TRUST IN THE INFORMATION SOCIETY

A Report of the Advisory Board RISEPTIS

Research & Innovation on Security, Privacy and Trustworthiness in the Information Society

In Collaboration with:

Think-Trust
www.think-trust.eu

Trust in the Information Society

A Report of the Advisory Board

RISEPTIS

Research and Innovation on Security, Privacy and Trustworthiness in the Information Society

Foreword

In the first fifteen years of its existence, the World Wide Web has had a profound and transformative impact on all facets of our society. While the Internet has been with us for 40 years, the Web has caused an exponential growth of its use; with up to 1.5 billion users worldwide now accessing more than 22 billion web pages. 'Social Networks' are attracting more and diverse users. With 4 billion subscribers to mobile telephony across the globe (there are almost 7 billion people on earth) and mobile phones being increasingly used to connect to the Internet, mobile web applications and services are developing fast.

And there is much more to come, which will go well beyond information processing and data exchange. The 'Internet of Things', the Semantic Web and Cloud Computing are all evolving fast, reflecting the dynamism of the technology developments that are related to the digitisation of the world around us and our relationship with it. They in turn raise issues of e-Identity and Trust in the digital interactions they enable.

However, while we are staring at this amazing new world and getting excited by the use of previously unimagined devices, we are also perplexed and concerned by the ease with which our data can be stolen, our profiles used for commercial purposes without our consent, or our identity purloined. We get more and more alarmed by the loss of our privacy; often justified by unseen security requirements, or by the risks of failures in and deliberate attacks on our critical infrastructures. The trustworthiness of our increasingly digitised world is at stake.

I read in this report about Jorge and Theresa living happily together, due to the many new convenient services made possible by technological advances in our digital society. Medical services based on trustworthy health records, jobs that are not strictly bound to a geographic location thus enabling the couple to live together, ambient assisted living that ensures proper care for older family members, as well as travel and hotel facilities adapted to their personal wishes.

At the same time they encounter unforeseen problems with the police, they worry about control over their personal data, which is now in the hands of hotels or doctors, and seem to get locked into the services of large insurance and care organisations.

We may be scared with the idea that we will have to live with a "digital shadow" that does not forget possible past little misdemeanours or indiscretions, and which can then be accessed by future employers or partners. The idea of being robbed or cheated by somebody at the other end of the world whom you have never met, without understanding how it happened and with little chance for legal redress, seems intolerable for European citizens.

I am very grateful that the RISEPTIS Board has addressed these issues in this report, founded on the key principle that a European Information Society should comply with the long-standing social principles that have served Europe so well to date. 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 for effective human communication and business transactions, and hence, for growth and competitiveness.

I am fully in favour of the recommended approach to technology development, comprising strong interaction between social innovation and the development of policy and regulation. Indeed, we need to develop the instruments to support this. Uncontrolled technology development and innovation can lead the Internet and the Web to become a jungle; where trust is lost, crime and malfeasance rise and each individual is forced to defend themselves with limited tools. At the same time, policy development without awareness of technology development and trends will choke innovation and economic growth. Most importantly, if citizens feel threatened, mistrustful and increasingly hesitant towards innovative applications and services, our whole society may end up being the loser.

I would like to thank the RISEPTIS Board for this insightful report and their constructive recommendations. I am convinced that the discussion started in this Report is a worthwhile and timely one and can help Europe to find the right way towards an Information Society that is wanted and deserved by its citizens.

Viviane Reding,

Member of the European Commission
Responsible for Information Society and Media

RISEPTIS: Advisory Board FOR RESEARCH AND INNOVATION IN SECURITY, PRIVACY AND TRUSTWORTHINESS IN THE INFORMATION SOCIETY

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, THINK-TRUST, 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.

RISEPTIS Membership

Chair:	George Metakides (U.Patras, CTI)
Members:	Dario Avallone (Engineering) Giovanni Barontini (Finmeccanica) Kim Cameron (Microsoft) William Dutton (Oxford Internet Institute) Anja Feldmann (Deutsche Telekom) Laila Gide (Thales) Carlos Jimenez (Secuware, eSEC) Willem Jonker (Philips) Mika Lauhde (Nokia) Sachar Paulus (U. Brandenburg, ISSECO) Reinhard Posch (CIO Gov. Austria, TU Graz, A-SIT) Bart Preneel (KU Leuven) Kai Rannenberg (U. Frankfurt, CEPIS) Jacques Seneca (Gemalto)
Observer:	Peter Hustinx (EDPS)
From Think-Trust:	Willie Donnelly (WIT) Keith Howker (WIT) Sathya Rao (Telscom) Michel Riguidel (ENST) Neeraj Suri (U. Darmstadt)

With support of: Jim Clarke, Zeta Dooly, Brian Foley, Kieran Sullivan (WIT)

Jacques Bus, Thomas Skordas, Dirk van Rooy (EC, DG Information Society and Media)

CONTENTS

Executive Summary and Main Recommendations

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.

Although the Web has only existed for about 15 years, it has quickly permeated our lives and society, through such concepts as: communication anytime and anywhere; Social Networks connecting people globally; ubiquitous information provision; and, numerous public and private digital services. However, with the Web moving towards the centre of our society, its many weaknesses are also exposed. We see cyber criminals exploiting networks' vulnerabilities, terrorists using the Web for information exchange and communication, data loss and data breaches, Identity theft and commercial data profiling and linking. Worse still, all of these undesirable interactions are increasing in frequency.

> The Internet is the network infrastructure that allows computers to communicate with each other. Sitting on top of this is the Web, which is a means of accessing information via the Internet. In this report, as in everyday language, the term "Internet" is often used to include the two together.

The Web also brings with it uncertainty at the level of the State; concerning applicable law, jurisdiction and law enforcement in global networks and the protection of its citizens and critical infrastructures. It renders business investments hazardous due to uncertainty when it comes to responsibility and liability, as well as affecting the development of infrastructures and regulatory environment. Citizens feel uncertain about the lack of transparency, accountability and control of data processing. The current rapid development of the digital space, including the Internet and the Web may well lead to a loss of trust in society and, hence, adversely affect economic growth.

This Report is divided into 4 chapters:

Chapter 1 introduces the Report and gives a contextual overview of the main themes and issues addressed therein.

Chapter 2 describes the use of concepts such as trust, trustworthiness, identity and accountability and explains how these relate to the EU legal framework of personal data protection and privacy. The case is made for their importance in society, as is the need to develop technology for trustworthy platforms and tools which properly transpose these concepts into digital space.

Chapter 3 discusses two concrete problems regarding our move towards becoming a more digital world, before presenting a picture of a possible near-future through a storyline that illustrates the issues at stake.

Chapter 4 lists out a number of recommendations based on the preceding chapters. Priorities for future research agenda and ICT work programmes are included in this recommendations chapter.

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.

Europe is well placed to lead the global trust and security drive in the Information Society. It has industrial strength in, for example, mobile communication, services, consumer industry, as well as academic strength in fields such as cryptography, formal verification and validation, identity and privacy management. Its political history, comprising extensive expertise in international diplomacy and cooperation, and most importantly it's broadly-established, strong social model, respecting freedom and the private sphere, gives Europe the authority to lead in building the necessary global frameworks and governance structures.

It would be too enormous a task to analyse, in the context of this report, all of the problems and to provide solutions for trust, security and privacy in the future Information Society. The Web has not yet matured and we will continue to encounter many surprises. Much research, societal discussion and experimentation remains to be done. 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 citizen-friendly Information Society.

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

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[1] could be a first step.)

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.

