UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- inforewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Cover page designed by Concha Arias-Pérez
"DNA in love" / © CEPIS 2010
Layout Design: François Louis Nicolet
Composition: Jorge Llácer-Gil de Ramales

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (August 2010)

"2010: Emerging Information Technologies (II)"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 3, June 2010

Monograph: 2010 - Emerging Information Technologies (I)

(published jointly with Novática*)

Guest Editors: *Alonso Álvarez-García, Heinz Brüggemann, Víctor-Amadeo Bañuls-Silvera, and Gregorio Martín-Quetglas*

UPENET (UPGRADE European NETwork)

CEPIS NEWS

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Trust in the Information Society: RISEPTIS Report

RISEPTIS, Advisory Board of the Think-Trust Project

The report issued in October 2009 by RISEPTIS (Research and Innovation in Security, Privacy and Trustworthiness in the Information Society), the Advisory Board of the European Union Think-Trust Project, is offered on these pages in abridged form. The report addresses highly important issues (privacy, security, trust, …), founded on the key principle that a European Information Society should comply with the longstanding social principles that have served Europe so well to date, because democratic values and institutions, freedom and the respect of privacy are essential for trust in our society. So too is law enforcement, accountability and transparency. The social trust thus created is essential.

The full version of the report is available at <http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html>.

Keywords: Information Society, Internet, Report, RISEPTIS, Think-Trust, Trust, Web.

Author

RISEPTIS, Advisory Board for Research and Innovation in Security, Privacy and Trustworthiness in the Information Society of the European project Think-Trust, has produced this report. In April 2008, RISEPTIS was established with the objective to provide visionary guidance on policy and research challenges in the field of security and trust in the Information Society. RISEPTIS has been supported by the EC-financed 'Coordination Action' project, THINKTRUST, whose objective it is to develop a research agenda for Trustworthy ICT. RISEPTIS was supported by more than 30 experts in two Working Groups: (1) Security, Dependability and Trust in the Future Internet; (2) Privacy and Trust in the Information Society. Think-Trust (FP7-216890) is a project funded by the European Commission's 7th Framework Information Society Technologies (IST) Programme, within the Unit F5 ICT for Trust and Security. <http://www.think-trust.eu/>

Executive Summary

Trust is at the core of social order and economic prosperity. It is the basis for economic transactions and inter-human communication. The Internet and the World Wide Web are transforming society in a fundamental way. Understanding how the mechanisms of trust can be maintained through this transformation, is of crucial importance.

It is clear that some issues are not simply technological, nor are they purely social. Their complex interactions mean that the promotion of trust in the Information Society requires a coordinated interdisciplinary approach, which is very much in line with the emerging Web Science.

It is the strong conviction of RISEPTIS that technological developments in trustworthy systems will be most effective if they are implemented through a strong interplay with social and business perspectives, as well as robust policy and regulation. Likewise, the latter will also strongly benefit from technological insight and support. Governments are best placed to take responsibility for leading this process of interplay.

This report makes some preliminary recommendations that may open perspectives and start activities in the right direction. The recommendations not only address research, innovation and infrastructural development, but also the legal framework, societal acceptance and the need for international cooperation, to demonstrate the interdependencies in the quest for a free, democratic, safe and citizenfriendly Information Society.

....

1 Introduction

The integration of Information and Communication Technologies (ICT) into our lives is transformational.

It acts as a catalyst for new forms of creativity, collaboration and innovation. Furthermore, it raises fundamental questions regarding ownership, trust, privacy, identity and the economy. Simultaneously, our increasing dependence on digital infrastructures and services has obscured the handling of our personal data and increased our exposure to new threats and mal-practices at an alarming scale.

....

2 Trustworthiness at Stake

In this chapter, we will discuss the concepts of trust, trustworthiness, identity and privacy.

These are developed against the background of the EU legal framework on data protection

and privacy, and the foreseen evolution in technology.

