privacy</p> <ul style="list-style-type: none"> • Udo Helmbrecht ENISA • Peter Hustinx EDPS • Mireille Hildebrandt Vrije Universiteit Brussel • Michelle Chibba Director Policy, IPC Toronto, CDN
---------------	--



	<ul style="list-style-type: none"> Alma Whitten Google
10h30 - 11h00	Coffee Break
11h00 - 12h30	<p>International Cooperation on Trust and Security Research</p> <ul style="list-style-type: none"> Neeraj Suri Technische Universität Darmstadt Tai Znati Director NSF, US Malcolm Crompton IISPartners, AU Priscila Solis Barreto University of Brasilia Barend Taute CSIR Meraka Institute Daniel Brett S21sec
12h30 - 13h00	Conclusions
13h00	Closure



7 Annex B – Background: The recommendations of the RISEPTIS report on Trust in the Information Society

The complete report is available at

<http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>

The RISEPTIS report comes to the following recommendations:

7.1 Recommendation 1:

The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the Information Society. The priority areas are:

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

7.2 Recommendation 2:

The EC should support concrete initiatives that bring together technology, policy, legal and social-economic actors for the development of a trustworthy Information Society. (The Partnership for Trust in Digital Life¹ could be a first step.)

7.3 Recommendation 3:

The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity.

7.4 Recommendation 4:

The EC should work towards the further development of the EU data protection and privacy legal frameworks as part of an overall consistent ecosystem of law and



technology that includes all other relevant frameworks, instruments and policies. It should do so in conjunction with research and technology developments.

7.5 Recommendation 5:

The EC together with industrial and public stakeholders should develop large-scale actions towards building a trustworthy Information Society which make use of Europe's strengths in communication, research, legal structures and societal values – for example, a Cloud which complies with European law.

7.6 Recommendation 6:

The EC should recognise that, in order to be effective, it should address the global dimension and foster engagement in international discussions, as a matter of urgency, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.



8 Annex C - Conclusions of Leon

The complete document is available at

<http://trustworthyict.inteco.es/index.php/en/conclusions>

The participants to the Conference Trust in the Information Society, together in León on 10 and 11 Feb 2010, representing public administrations, industry, research organisations, universities and societal stakeholder groups, from Europe and abroad come to the following conclusions:

CONCLUSIONS OF LEON

The participants to the Conference Trust in the Information Society, together in León (Spain) on 10 and 11 February. 2010:

- **Confirm** the essential importance of the development of Trust in the Information Society for economic growth, prosperity and the promotion of our societal values.
- **Endorse** the analysis and recommendations presented in the RISEPTIS Report, in particular to:
 - Strengthen interdisciplinary RTD for Trust in the Information Society.
 - Stimulate ICT products and services based on "Trust by Design".
 - Develop an EU Framework for electronic identification in full respect of privacy and for broad societal use, including e-Government, e-Health and the Private sector.
 - Develop an ecosystem of technology and law preserving our societal values and creating trust in the society, all within a global context.
- **Emphasise** the urgency to develop a platform for effective cooperation on trust issues between stakeholders in RTD, industry, society, law and regulation and education and awareness.

And recommend to the European Commission and Member States

- To give urgent attention to these Conclusions of Leon in their upcoming decisions on the European Digital Agenda and Granada Strategy as well as in other relevant discussions, like those to be held at the WCIT 2010 in Amsterdam.
- To call upon ENISA, in close cooperation with stakeholders, to actively support programmes of the European Commission and Member States, related to security and trust in ICT, in particular in bridging the gap between technology and policy, and ensuring efficient uptake of research



results in operational environments."

- To strengthen international cooperation to promote and develop Trust in the Information Society at a global scale.