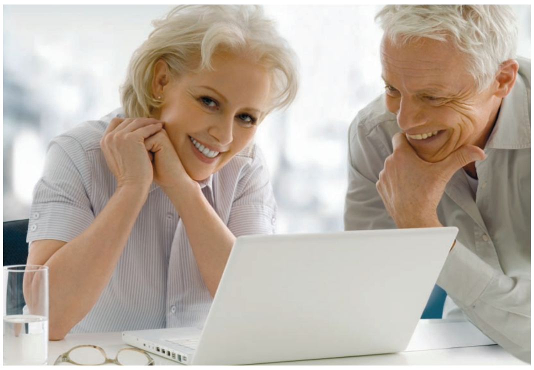
Recommendation 4: The EC should work towards the further development of the EU data protection and privacy legal frameworks as part of an overall consistent ecosystem of law and technology that includes all other relevant frameworks, instruments and policies. It should do so in conjunction with research and technology developments.

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.

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.

Further details on these recommendations are given in Chapter 4.

[1] http://trustindigitallife.eu/Home%20Page.html



01 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. It also deeply affects human communication and transactions, and the way in which we deal with information and knowledge globally. 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.

The trust of our society in the new generation of ICT products and services is at stake. And with it our competitiveness and economic growth, since these are strongly dependent on trust levels in a society. It may be counterintuitive to think that digital technologies, infrastructures, products and services are still at a relatively early stage of development.

But the Web, one of the most transformational technologies, has really been with us for only about 15 years. It is indeed still going through a sort of adolescence period.

> *"Do you want the internet to turn into a jungle? This could happen, you know, if we can't control the use of our personal information online. Now, privacy is a particular value for us Europeans; a value reflected in European laws for many years. However, in spite of the many advantages of technological development, there is an undeniable risk that privacy is being lost to the brave new world of intrusive technologies. On the global information highways, personal information is increasingly becoming "the new currency". And I believe that Europeans in many ways take fuller advantage of new technologies than other continents – just look at Europe's strong broadband and mobile phone take-up. I believe that Europeans must have the right to control how their personal information is used.*
>
> *…*
>
> *The European Commission takes the protection of your personal information very seriously. We all have a fundamental right to privacy, also when using new technologies.*
>
> *…*
>
> *I finally believe that it is imperative for the next Commission, which will come into office by the end of this year, to review Europe's general rules on protecting personal information, which date back to 1995. Such a reform is long overdue, in view of the rapid technological development."*
>
> From: Commissioner Reding's weekly video-message, 14 April 2009

Some figures:

- 1.5 Billion Internet users worldwide, up from 360 Million in 2000
- Users spend about 32.7h/week on the Internet, compared with 70.6h for all media, and 16.4h watching television
- The Internet represents 32.5% of the typical "media day" for all U.S. adults.
- 4 billion mobile users world wide
- The web is estimated to contain 22 Billion pages (in 2009)
- Facebook and MySpace have each attracted more than 200 million users worldwide
- Social video sites add 13 hours of user videos to the Internet every minute.
- User-generated content such as YouTube produced more than 73 billion streams in 2008

But:

- In 2008, Symantec detected 1,656,227 malicious code threats, this is more than 60 percent of the approximately 2.6 million that Symantec has detected in total over time
- In 2008, the average cost per incident of a data breach in the US was $6.7 million, which is an increase of 5 percent from 2007. Lost business amounted to an average of $4.6 million per incident
- Roughly 8.4 million U.S. residents were victims of identity theft
- An academic study reports that a quarter of the public-sector databases reviewed in the UK [of a total of 46] are almost certainly illegal under human rights or data protection law

In the last four years alone we have seen the rise of Social Networks which, in turn, are fast evolving into complex professional platforms, significantly transcending their original concept. And there is much more to come.

As with most adolescent experiences, there is new ground to be broken, with occasional traumatic experiences along the way. Loss or extreme curtailment of privacy could easily fall into this category. As the role of the Web moves from the periphery to the centre of social and economic activity, its vulnerabilities are exposed.

Hackers, criminals, terrorists and other malevolent entities have shown how easily the Web's weaknesses can be exploited. This exposure has been facilitated by a lack of user awareness and sensitivity, technologies and infrastructures that were not developed with such threats in mind, and the fact that governance and jurisprudence have not kept up with developments.

Networks and systems become increasingly vulnerable to attacks from various sides. A stunning percentage of computers worldwide are infected with malware; turning them, potentially, into unwilling malfeasant zombies, with their owners unaware of the illegal content stored in and activities performed on their machines - all under their legal responsibility.

Through new forms of social interaction, social platforms and networking as well as through access to Web services and other online activities, we leave behind us life-long trails of personal data in the form of a *digital shadow* that becomes increasingly difficult, if not impossible, to shake off.

Data can be stored, aggregated, processed, mined and used anywhere in unforeseen ways by numerous different entities with little protection, giving rise to new problems of transparency and accountability.

The new digital world, of which the Web is the most important part, is a fragile one. And as with every adolescent, the Web needs some sort of guidance, which should strike the right balance between preventing it from becoming a jungle or wasteland and overly restricting and thus suffocating its immense creative potential and development.

This report endeavours to make a contribution towards striking such a balance in the full realisation that this will indeed be a long process in a rapidly changing context.

Europe is uniquely placed to play a leading role in the development of trust and security in the future Information Society, as the latter evolves in terms of new technologies (products or services) and new policies (directives or regulations).

Europe has clear industrial strengths and assets in areas such as mobile communications and services, as well as consumer industry and system security. It also has a number of world-leading research communities, working in areas such as architecture, cryptography, formal verification and validation, and identity and privacy management. Moreover, Europe has a leading role in the Web Science Research Initiative[2], which has pioneered the approach of Web science.

The first steps towards cooperation have already been launched by the Commission to ensure an interoperable and trustworthy ID management platform in Europe[3], following joint efforts of Member States in the project STORK[4].

Europe has experience and strength in seeking consensus at both European and transcontinental levels and between stakeholders of different cultural backgrounds; something that is essential in the quest for interoperability and trust in a global digital economy. Most importantly, Europe has a broadly established social model, respecting freedom and liberty with particularly strong attention given to privacy[5]. The EU, and in particular the Member States acting in their own interest as well as that of the whole EU, have a heavy responsibility to protect and further develop this model for our digital future.

Trustworthy systems and practices have always been part of the essence of European societies. Whether written as legal code, simply practiced as a code of honour, by habit induced through education or based on secure and reliable technology and management, trustworthy systems provide the glue that holds together elements across the entire societal spectrum - needless to say that with the Web coming of age, our systems and practices should keep pace.

This report attempts to recognise, among the ranks of emerging problems related to trust, security and privacy, those that pre-existed and are simply inherited in a digital guise; which can be addressed satisfactorily with existing knowledge and established measures, thus ensuring continuity and stability. Where, for such inherited problems, their new digital reincarnation entails differences in scale or applicability – rendering them qualitatively different - the report attempts to recommend research or additional actions deemed necessary.

There is also a category of new problems which arise with unprecedented speed and impact and which, after a first analysis, do not seem amenable to handling through established approaches. For such problems, further research or action might be pointed at when it is felt that there is enough evidence and understanding for doing so. But for other new problems, this Report simply raises the issues involved and points to the need for further research, with concrete recommendations to come at a later stage.

This approach has led to the recommendation of the main topics identified for research, which are needed to develop new infrastructures, technology and tools. It is recommended to consider these for future

[2] http://webscience.org
[3] COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game
[4] http://www.eid-stork.eu/
[5] ISS Report 05, Feb 2009: The European Security Strategy 2003-2008 – Building on Common Interests

ICT work programmes related to Trustworthy ICT.

As an illustration of other recommendations this approach has led to, we can mention one providing a possible path for the development of a common European platform for privacy-protecting identity management based on state-of-the-art research achievements; or another concerning the development of tools and instruments for businesses and citizens to make informed decisions on data management and digital security.