2.1 Concepts

We see **trust** as a three-part relation (*A trusts B to do X*). Parties *A* and *B* can, in this respect, be humans, organi-

sations, machines, systems, services or virtual entities. The evaluation of the trust *A* has in *B* to do *X* plays an important role in the decision of *A* to partake in any transaction, exchange or communication between them. By reducing risk, trust effectively facilitates economic activity, creativity and innovation. Trust is highly context dependent. Trust is easier to establish when the identity and/or other authentication information (claims) about the third party are known.

Trustworthiness relates to the level of trust that can be assigned to one party *(B)* by another party *(A)* to do something *(X)* in a given relational context. It is an *attribute* or *property* assigned by *A* to *B* which influences the trust relationship, as perceived by *A*. In this sense, it is not an absolute value and is context dependent. Digital systems should give minimum and, as much as possible, measurable guarantees and information on related risks concerning quality of service, security and resilience, transparency of actions and the protection of users' data and users' privacy, in accordance with predefined, acknowledged policies. We call systems satisfying such characteristics: *Trustworthy Systems*.

For further discussion on these two related concepts, see Russell Hardin[1], Kieran O'Hara[2] and Trustguide[3].

Identity and **Identification** are concepts which are difficult to grasp in a formal way. Digital identity, in a general sense, will include all kinds of attributes: those needed for our identification, our personal data provided through Web community systems, the information on all sorts of web pages that register our professional lives; in general, our full digital shadow.

Anonymity refers to the absence of identifying information associated with a natural person. **Pseudonymity** is the situation where certain claims are provided, but these cannot be connected to directly obtain identification; however, the natural person is still identifiable, if necessary.

....

3 Technology in Societal Context

To place the general discussion and concepts presented in the context of everyday life we discuss in this chapter the attractiveness of certain future service scenarios and the dangers of data collection when it is either not controlled at all or, at best, is insufficiently controlled by the data subject.

Before showing the scenarios, we first discuss briefly two of the problems facing us today as we move increasingly towards a Digital Society:

3.1 The dangers of our digital shadow

Many people freely enter various personal details onto Internet websites. Similarly, users will publicly declare all manner of sensitive and revealing information on dedicated social-networking sites. Neither the person who inadvertently reveals their identity and lifestyle choices, nor the *facebook*™ friend, who apparently does not care that he is disclosing identifiable data to more people than he thinks, seems to be worried about the life-long digital shadow they are creating.

3.2 The weakest links in the data storage chain

By its very nature, the process of transferring and processing data is a problem. This procedure presents the attacker with the data in its most vulnerable form. Therefore, despite the sophisticated means and considerable resources deployed to protect sensitive information when it is digitally *stored*, the fact remains that *transferring* this data means that the chain of data trust is not being evenly serviced.

Human perception is one of the factors to be considered too, when the issue arises of compelling companies and governments to report data breaches. It is argued that public trust in the breached organisation will drop as reports of their security violations increase. Whether such decreases of confidence are justified or not remains to be seen. Either way, public perception and users' trust is a significant issue in the digital world.

3.3 Living in the future Information Society

3.3.1 Prologue: Setting the scene

Jorge is a 23-year-old student. He is living in London with Theresa, his 21-year-old girlfriend. Theresa has a degree in financial studies and is currently working part-time, doing various "odd jobs", while she looks for a full-time position. Theresa's grandmother, Helena, lives in London also; in a quiet, residential area.

Like most of their friends, Jorge and Theresa appreciate the smaller carbon footprint generated by using on-line services as much as possible.

3.3.2. Jorge's smart dentist visit

It's Friday morning and after reminding Jorge that he is supposed to sort out his soon-tobe-expired ID card today, Theresa leaves their apartment on the way to a nearby lawyer's 21 office, where she does some financial bookkeeping for the small firm of lawyers every week.