In no way does this report profess to know how the future Information Society will further develop or what it will look like in the years ahead. In completing this report we have searched, as thoroughly as we could, for existing analysis and recommendations in the field. In fact, numerous good reports have already been presented with insight and guidance from different vantage points and these are referenced in this document. Also, substantial agreement has been reached through these various other reports, on many key issues and how to address them.

This report describes concepts, stakeholder views, and problems in Chapter 2. It then illustrates these in Chapter 3 through a number of related, near-future scenarios. Conclusions and recommendations are given in Chapter 4, which could lead to a balanced approach to some of the problems discussed.

In this report, we provide links to the valuable work that has already been carried out in this domain and we try to build on this. Adopting the approach presented above we hope to make a substantial contribution to this fast moving, complex and fascinating process.

02 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. Based on this we highlight some perspectives of stakeholder groups. Finally, we discuss ongoing research technology developments and the requirements of infrastructure and governance.

2.1. Concepts

Trust, trustworthiness, identity and identification are concepts which are at the basis of human existence. We use them intuitively and their interpretation is often context dependent. Related to this, societies have developed concerns for privacy as a human right. When we transpose these issues to a digital environment, we can easily run into trouble. For the purpose of this report, in order to avoid confusion, we adopt interpretations of the concepts as given below.

We see **trust** as a three-part relation (*A trusts B to do X*). Parties *A* and *B* can, in this respect, be humans, organisations, 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. It is contingent on time (one could easily lose trust in someone, but also the concept changes over time); history and memory; place and situation; culture; role (private or professional); emotions; and, a number of other variables (For example, sociological considerations like reputation, recurrence and recommendation). Trust is easier to establish when the identity and/or other authentication information (claims) about the third party are known. Where human interaction involves the exchange of personal information, citizens will trust the handling of data within their society if: privacy and personal data protection regulation is respected; organisations comply with citizens' perceptions of a culture of accountability, auditing and transparency; and responsibility and liability in the chain of actors in a transaction is well established, allocated proportionally through regulation and contracts, and enforceable in an efficient manner. Moreover, citizens and organisations must have fair tools to enable confirmation of claims made by another party and to access information about reputation, creditworthiness, identity, etc.

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*. Moreover, Trustworthy Systems should provide tools and mechanisms (or allow third-party service providers to do so) that enable the user to assess the risks and audit the qualities it is claimed to possess. These tools and mechanisms should also support the user, where relevant, in his security and trust management.

For further discussion on these two related concepts, see Russell Hardin[6], Kieran O'Hara[7] and Trustguide[8].

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.

In FIDIS[9] (an FP6 'Network of Excellence' project), an effort is made to conceptualise these notions. Two perspectives are described:

(1) A *structural* perspective, in which identity is seen as a set of attributes characterising the person (or other entity) in a certain context;

(2) A *process* perspective with identity attributes used for identification; here identity is considered according to a set of processes relating to disclosure of information about the person and usage of this information.

Within some cultures, the State has developed a way of distinctively registering each of their citizens to ensure uniqueness of identity. However, in reality a person manages many identities (as a citizen, an employee, a consumer, a client, a patient, a parent, a victim, etc.). Sometimes the same identity is shared by many people (e.g. a guest account). FIDIS established for this the notion of "Partial Identities".

In this report we will take a process or functional approach and refrain from the more philosophical thinking about identity in terms of the set of essential attributes or characteristics of a person or personhood[10]. Physical or virtual persons seek access to data or services, or take responsibility for certain actions in digital space. Service providers may need to authenticate themselves to the customer. To do this, the parties involved often need to prove certain claims about themselves to convince the "relying party" (service or data provider, auditor, employer, customer) to trust them sufficiently to allow the transaction, exchange or communication to proceed. Such claims include, for example: name, birthday, age, being older than 18, a credit card number, a company registration, a password, personnel number, biometrics, etc. A relying party will act as requested if it has sufficient trust in the claims provision. In this discussion we will be led by basic principles laid down in the EU legal framework.

The OECD formulated guidelines for privacy protection in 1980[11]. In an effort to develop a set of general implementation principles for the Internet, Kim Cameron presented, in 2005, his *Laws of Identity* [see Fig. 1]. Within these Laws, the process of authentication, where a subject would use a trusted claim provider to prove its claims to the relying party, is described formally at a meta-level[12]. Clearly, the claims provided for a certain transaction depend on the transaction, the parties and the context. To obtain a passport from a public administration office, to make a payment through e-banking, to gain access to a web community, or simply to provide comments on a blog, all entail different considerations when identifying oneself.

Anonymity refers to the absence of identifying information associated with a natural person. In such cases no claims allowing

[6] Hardin, R. *Trust & Trustworthiness*, Russell Sage Foundation, New York 2002

[7] O'Hara, K. Trust: From Socrates to Spin, Icon Books, Cambridge 2004

[8] Lacohee, H. Crane, S. and Phippen, A. Trustguide: Final report – www.trustguide.org.uk

[9] Rannenberg, K. Royer, D. and Deuker, A The Future of Identity in the Information Society, Springer 2009

[10] OECD "At a Crossroads: Personhood and Digital Identity in the Information Society", http://www.oecd.org/dataoecd/31/6/40204773.doc

identification are provided, although other claims might be needed (e.g. non-repudiation). Pseudonymity is the situation where certain claims are provided (For example, a number or login name and password), but these cannot be connected to directly obtain identification; however, the natural person is still identifiable, if necessary. Similarly, one can argue about the identity of organisations, or artefacts, although the claims might be of a different character.

THE LAWS OF IDENTITY

1. User Control and Consent: Technical identity systems must only reveal information identifying a user with the user's consent.

2. Minimal Disclosure for a Constrained Use: The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3. Justifiable Parties: Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity: A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies: A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6. Human Integration: The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience Across Contexts: The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Figure 1 The Laws of Identity[13]

2.2. Trustworthiness in context

Trustworthy systems and practices have always been part of the essence of almost any society. Whether written as legal code, simply practised as a code of honour, or based on secure and reliable technology and management, trustworthy systems are the adhesive elements across the social spectrum. ICT solutions create enormous economic and social benefits for citizens, businesses and governments and these must be embraced. However, prerequisites for the optimal and rapid acceptance of ICT solutions by citizens and society include: (a) ensuring trust in their use; and, (b) providing assurance that personal integrity is protected and opportunities for criminal abuse are minimalised.

The current technology evolutions, including Web 2.0, Cloud computing, the Internet of Things and others still to come, will bring more data collection, a higher persistency of data in digital space, higher scales and more heterogeneity, pervasiveness and increased complexity. This will affect various elements of trust and render its management more difficult.

Our Information Society is partly being built on a virtual environment comprising increasingly uncontrollable, opaque, mobile computer programmes, and a scattered cloud of volatile yet persistent information. The computer landscape and information highways are becoming congested and fragile, caused by insufficient knowledge and control of underlying infrastructures by its designers, manufacturers and vendors, and by the lack of transparency for users. This leads to high vulnerabilities for our society and our economy. The reasons are manifold: technological, practical, economic, and sociological. Moreover, main concerns are directed towards technical interoperability and inter-compatibility rather than security and operational reliability.

[11] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_37441,00.html

[12] Cameron, K. Posch, R. and Rannenberg, K. Proposal for a Common Identity Framework: A user-centric Identity Metasystem www.identityblog.com

[13] See: http://www.identityblog.com

We should not however, give the impression that ongoing efforts towards trustworthy systems have been uniformly inadequate. The score is uneven. In some domains, such as banking, problems arising are dealt with more adequately than in others – health, for example.

Moreover, some of the issues that are developing could be viewed as straightforward transpositions of older, well-understood problems, which are now appearing in a new digitally enhanced context. These can be tackled with existing legislation; albeit adjusted to the new context. An illustration of this is blackmail or libel in the blogosphere.

Other problems appear to be genuinely novel and less amenable to a simple transposition of existing provisions. These will need sufficient attention. Some of these relate to the increasing complexity of networks and systems and the need to ensure sufficient security and resilience of the infrastructure. The absence of a tangible "salesperson" that can be seen and identified in a web transaction is another new challenge.

Nevertheless, **trust** remains essentially the "classical" concept we know, and which needs transposition to the new, digital space.

2.3. The EU legal framework for personal data protection and privacy

The Internet and Web emerge together as an essential system for daily communication, an increasing variety of services, and massive data exchange. In the future, mobile networks, the Internet of Things, as well as *Linked Data*[14] will form seamless parts of it. As a consequence, we will see an explosion of content, and the architecture of data and programmes associated with an individual or an organisation will become highly complex.

The high dependency on ICT undoubtedly creates many vulnerabilities in the systems that process data, whilst at the same time citizens fear the potential "surveillance society" that may arise through arguments for civil security and safety, as well as technology use. Indeed, many activities, that were not traceable in the past, are traceable now, due to the use of media and recording; and virtually unlimited storage capacity.

In 1948 the UN adopted its Universal Declaration of Human Rights (UDHR), which states in Art.12: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

The 28th International Conference of Data Protection and Privacy Commissioners (London, 2006) stated: *"The protection of citizens' privacy and personal data is vital for any democratic society, on the same level as freedom of the press or the freedom of movement. Privacy and data protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous."* In this context, great attention is given in democratic societies to the means of assuring privacy and the protection of individual rights and personal life without negative impact on neither the general public interest, the vital interests of involved parties or legal and contractual obligations. It is argued that all legitimate interests and objectives may be accommodated without unnecessary trade-offs being made.[15]

In Europe, technology or economic considerations have in the past often been looked at in relation to our basic values and fundamental principles. The French Act of 1978 on Data Processing, Data Files and Individual Liberties[16] provided an early and clear statement that *"… information technology should*

[14] Using the web to connect related data that was not previously linked; see http://linkeddata.org

[15] See: Cavoukian, A. and Hamilton, T. *Privacy Payoff*, McGraw-Hill 2002 and Cavoukian, A. ***Privacy by Design***, IPC Ontario 2009 www.ipc.on.ca

[16] www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

be at the service of every citizen …" and *"… shall not violate human identity, human rights, privacy, or individual or public liberties …"*. The German Constitutional Court ruled in 1983, that: *"Informational Self Determination is a fundamental constitutional right, as citizens who do not know who knows what about them will be less active in public and democratic activities, which could lead to a chilling effect on democratic life and culture as a whole."* These approaches have led to the inclusion of a specific right to "protection of personal data" in the Charter of fundamental rights of the European Union adopted in 2000.

Europe currently has a relatively strong legal framework for data protection. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[17] is transposed into law at member state level. The Directive establishes a set of rights for the data subject (including the right of access; the right of rectification; the right to object; the right not to be subject to automated individual decisions; etc.). It also sets obligations to be respected by the data controller (including the obligation to provide certain information - determined by the legislation - to the data subject; to notify the data protection authority; to adopt technical and organisational security measures; to avoid, in principle, the transfer of personal data to third-party countries that do not provide for an adequate level of protection; etc.). Finally, it provides for elements of accountability, transparency and law enforcement (through prior checks by the supervisory authority, publicising of processing operations, the right to judicial remedies, liability for unlawful processing and sanctions in case of infringement).

Specifically for the ICT sector the EU has established the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector[18] (known as the "e-privacy Directive").

This framework defines:

> *personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

Its structure is based on three concepts defining the space for actions:

1. *material scope:* which information and information processes, storage procedures etc. do we address with the legal framework

2. *personal scope:* which roles are the relevant ones in this context (data controller, processor, subject), and how is accountability and transparency related to these roles

3. *territorial scope:* applicable law, cross border data transfers, EU regulation and international rules and agreements.

How, in this framework, can citizens' worries be better addressed? What are the measures that can be taken within this framework to reduce security breaches, and further improve accountability and transparency? Can better alignment be obtained with other legal instruments concerning consumer protection, product and service liability?

And, more importantly, can technology development provide the architectures, systems and tools for effective implementation and enforcement of applicable law.

It is obvious that constructive answers to these questions can only be found if we take a simultaneous and coherent approach along all three lines of action:

[17] OJ L 281, 23.11.1995, p. 31

[18] OJ L 201, 31.07.2002, p. 37

- *Development of practical and effective technology implementations*. New system architectures that support privacy by design, new security instruments and infrastructures aiming at prevention, protection and recovery, legal reporting templates and languages, and assurance methods.

- *Policies, procedures, contracts, legal templates* and *standards*. A coherent legal infrastructure is needed, with support for compliance and law enforcement. It should include accountability, transparency, reporting and audit practices in data and software management and use, and it should enable redress and compensation, as required.

- *People and organisations*. We must strengthen the responsibility of management for personal data processing and for ICT usage, through training and awareness programmes and the development of 'best practice', as well as mandatory transparency.

None of these three lines of action can be addressed in isolation, and it is this principle that forms the basis of the philosophy behind this report.

It can be argued that data used for profiling (including location-based data or Web profiling), may "relate" to an "identifiable" natural person, and hence may fall under the definition of "personal data"[19]. However, this is a non-straightforward issue and might need to be addressed in more detail. For example, when making his decision whether data processing is legitimate, can a data controller always reasonably know whether that data can be used for profiling at some stage later? One may argue that at some point in the future any data can become a personal data through "linked data".

Other questions arise about meta-data and even encrypted data that can reveal IP addresses visited. There are also questions regarding data contained in RFID tags that are attached to things which may change hands – can this be labelled "personal data"? Data captured and stored by sensor technologies about a person's whereabouts and their interactions with the environment may constitute "personal data", but it depends on an understanding as to what it means to be identifiable. For example, should the use of biometrics to re-recognise a person, without linking this data to a name, address, etc. be considered use of "personal data"?

These questions are being discussed in the previously mentioned FIDIS project. In general, we may ask whether the focus of the legal framework on the concept of "personal data" can solve the problems that will occur in an ever more dynamic and smart world, in which data is constantly in flux and correlated with other data. It is clear that constant vigilance is required concerning interpretation, completeness and consistency of the legal framework in relation to new technology, which may rapidly change digital reality.

Protection of personal data is one of the most important aspects of privacy. The person concerned (data subject) would like to be in control of his own personal data or to trust the organisation who handles it. The role, trustworthiness and accountability of the relevant data controllers are therefore of crucial importance, since much personal data will be under their control. Technology support in this process is essential, so as to provide the knowledge and tools needed to the data subject, to exercise his/her options; and to ensure transparency and accountability of the data controller towards the data subject to enable assessment of trustworthiness.

[19] Opinion 4/2007 on the concept of personal data of Art 29 DP Working Party. Information "relates" to a person also where it may have a direct impact on that person. To determine whether a person is "identifiable", account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify that person (Recital 26 of Directive 95/46/EC). Both elements therefore, also depend on the relevant context. This is fully illustrated with many examples in Opinion 4/2007.

2.4. Privacy, anonymity and accountability

Privacy has aspects which go beyond legislation, that are more difficult to model, and are dependent on culture, time and other contextual elements. While the legal framework is applicable in all cases, it is useful to look at these other aspects to understand what are the necessary architectures and tools that fit best in certain contexts.