When he's finished reviewing some course work, Jorge goes on-line and logs onto the Government's *ID-Card* website. Though it isn't something he had previously considered (or even thought possible), he selects an *e-ID Card* that has the capability to store his health insurance profile and a token to access his health record if he so chooses; which he does, when he realises that having his medical details readily on-hand may be useful and time-saving in the long run. After confirming his e-ID choice –

[1] Hardin, R. *Trust & Trustworthiness*, Russell Sage Foundation, New York 2002.
[2] O'Hara, K. Trust: From Socrates to Spin, Icon Books, Cambridge 2004
[3] Lacohee, H. Crane, S. and Phippen, A. Trustguide: Final report – www.trustguide.org.uk.

a range of options was available to him – Jorge sets up an appointment with the National Health Care Administration and later goes to their nearest office in his area. At the Services Counter he provides his old ID card and the reference number of his on-line reservation. In a matter of minutes, he gets his new *e-ID Card* issued. No weeks and weeks of waiting, no long queues, and no paperwork to fill out.

Since he now has his new smart *e-ID Card*, Jorge thinks it may be time for a long overdue visit to the dentist. Thanks to one of the useful applications loaded onto the microprocessor of his Card, Jorge simply inserts the device into the card reader on his PC and, via a web browser, selects Dr. Malcolm Bond, a nearby dentist, for his second appointment of the day.

When the appointment is confirmed, Jorge clicks Dental Records Only from a list of options which allows him to decide how much of his medical information is shared with the dentist's web-service provider. This will save Dr. Bond the inconvenience of redoing a complete new set of x-rays; meaning less time in the dentist's chair for Jorge. Maybe a smaller bill too! Jorge is slightly concerned though, about transferring his dental records across the Internet. He also wonders whether a copy of his dental records will now be permanently stored on the dentist's web portal. He intends to ask Dr. Bond about this, but is not optimistic about a dentist's knowledge of data transfer or data storage! "An explanation from the dentist, the Card people or the Internet booking site would be useful," thinks Jorge, "but this system is just so convenient and I guess my information will be OK," he concludes.

3.3.3 Theresa's Memorable Shopping Trip

After finishing her work on the lawyer's accounts, Theresa decides to treat herself to some retail-therapy in the local Shopping Centre. Her grandmother, Helena, will be visiting them for Sunday lunch the following weekend and Theresa would like to buy herself a new outfit to impress her grandmother. The *RFID tag* on her jacket is picked up by a *Reader* outside a large department store. The *Reader* sends the tag's serial number to a *Localisation Service*, which forwards this data to a centralised system that handles consumer-related data for that particular area.

Theresa is oblivious to all this work going on behind the scenes, which involves her clothing, her location and her mobile phone number. So, when the system recognises Theresa and looks up her pre-submitted preferences, the first she knows of this extensive wireless infrastructure is when she receives a text message on her mobile phone, offering her a 20% SALE reduction inside the store.

After making her selection, Theresa hands over her and Jorge's joint credit card to pay for her chosen item. The cashier asks her for either her passport or Government-issued *ID Card* in order to verify her identification. However, Theresa doesn't have her *ID Card* with her and she prefers to keep her passport locked in the safe of her apartment. Her old student ID card is unacceptable for this transaction and therefore, the cashier logs a 'Potential Fraud' event on the shop's payment system. With no means to identify herself and, therefore, no way to authenticate her ownership of the credit card she has just presented to the cashier, Theresa finds that she is starting to feel very embarrassed in front of the other shoppers in the store. She doesn't realise that this little identification/authentication mishap is about to get much more upsetting…

For security purposes, an alert is sent to a credit card clearance agency, who check the credit card number against other potentially fraudulent activities. Unfortunately for Theresa, the over-zealous system asserts that there has been another possible fraudulent action using this credit card recently, and the agency informs the police. The *Police Management System* accesses the *Localisation Service* to get the location of the consumer and sends two policemen from the closest office to speak to the hapless Theresa. Being a co-signee of the credit card, Jorge is also on his way to the store, having received an SMS message informing him of the possible criminal activity; generated by the seemingly comprehensive, but ultimately disjointed, credit card transaction infrastructure.