The concept of privacy and its evolution has been studied by various authors[20, 21, 22]. *O'Hara* and *Shadbolt* [23] give a vivid description of its evolution under the influence of the Web. It may help to structure thinking if we consider its tri-partite distinction: the *private realm* of intimacy and individualism; the *public realm* or *realm of the polis* of citizenship and active participation for the societal good (this includes professional activity); and in between these two a *third realm – the privatised space* - of public life, sociability and public opinion, with public interactions and visibility, but private reasoning and motivation. *O'Hara* and *Shadbolt* argue that the Web, as a public information space, currently functions, for a large part, as a privatised space, midway between the completely public and the completely private realms. Such spaces are important for the formation of public opinion and the development of a constructive discourse about society. It is here where personal opinions can be expressed without constraint, except for being within certain legal rules limiting freedom of expression. At the same time, one can publish his own very personal and intimate information if one so chooses, assuming one can do so in an appropriately informed fashion. Naturally, legislation comes into play where publishing the information of others.

But digital space, of which the Internet and Web are the most important platforms, is becoming more and more a public space, where services from business and government are provided, and formal transactions made. Such services can be performed in the Cloud, creating massive amounts of data about individuals, introducing serious problems of informational self-determination, and thus violating the essence of what was previously described as the privatised space.

In fact, the Web and the whole of digital space, is also used as private space, in which people assume, often incorrectly, that data is not accessible to anyone, other than those friends or family to whom it has been addressed. Similar situations were appearing previously within the telephone network, where conversations could, and still can, be eavesdropped without knowledge of the callers.

Privacy can be looked at in terms of informational self-determination (including the right to act anonymously), but also in terms of spatial privacy - the space to retreat. Both aspects of the privatised space are profoundly changed with the Web. Information control in digital space (including control of personal data) is substantially more difficult, and visibility of acting in this space is, at least at this moment, practically absolute (although it could well be that nobody will ever see such "long tail" visibility). Clearly, the privatised space is, in practice, the most difficult to manage and control for a citizen acting in digital space. Visibility is sometimes deliberately sought, while in other cases it is avoided. (Often, tools to support this invisibility are unavailable.) Personal information can be generated by oneself and by a third party (through profiling and data linking, for example). It can be made accessible on one's own website or via a social network run by a private company in the Cloud. It can also be used only proprietarily, for commercial purposes. All these choices have business and legal consequences which need to be understood and may require new or revised legislation and technology tools.

[20] Rigaux, F. *La protection de la vie privée et des autres biens de la personnalité*, Emile Bruylant Brussels, 1990

[21] "The theory and politics of the public/private distinction", in Weintraub, J. and Kumar, K. (eds), *Public and private in thought and practice: Perspectives on a grand dichotomy*, Chicago, Univ Press, 1997, 1-42

[22] Habermas, J. *The structural transformations of the public sphere*, Cambridge, 1962 (trans 1989)

[23] O'Hara, K and Shadbolt, N. The spy in the coffee machine – *The end of privacy as we know it*, Oneworld Oxford, 2008.

In the early days of the Internet, principles of the private and privatised space were enabled through the option of using any one of a vast array of untraceable access points to the Internet. This facilitated users to act anonymously, in practice. These are now gradually being removed for the sake of accountability on the Internet, in favour of the public space. To preserve the societal values of the privatised and private spaces, a number of initiatives have been undertaken to enable untraceable, anonymous activities on the Internet.

Whilst in the private realm, one should have privacy and *untraceability* by default, in the privatised realm one should have informational self-determination and the *ability to claim* privacy and untraceability, if desired within certain legal limits. Such claims can be total or partial: "anonymity in front of a particular person or a certain group", making it impossible for a defined set of stakeholders to uncover the user's identity.

Accountability, as it is normally seen, relates to acceptance of responsibility for activities that: are under contractual obligation; require compliance with legal obligations; or, are carried out in the public interest or when exercising official authority. The legal framework gives the criteria for making personal data processing legitimate. Technology to support transparency of the processes and allocation of responsibility for the various process steps are both necessary to make accountability more effective.

It seems a logical conclusion that accountability is the essence of the public realm, in compliance with data protection and privacy law, but this must not be confused with enabling traceability of the user. Whereas unobservability and traceability do exclude each other, privacy and accountability do not, and there are many use cases where a combination of both would enable taking full advantage of the digital space. A typical case is the health record where the accountability of the doctor for the quality and integrity of the data as well as the privacy of the patient both play a role in the data management.

Within a technological infrastructure, the challenge is to reinforce the legal framework, by understanding these concepts and their inter-relations in digital space[24], leading to "technologically embodied law of a digitised constitutional democracy"[25]; for example, including technical support for privacy-friendly accountability.

Technology development should aim at alleviating the need for our societies to limit privacy if it would conflict with general public interests; for example, in the case of national security or legitimate suspicion of criminal behaviour. Currently within the EU, this maxim is partly subject to interpretation by the data controller or its transposition into Member State law. One would assume that personal data is only uncovered by administrative authorities when there is legitimate cause. However, as noted already, at some point in the future any data can become personal data. Transparency of the data controller actions is essential for the data subject in such situations and Art 12 of D95/46EC provides the right to be informed about the logic of processing that is the basis of automatic decisions. Such transparency should not only include processes used for data processing, but also types of profiling actions to understand the nature of profiling actions and profiles, and support appropriate governance.

The decisions on the rules, technologies, processes and limitations are in the political realm and they differ between cultures. They also change over time. The discussions on the fear for a surveillance state or "big brother" scenario illustrate this. Development of trustworthy ICT can help to avoid conflicts between privacy and security and make it a positive-sum game.

[24] Weitzner, D. Abelson, H. Berners Lee, T. Feigenbaum, J. Hendler and Sussman, J. *Information Accountability*, 2008

[25] Hildebrandt, M and Koops, B-J (eds) *A vision of Ambient Law*, (2007) available at www.fidis.net

2.5. Stakeholder perspectives

For a broad view on the problems we need to look at various stakeholder perspectives. Important parties in this discussion are: *government*, *business* and *citizens*. Below we look at some important aspects of these perspectives.

2.5.1. Governments and Jurisdiction

By their global nature, ICT infrastructures come under different laws in different jurisdictions. These various laws are driven by different national interests and political and judicial systems. The liability of perpetrators of security attacks is often difficult to invoke and mostly non-existent across different nations. At the same time, network governance, dynamically established chains of services, software patching, software in the Cloud, provenance of basic IT data (from where it is *created*, to where it is *transmitted*, *stored* and actually *accessed*) and notably cyber criminal networks often span multiple countries and jurisdictions. This raises issues with regard to the role and responsibilities of network-, service- and software-providers concerning the security of their products and services, and of the data controllers and processors as defined in the pertinent EU legal framework. It will not always be obvious or even well-defined *where*, *by whom* and *how* control is exerted and how consumer rights, data protection rights or product liability law[26] can be enforced. A typical problem in this context is the responsibility of the data controller, who utilises various systems and tools of which liability is not clear. More importantly, national security may be at stake if control is lost and law enforcement becomes more and more difficult.

The vast amount of personal information being processed currently makes it practically impossible for consumers as well as suppliers to always explicitly adhere to legal obligations on active consent (opt-in). This is aggravated by fragmentation and often cross-border incompatibility of legal frameworks on privacy and data protection. Although the EU framework is "data-controller centric", the emergence of the Cloud will limit further the ability for user-centric, cross-border data protection, since it is not always clear under which jurisdiction the Cloud provider is established.

Methodologies for solutions need to be found through age-old diplomacy and international negotiation practices. However, the complexity and technicality of digital space may make political control and international agreements on technology developments increasingly difficult.

Law enforcement in digital space is also difficult. Obligations for the reporting of data breaches and an annual review of data processing in organisations, as exists for finances, are inadequate. The lack of proper authentication and privacy-respecting auditing technology, and the obscurity of business processes, seem to create an environment with ever decreasing accountability, responsibility and liability for business and public services.