3.3.4 A Very Modern Holiday

Luckily, but unknown to Theresa, her and Jorge's credit card was not used in any criminal manner recently. Rather, when the card was used while she and Jorge were on a short break in Italy a few weeks previously, the clearance agency automatically added its details to a "potentially fraudulent" list. This was because the restaurant where Jorge and Theresa dined while on holiday had since reported several acts of credit card fraud.

This was the only downside to the couple's trip to Italy, as everything else had gone perfectly during their holiday. Jorge had decided on the spur of the moment to whisk Theresa away for a quick break and booked their flights at the last minute, through an on-line holiday website. However, he didn't have time to book any accommodation in advance – they just packed their bags and went to the airport to catch their flight. While waiting in the airport departure lounge, Jorge filled out a 'hotel preferences' survey, which was sent to his Internet-enabled mobile phone from the International Hotel Group billboard nearby. Jorge did wonder for a second how this message arrived on his mobile phone but didn't really consider it an invasion of his privacy. "They have some sort of laws in place so that big companies can't take advantage of you like that," someone in the university café once told him. "Still though, it would be nice to be able to check," he thinks. After checking with Theresa, he nonetheless proceeds to also fill in 'food preferences' in the survey.

Upon landing at the main airport terminal in Rome, Jorge's mobile phone beeps with an incoming SMS message and he's happy to see he's been sent a list of hotels and restaurants that match his preference lists.

Through the same Internet interface on the mobile phone, the young couple choose what seems like a romantic hotel and are subsequently sent another SMS message informing them that a courtesy car is on its way to pick them up from the airport. After arriving at 'Casa Della Rosa', Jorge and Theresa receive a tailored menu, which only includes dishes that fit with the preferences filled out by them while they waited to board their flight back in London.

As he would again contemplate a few weeks later when allowing his dental records to be sent to the dentist, Jorge wonders about his preferences details being insecurely stored and possibly stolen, but he naively assumes that his data – now apparently stored someplace in Italy – will not get into the hands of any market researchers back in London.

3.3.5 Looking After You

Theresa's grandmother, Helena, is feeling a little lonely. Since she has had all the 'health/well-being' monitors installed in her apartment, her family know that they will be alerted if anything happens to her – hence, they don't call to check on her as much as they used to. Helena misses them, but the exchange of videos and photos and multimedia calls help to fill the gaps between visits.

In addition to the emergency motion detectors installed in every room of her apartment and the inbuilt heart-rate monitor in her bath, she also has a number of sensors in her kitchen, which can detect gas leaks, smoke and excess water on the floor. Helena has a panic button too that is linked to the local health care office. She finds the RFID scanners on her fridge and cupboards are very useful for managing her grocery shopping. Her subscription to a local supermarket's home delivery service means that she gets a weekly supply of all the provisions she needs, without having to brave the sometimes inclement weather.

Helena also enjoys her regular 'Well-Woman' check-ups, the times of which she manages via her on-line health service portal. As well as observing what food items she is consuming, these check-ups also take data from the heart-rate monitors and other sensors that are installed in her home. However, in spite of this state-of-the-art care she receives, Helena feels slightly uncomfortable with the fact that her health service provider is gathering up so much information about her. They have also recently informed her that they will now be constantly comparing the results of her check-ups with other women of her age from various health authorities across the country.

The health service provider says that this profiling work will help them decide on risk factors, so that, for example, heart attacks can be predicted more accurately. And that tailored dietary advice will now be offered to Helena too. The gathering of such personal information, together with the seemingly constant news in the papers and on television of CDs containing personal data being lost and stolen make Helena ill at ease. Her randdaughter, Theresa, has also told her that her health service provider is fighting off big cash offers from insurance companies to access their collected data files. In the current financial environment, Helena thinks that these offers must be increasingly tempting and she is now anxious to know the real long-term effects of her state-of-the-art home-health system.