Administrations are discovering the gains in efficiency and effectiveness that can be obtained by better citizen registration, creating personal health-care records, using biometrics for travel documents, immigration control and anti-terrorist actions, and providing more and more electronic services to the citizens. The change-over however, raises many concerns for data security and unauthorised secondary uses. Several cases have emerged in the last few years, where millions of personal data records were stolen or lost.

Finally, critical infrastructures become fully dependent on networked control systems and connections over borders. Protection of the critical infrastructures, including telecommunication, energy and transport is essential for the national security of States.

[26] Including Directive 1999/5/EC, which requires safeguards in telecom terminal equipment to ensure personal data and privacy protection of the subscriber

2.5.2. Business

Eurobarometer 2008

Organisations' perspective on data protection:

— 91 % "necessary requirements"

— 63 % "but improvements needed"

Today, there is a lack of any incentive for businesses to invest in trustworthy solutions. In many cases, those who decide on and create risks are not those who pay the costs if things go wrong. Also, governments require retention of data processed by businesses, making it more difficult for them to reach agreement with customers about the protection of such data. Technical infrastructures and legal frameworks are needed to assign costs and liability appropriately. This would remove barriers to innovation and uncertainty on regulation and would connect mutually incompatible international legal frameworks. Only if benefits, legal obligations and international frameworks are clear, will businesses sufficiently invest in usable solutions for e-services.

Europe does not have an interoperable, secure and widely usable electronic identity management infrastructure that enables businesses and citizens to use efficient authentication mechanisms for interactions. As a consequence, whereas large companies can rely on identification solutions that they already have available within their organisation, small companies and start-ups need to build them from scratch when bringing innovative services to the market. This can lead to enormous overheads and macro-economic waste.

As argued earlier in this chapter, trust is a vital element for economic sustainability. It is confirmed in literature that there is a strong correlation between the level of social trust in society and economic growth and prosperity[27, 28].

A recent study[29] estimated that the digital service market will grow to €436 billion in market volume by 2012. The study states also: "The difference between "getting Digital Confidence right" in a best-case scenario and "getting it wrong" in a worst-case scenario adds up to €124 billion, or almost 30 percent of the total market at stake—approximately 1 percent of total EU-27+2 GDP in 2012! The combined downside of failing to establish Digital Confidence is, at €78 billion, far greater than the upside at €46 billion—primarily driven by the effects of Privacy and Data Protection as well as Network Integrity and Quality of Service."

A well-developed and globally respected European legal framework for data protection and privacy, commercial transactions and consumer law, all fit for the Internet of the Future. These can give European industry a head start for global competition in innovative products and services that will be trusted by consumers.

2.5.3. Citizens and Society

Eurobarometer 2008

Citizens' perspective on data protection on Web:

64 % "concerned or very concerned"

48 % "data adequately protected"

77 % "only limited awareness"

Citizens and society are eager to avail of the exciting possibilities presented by technology development for communication and information handling. At the same time people are becoming more aware of the potential risks that this creates for security and privacy. From the citizen point-of–view, key issues for trusting ICT solutions are: the allocation of liability and risks in the product- and service-chains; the ease of use and trust in delivery; the ability to make informed trust and security decisions; and, the power of control over their digital assets and personal information.

[27] Fukuyama, F. Trust: *The social virtues and the creation of Prosperity*, Free Press, New York, 1995

[28] Akcomak, I.S. *The Impact of social capital on economic and social outcomes*, Un Press Maastricht, 2009

[29] Digital Confidence – Searching the next wave of digital growth, Booz & Co, Liberty Global Policy Series, 2008

Citizens feel lost by the lack of transparency and accountability of data handling by government and business. They are perplexed by the ease with which they can be profiled, traced and tracked and by the apparent simplicity with which data flows from domain to domain and between businesses and government, without their knowledge or consent. They feel uncertain and unprotected against cyber criminals going after their identity, money, children and dignity.

Citizens want to be safe and secure, with their private space protected; while at the same time they want to profit from the many digital opportunities offered. Essentially, they want a positive-sum game, giving them a clear sense of progress through technology. The goal is to minimize the collection and use of personal data, if citizens don't feel comfortable or feel an affront to their dignity, while at the same time, strengthening data security, and empowering individuals to feel confident in their communication on the Internet and to exercise choice over their own information.

2.6. Research and Technology development[30]

The fundamental building blocks of security have been with us for many years: information encryption with cryptography to protect information in storage or transit; cryptographic protocols to authenticate IT exchanges; secure principles in engineering for the construction of computers and devices whose functionality can be assured; and, methodologies for the provision of software that can be assured – to some degree – to function in expected ways.

However, huge computing capacity in the hands of everybody, as well as hackers discovering and continuing to develop attacks not previously predicted or understood, has resulted in an "arms race", between those developing software components and deploying systems on one side and criminals abusing them on the other. Success in hardening basic layers of the infrastructures against attack (operating systems, for example) has led to new attacks on other "links in the chain" (browsers, for example). Further, hasty repairs and insufficiently tested new applications have caused many more vulnerabilities. The emergence of the Internet of Things will also add a new dimension to reconciliation between the virtual and the physical - between information technology and reality.

We may be able to use and scale-up existing security knowledge in our systems or, in some cases, in certain industrial sectors to re-build the information and service systems of the future, in order to have security and privacy designed in from the start. But the real challenge seems to be to develop new usage models and to produce new paradigms to handle more efficiently and securely the new virtual constructions that come with the Future Internet.

A major weakness of the Internet comes from the lack of reliable verification of claims, including identity. It leads to uncertainty when explicit authentication or non-repudiation is required. In the absence of a reliable scheme, inferior methods are employed that lead to an increased risk of identity theft, phishing, pharming and spoofing. Consequently, mechanisms ensuring accountability, auditing, non-repudiation and law enforcement are increasingly difficult to implement. A trustworthy and privacy-respecting identity claim management regime can ensure that the right people get to the right resources in a practicable way.

Nevertheless, one can never fully exclude theft and/or the abuse of credentials. A major mechanism to reduce risk in such cases is to avoid over-identification – the use of identification in contexts where it provides

[30] For further information on Security research in a wider sense, not restricted to ICT, see the report of the European Security Research & Innovation Forum (ESRIF), http://www.esrif.eu/documents.html

insufficient benefit. Minimal data disclosure technology has been developed to address this. In addition we need accountability properties and mechanisms.

Over-identification could lead in the worst case to illicit network computing, with search engines digging into the private sphere and identifying user profiles and activities (targeted profiling). This is aggravated by the risk that in highly integrated dynamic applications we lose transparency concerning the relationship between the collection of data and the purpose of its use.

The European Commission gives significant attention in its ICT Programme to research and technology development in the field of Trust and Security, with projects and schemes being funded for more than a decade now. The **Work-programme 2009-2010** research targets are:

Trustworthy Network Infrastructures particularly emphasising the development towards the Future Internet. It includes the development of novel architectures with built-in security, dependability and privacy; secure interfaces and scalable dynamic security policies across multiple networks and domains; autonomously monitoring and managing threats; and trustworthy management of billions of networked devices, 'things' and virtual entities connected in the Future Internet.

Trustworthy Service Infrastructures as part of the development towards the Future Internet, supporting adaptability, technical interoperability, scalability and dynamic composition of services for citizens and businesses. Work includes flexible and dynamic mechanisms and risk-based methodologies to respond to threats and vulnerabilities, as well as to changes and conflicting demands in operating conditions, business processes or use practices through the full life cycle. Strong attention is also given to interoperable frameworks for identity management for persons, tangible objects and virtual entities, with emphasis on user-centricity and respect of privacy for personal users.

Technology and Tools for Trustworthy ICT addressing networked process control systems; pro-active protection; user-centric and privacy preserving identity management; risk management and policy compliance verification; assurance of security; integrity and availability of data; complexity and dynamicity; cryptography, biometrics, trustworthy communication and virtualisation.

In addition the programme gives opportunities for *networking, coordination and support activities.*

Significant progress has been made in areas, but the rapidly developing digital world requires reconsideration. The effectiveness of trust and security technology is questionable if it is developed as an add-on to existing systems, as has been the case up until now.

More importantly, trust and security technology becomes uncontrollable and largely ineffective if it does not take into account the individual and societal dimensions. For the **individual** we need to understand how the incentives for behaviour have been altered in the digital world and how new types of collaboration will emerge. For **society**, we need to understand how technology alters the allocation of competing resources; has trust become scarcer as information has become more abundant? The Web, as engineered technology, generates a network of overlapping social networks and a linked repository of content created by humans and relevant to their lives. For all these reasons, an interdisciplinary approach taking into account all these dimensions is essential to make progress. The area of trust in the Information Society is clearly one where insights from Web Science[31, 32], would be applicable.

The recommendations on research and technology development in this report aim

[31] Shadbolt, N and Berners-Lee, T. Web Science emerges, Scientific American, Oct 2008, 32-37

[32] Berners-Lee, T. Hall, W. Hendler, J. O'Hara, K. Shadbolt, N. and Weitzner, D. A Framework for Web Science, Foundations and Trends in Web Science, 1(1), 2006, 1-130

to provide input to the planning for ICT Trust and Security research for the programme period 2011-2013 and beyond. They are based on the work of two Working Groups, which were established by the FP7 project, Think-Trust[33]. Their main findings may be divided into two sections: the first mainly from the user standpoint, with the second looking at means (mainly technological) of supporting the users' needs.

The headline concerns of the first working group are about privacy, identity management and accountability in the Information Society. Wider privacy needs concern the protection of all aspects of identity-related information; not only the prevention of unauthorised or unintended disclosure of the primary parameters of identity, but also limitations on building unique identifying or identifiable personal profiles by amassing and aggregating snippets of information trails that users currently leave behind. Similarly, data protection is not only about the technical prevention of disclosure of personal information, but also about the responsibilities of those handling, processing or storing it.

The second working group centres on what is needed to: (a) support the nomadic, mobile user; and (b) to enable the trusted use of Cloud-based services. A number of key characteristics and requirements were identified, together with an indication of possible regulatory support. These highlight the need for architectural frameworks for trust and security that enable interoperability and the establishment of mutual trust; and the use of virtualisation to maintain separation between entities in an environment where physical boundaries no longer exist. Within the architecture, a measurement infrastructure is needed that facilitates: the monitoring of security status and indicators, the identification and analysis of attacks and intrusions; and the building of insight into merging threats. The continued development of underlying technologies is needed to keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Accountability, that must be respectful of privacy, is seen as vital in ensuring transparency, deterring malicious action, and providing diagnosis of failure. Possibly also typical of other platform/service-related areas, a specific need for automated security policy governance was identified, extending from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to remedial actions for non-compliance.

Further details on the results of the Working Groups will be given in a report expected in the autumn of 2009.

2.7. Infrastructure and Governance

While multiple technical aspects are important for providing trust and security, one must recognise that just the technical nuances of security do not automatically imply a "trustworthy system". A bona fide trustworthy system must also entail quantifiable and auditable technical and organisational aspects of delivery (policies, architectures, Service Level Agreements, etc), as well as the user's perceptions on its operation. When developing infrastructures that address the needs of the stakeholder groups in the digital world we must consider metrics, certification, standardisation, governance and management, and international agreements on interoperability (including process interaction, definitions and meta-level standardisation and technical interoperability), or federation of often incompatible systems and platforms.

Trust requires an infrastructure to build trust relations, using tools to confirm, measure or rate various aspects such as identity, reputation, relationships, risks, or security of the environment. It requires instruments to ensure a certain level of transparency and accountability, dependent on the situation.

[33] http://www.think-trust.eu/general/general/wgs.html

At the basis of trust lies the assessment of claims on the party to be trusted. A basic framework for managing claim verification, including identity, non-repudiation, creditworthiness, reputation etc. is needed to develop federated, open and trustworthy platforms in various application sectors, e.g. health care, government services, public procurement, smart and energy efficient living. Electronic Identity Management (eIdM) systems are available, integrated in services provided by industry or by public administrations. However, interoperability is practically non-existent, nor is sufficient attention given to privacy and minimisation of data exchange. The development of a common framework for federation and interoperability between governmental eIdM systems of different EU Member States is still a matter of study and trial [34]. Banks mostly have their own systems, with no connection to citizen registrations other than via an ID card or passport.

The development of a common European framework for federation and interoperability of governmental eIdM systems that can form the basis of a wide digital claim management framework, compliant with the legal framework for data protection and privacy, can make Europe a global leader. However, it requires urgent joint EU action and the political will of all Member States, as well as cooperation with industry. Europe has the knowledge and expertise to achieve this. Success will boost trustworthy Internet communication and innovation in web services. It will also support accountability in the public space and strengthen control on cyber crime.

2.8. Conclusions

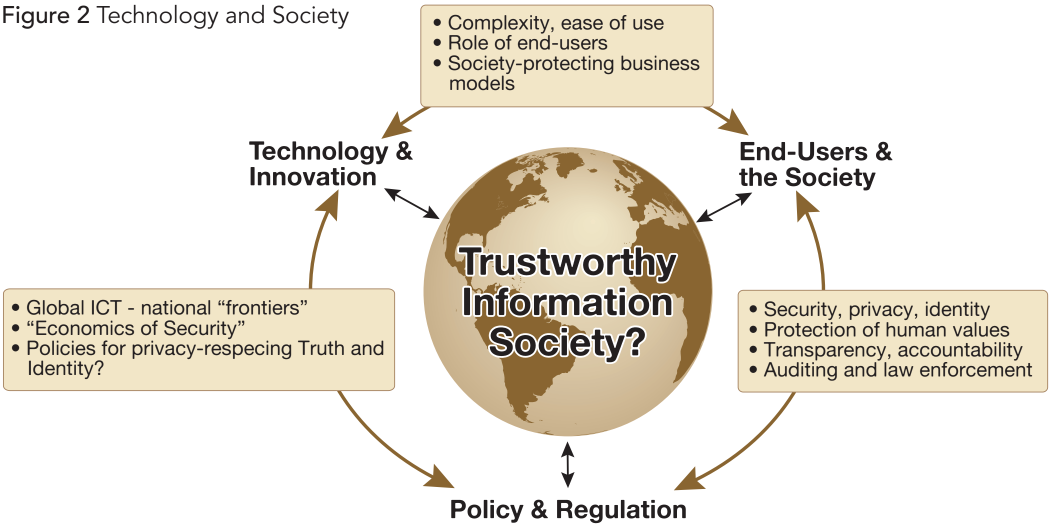
In this chapter we discussed concepts and contexts, perspectives of major stakeholders, and the possibilities as well as the risks for our societies as future digital infrastructure systems are developed.

Europe must protect and exploit its industrial strengths, academic quality of research, and strong societal values and democratic systems in order to lead the development of trustworthy ICT solutions for the Information Society. Public and private stakeholders must come together and develop a coherent strategy; taking account of the interplay between technology development, societal needs and acceptance by citizens, the law, regulation and other public policies.

Policy makers and regulators will be most effective if they base their work on sufficient technological insight and the expectations of business, consumers and public organisations.

It is this interwoven network (Fig. 2), of technology development for trustworthy ICT with the societal context in which it will be applied, that needs strong attention. Without attention to all elements, one cannot expect sustainable progress.