Helena thinks about changing her health service provider. This would mean transferring/sharing all her data – including her financial details – with a new provider. What she doesn't know, however, is that this will only be possible if the old and new providers have compatible data storage and sharing systems. Neither does she know who actually controls "her" data now or how exactly it will be used. She phoned her current health service provider and was put through to the ironically named 'Helpline', but automated voices and opportunities to upgrade her service were all she heard on the other end of the phone line.

3.3.6 The Invisible Office

A few days after the drama with the credit card and the police in the Shopping Centre, Theresa receives an e-mail asking her to submit her CV for a temporary position with a recently-formed company, called *CEANNAIM*. Before deciding whether or not she will apply for the job, Theresa does some Internet research on this organisation.

She discovers that *CEANNAIM* is a Cloud company. It has a network of employees spread across Europe in various locations. The employees are essentially sub-contractors, and each receives a tailored, rolling contract, which they are obliged to digitally sign before returning to company HQ. The geographic location declared by the employee in their third-party-verified contract determines the legal and financial jurisdiction for any redress actions, on behalf of the company or the employee should the need arise.

Being averse to flying, Theresa is encouraged by the fact that the organisation does not have any specific physical office space and, therefore, company meetings are held by using on-line conferencing tools provided by the Cloud. *CEANNAIM's* employees use on-line storage for company documents, a service-based customer-relationship management system, and service-based financial-performance management software.

Theresa also discovers that employment at the company is highly dynamic, i.e. people join and leave on a very short-notice basis. When a particular skill is needed within the company, its Human Resources (HR) service scans various on-line community outlets in its search for suitable people. Once a number of possible candidates

have been selected from the dedicated employment sites, the HR service proceeds to trawl through various social-networking sites for information on their chosen candidates, in order to get a more rounded picture of its potential future employees.

Theresa is not aware of this invasive social-search and knows that she may join the company for only a short period of time. However, work is scarce and she needs the money. Therefore, she decides to apply for the job. As she enters the requested data via the company's HR service portal, she doesn't realise that her new employers have already built up a profile on her; and that she knows little about the work practices and expectations of her new pan-European co-workers.

3.3.7. Jorge's Free Ads

A few weeks after getting back from their short-break in Italy, Jorge begins to receive text messages on his mobile phone from *SEIRBHIS*, an advertising company, offering him discounts at various restaurants located in London. At first he simply ignores them, but after a few days of receiving this 'spam', he contacts his network provider to try to find out where these messages are coming from.

Once through to the provider's call centre, an operator informs him that although the messages are originating in the UK, they did not disclose his 'phone number to any such organisation. The operator asks Jorge if he subscribed to any new services recently and Jorge says no, but states that he did reply to a survey about hotels and food that he was sent while at the airport recently. "Aha," says the operator, who then proceeds to explain to Jorge that his hotel/food opinions would have been forwarded to a marketing firm in his country of destination (Italy, in this case) who use them to suggest personalised services to incoming visitors. While the marketing firm complied with the privacy statement supplied to Jorge and didn't distribute his preferences data to any other Italian hotel/food companies, they didn't make any reference to NOT sharing his data with their sister companies around Europe, including *SEIRBHIS*, in the UK. "This is probably how they got your number," concludes the call centre operator.

Jorge could pursue the matter further and make a complaint to "someone", but at this stage he doesn't even know in which country his and Theresa's hotel/food-related data is stored. Jorge immediately decides to switch from the network provider who facilitated this intrusion and vows to never again visit the hotel or restaurant he and Theresa used on their holiday since he considers them to be complicit in the deceitful chain of events.

3.3.8. Epilogue: The Digital Shadow Is Cast

In these scenarios and stories, the three characters engage considerably with the digital world around them. Therefore, if an attacker were to monitor the data being transferred and shared from the home PCs and mobile phones of the characters, he would retrieve a significant amount of raw data about them.

For example, if someone were to access Jorge's online activity, they could see that:

(1) He booked flights from London to Italy recently;

(2) He has ordered a new *ID Card*, which will contain his medical information;

(3) He had two appointments on certain days at particular addresses (the National Health Care Administration office and the dentist's office).

The attacker may also discover Jorge's dental records and associated background medical information. If the same attacker breached Jorge's mobile phone records, he would obtain information about Jorge and Theresa's favourite foods and the types of hotel they stay in, as well as the exact address of their chosen location in Italy.

What could also be easily discovered about the couple is that they have a close friend or family member whom they speak to regularly; since, if someone was monitoring Internet traffic, they would see that there are a number of video calls between the couple and a particular user. It would be reasonable to deduce that there is a close relationship between the two callers, especially if the calls took place outside of normal office hours. Grandmother Helena, would be further exposed if an attacker gained access to her automated communication with the local supermarket's home delivery service. Not to mention her vulnerability if her health service provider's database was penetrated. If an attacker intercepted both the suggested dietary advice she receives from the health service provider and the list of food automatically generated by her smart kitchen, then he could see whether she follows this advice or not. (Her health insurer may be interested in this alignment.)

The Cloud nature of *CEANNAIM*, the company which invited Theresa to submit her CV to them, means that there is much potential for data protection violations. Because *CEANNAIM* has employees in various European States, they may need to supply details on all their workers in each of those States, in order to establish proper channels of legal and financial redress. The details supplied by Theresa herself, as well as the summary of her drawn up by *CEANNAIM*, based on their contentious rummaging around on social networking sites, may then be stored in several different jurisdictions around Europe. Theresa's control over and ownership of her own data is, thus, compromised. And this is even before a security breach of the company is considered or the level of privacy and data protection of the on-line conferencing and on-line storage tools that they use are taken into account.

3.3.9 Super Sleuth Deductions

If any would-be attacker were to gain access to all the raw data made available, both deliberately and unintentionally, by the characters in the above stories, he may also

infer more contextual information about the characters, their movements and the relationships between them; thereby building up a rich and potentially lucrative profile of them. Amongst other details, he may surmise that:

- Jorge and Theresa are involved in a relationship;
- An elderly woman named Helena is the grandmother of one of them;
- The young couple and Helena are close and get on well;
- Helena doesn't always follow the dietary advice she is given;
- Jorge and Theresa like travelling/Italy;
- Theresa is unemployed, but is actively seeking work;

4 Towards a Trustworthy Information Society

In the previous chapters we discussed the various problems which lay ahead in the development of an Information Society, where widely available digitised communication, data processing and service provisioning is quickly becoming an integral part of our physical and social lives – i.e. of real life.

We see the risk that the pendulum swings too far in the direction of losing trust in the organisation and governance of our society, due to a lack of accountability and transparency, and rampant crime that cannot be controlled by law enforcement due to its global nature.

Our recommendations focus on positive development. The future trustworthy Information Society will be based on an ecosystem of digital communication, data processing and service provisioning, which should respect human and societal values and cultures. In our recommendations below we focus on some major issues that would facilitate or stimulate the development of such an ecosystem.

4.1 Research and Technology development

Our first recommendation focuses on the development of a research agenda for Trustworthy ICT. It should be noted that there is a clear continuity here with the existing FP7 ICT **Work-programme 2009-2010**. Important research activities are already implemented, but the extension of these and changes in emphasis should be considered. Four major areas of attention are proposed following the work performed by the Working Groups that supported RISEPTIS.

(1) Security in (heterogeneous) networked, service and computing environments, including the elaboration of security challenges for the design of architectures, protocols and environments that will constitute future large-scale and globally networked ICT systems. Specifically, these focus on the emerging future internet; cloud computing; the "Internet of Things" with its mixed mode environments, consisting of diverse computing; communication and storage elements; and, global e-service infrastructures.

The *trustworthy polymorphic future internet* is an important instance, requiring security of the core network and the critical nodes through protocols and architectures at a very large scale and a high data rate.

Trustworthy global computing will require contextual security with secure smart services in the Cloud for sharing information, as well as cooperative environments, which enjoy societal acceptance, in order to feel in control of the digital ambience. It will also require new infrastructures, using ICT as a tool to make real world artefacts more reliable in the various application sectors.

(2) Trust, Privacy and claims management (meta-systems) infrastructures: Public and

private *trust infrastructures* must be provided by trusted new stakeholders, which compute trust assurance using diverse trust models. It will require: trust architectures and new protocols to delegate trust and partial trust; trust instrumentation and high-level tools at the end-user stage; cognitive and learning instrumentation for trust; and, profiling services and communities.

(3) Underpinning engineering principles to: establish trust, privacy and security in the digital space and develop measures or rating models for it; implement transparency, accountability and privacy properties for the main computing entities and domains; develop metrics and tools for quantitative security assessment and predictive security in a complex environment; and, composition and evaluation of large scale systems.

(4) Data policy, governance and socioeconomic aspects, including policy and governance issues related to data processing in the ubiquitous, scale-less Web or Cloud. This will raise the desire to develop technology-invariant security concepts, but also issues of liability and compensation.

In order to deal with the global problems of the Future Internet, we need to address multi-polar governance and security policies between a large number of participating and competitive stakeholders.

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.

4.2 The interplay of technology, policy, law and socio-economics

The keywords in any vision for the future Information Society should be *trust* and *trustworthiness*. They form the basis for our communications, transactions and economic and social behaviour in the private, public and privatised space.

The relational and contextual properties of trust make it

impossible to completely engineer trust in digital life. It will always depend on emotions, circumstances, and personal moods, and it will change with cultures and social environs. Nevertheless, there are elements which can help to establish trust; some based on existing laws and regulations which can be fully applied or made applicable with relatively small changes. Building new mechanisms and tools that help citizens, enterprises and public organisations to control their assets and flow of actions may also contribute to the establishment of trust.

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 Life[4] could be a first step.)

4.3. A common European framework for Identity management

An essential element for ensuring a trustworthy Information Society is a framework for authentication and claim management, including governmental eID systems. Trust is built primarily on information about the other party in any relationship. Such a framework is needed for accountability, non-repudiation and transparency.

Europe needs a common framework that allows federation and forms of interoperability between all these systems. At the same time, we need to ensure reasonable instruments for forensic analysis are available.

The Commission has proposed the development of European Large Scale Actions, on e-Identity, in its Communication[5]. Members of RISEPTIS have developed a roadmap which details actions to be taken to achieve a common European framework.

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.

4.4 Further development of EU legal Framework for data protection and privacy

Discussions are ongoing on further developing the EU legal framework for data protection and privacy. In the proposed Directive[6], mandatory data breach notification has already been extended. Researchers[7] have questioned the completeness of the definition of personal data, in relation to location-based information and profiling. Technology developments in data linking suggest that in the future any data may become personal data at some point in time.

Development of the legal aspects should be part of an overall policy that should be closely interlinked to technology progress. This would enable more efficient reaction.

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.

4.5 Large scale innovation projects

It has been argued that Europe is in a strong position to take a lead in trust and security technology development and innovation. However, substantial and coherent European largescale projects, which take full advantage of these European strengths, need to be targeted.

Europe should develop a techno-legal ecosystem for trust, security and privacy that should be amenable to global cooperation, boost European growth and provide a solid basis for international cooperation.

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.

4.6 International cooperation

The Internet and Web form a global infrastructure for communication, data processing and service provisioning. Explicit steps should be taken to reach an international understanding, cooperation and interoperability, and to work at joint international measures and standards on governance, anti-crime measures, identity management, security and other relevant topics.

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.

---

[4] <http://trustindigitallife.eu/Home%20Page.html>.
[5] COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game.
[6] Proposal for a Regulatory framework for Electronic communication networks and services.
[7] Rannenberg, K. Royer, D. and Deuker, *A The Future of Identity in the Information Society*, Springer 2009.