Figure 2 Technology and Society


• Complexity, ease of use
• Role of end-users
• Society-protecting business models
Technology & Innovation
End-Users & the Society
Trustworthy Information Society?
• Global ICT - national "frontiers"
• "Economics of Security"
• Policies for privacy-respecing Truth and Identity?
• Security, privacy, identity
• Protection of human values
• Transparency, accountability
• Auditing and law enforcement
Policy & Regulation

[34] http://www.eid-stork.eu

03 Technology in Societal Context

To place the general discussion and concepts of the former chapters 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. We first discuss two of the problems facing us today as we move increasingly towards a Digital Society. After that we present some story lines on how the future might look.

3.1. The dangers of our digital shadow

Simply for the chance to win a cuddly toy, or some other equally insignificant prize, many people will freely enter their name, home address, date-of-birth and various other personal details onto an Internet website. 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 in an effort to win a teddy bear, 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. Knowledge about data ownership, data access rights and the ability to withdraw and/or delete "their" data is apparently not something that a great many users of the Internet are concerned about.

Data mining, however, and the collation of information on individuals and groups from various sources across the Web is a serious danger to our private life today.

Consider the ease with which the French magazine *Le Tigre* constructed and published a portrait of Marc L.[35], a pseudonym for a randomly selected young man. Using nothing more than information publicly available on the Web and some deductive reasoning, a surprisingly accurate and intimate profile of Marc L. was developed. Upon hearing of *Le Tigre's* experiment, the young man contacted the magazine and requested that the article be removed. However, legal advisors told him that he could not compel *Le Tigre* to delete the piece and that he would not achieve much recompense through the Courts, since all the information used by the magazine was obtained from public sources.

Besides the embarrassment to the person concerned, there are other more grave incentives for following the data trail left by users on the Web. The availability of social and personal details on one website and professional details on another implies that our work colleagues (and prospective new employers) can find out more about us than we might prefer, given the relatively easy means of connecting these two categories. Market researchers and cold-calling salespeople would benefit too from observing the preferences and lifestyle choices revealed on-line by users.

[35] http://www.le-tigre.net/Marc-L.html

There are also more sinister dangers inherent, when data remains lying around, unlegislated for in hyperspace: so much private and public information means that the replication of a user's virtual identity is potentially easy to achieve. This gives rise to numerous fraudulent possibilities for would-be 'identity thieves'.

3.2. The weakest links in the data storage chain

There have been a number of high profile news stories, reporting the loss and theft of data storage devices such as CDs, USB sticks and laptop computers; all of which contained confidential information regarding members of the public.

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, on a portable device, means that the chain of data trust is not being evenly serviced.

By physically moving data via a portable device, as opposed to electronically over a network infrastructure, the exposure to eavesdropping attackers is lessened. However, the integrity of the data can still be potentially compromised – the attacker must now just change his line of attack and physically take charge of the data-carrying device. Even if the data on the lost or stolen device is never used for malicious means, the very fact that it was misplaced at all, makes people feel exposed. The encryption of data during transfer may lessen the potential for the malicious use of same. This also offers some reassurance to those whose data has been lost/stolen. However, this is hardly sufficient.

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.

These two concrete problems – namely our casting of digital shadows and the apparent lack of security when transferring our data – are becoming all the more prevalent as we move towards an on-line, Information Society. These and other similar trust and security issues are plain to see in the following scenarios, which animate the requirement for strong guidance in our Digital Information Age.

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 are committed to a clean planet: "going paperless", for example, sounds like a cool idea to them. Both also 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-to-be-expired ID card today, Theresa leaves their apartment on the way to a nearby lawyer's 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 – 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 (and less x-ray exposure) 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, not surprisingly, 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 (via a web-service) 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 (again via a web-service). 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 web-site. 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 (i.e. personal and potentially identifying data) 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 multi-media 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 granddaughter, 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. "Ah-ha," 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 on-line activity, they could see that:

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

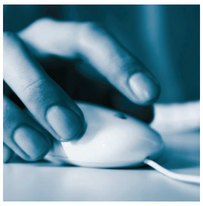
(2) He has ordered a new *ID Card*, which will contain his medical information;

(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 when Theresa does forward her CV. 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;

04 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 discussed stakeholder interests for trust, including security, resilience, data protection and privacy. We discussed the technology issues in relation to societal, economic and legal consequences to demonstrate that real progress towards a trustworthy Information Society can only be achieved by taking account of all perspectives. Indeed, the innovation that provides many opportunities and a wealth of information to citizens is at risk if sufficient attention is not given to its socio-economic embedding and acceptance. We examined the subtle balance in our democratic societies between privacy and personal data protection on the one hand and public interest and legal and contractual obligations on the other. We argued for the potential of ICT to improve security and privacy simultaneously, without the need for a trade-off in a zero-sum game. We gave special attention to the fundamental issue of creating a common framework to enable the federation and interoperability of the various identity management systems in Europe and beyond.

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. Of course we cannot address each and every issue discussed above. 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** given in section 2.6 of this report. 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 desired characteristics of dynamic, adaptive, scalable, autonomic control are attractive in abstraction, though as global-scale systems develop, heterogeneity (in design, resource types, operational policies, etc.) is often, in reality, the attribute that makes systematic end-to-end security a challenge.

This area encompasses virtualisation, the Cloud, and private and semi-private spaces; realised by service-oriented platforms. It requires resilient underlying infrastructures in all environments and conditions and technologies to realise: ecosystems with key attributes of heterogeneity and scalable scope for growth; multi-domain security; managing heterogeneous computing environments and corresponding trust domains.

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 (embedded security by design). It is quickly becoming the most important Critical Infrastructure, demanding strong physical security in balance with privacy. It also requires federated, seamless, transparent and user-friendly security of the edge networks in smart ecosystems, with interoperability throughout the heterogeneous landscape of access networks.

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. It will need: resilient, pervasive, self-organised and opportunistic computing; security in the presence of scarce resources; security of services and content, and of software and data. Many specific aspects need to be considered such as; security policy compliance, security in dynamic aggregation or composition of services, protection of intellectual property and usability.

(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 (e.g. by claims on identity, reputation, recommendation, frequentation, voting). 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.

Privacy infrastructures require the development of protocols, tools to check privacy assurance, and multi-identity systems to maintain privacy. At the hardware level, the privacy of personal, sensitive communicating devices must be advanced. Important issues include unobservability, unlinkability through search engines or social networks while enabling personalised services, usability with diversity and ethics.

The management of identity claims is at the core of providing trust. ID claims provision on a wide scale requires that existing and future identity management systems are interoperable or federated and enable the integration of privacy, accountability, non-repudiation and traceability and the right to oblivion at the design level, in order to provide freedom and protection against cyber crime. Research must focus on technologies and standardisation that facilitates this, as well as removing the barriers to interoperability, allows use of multiple authentication devices which are applicable for a diversity of services, and provides auditing, reporting and access control.

(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.

Under this heading we should also consider enabling technologies, such as declarative languages, biometry, certification and, certainly, cryptography.

(4) Data policy, governance and socio-economic 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. This will include: mutual recognition security frameworks for competing operators; transparent security for re-balancing the unfair, unequal face-to-face relationship of the end-user in front of the network; tools for trust measurement, based on cost-benefit analysis; instruments for early detection of attacks; real-time and large-scale tests for crisis management procedures. And all this must be done with economic viability in mind.

The proposed interdisciplinary research agenda is summarised in the recommendation below. It must include work on a number of paradigms, including social sciences, technical engineering and the socio-technical interface. A detailed report is in preparation by the Think-Trust project, based on the results of the Working Groups, which will be used as input to the discussions for upcoming ICT Work-programmes.

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*. These concepts have always been and still are at the heart of our free societies; this is reflected in the European Charter of Human Rights. They form the basis for our communications, transactions and economic and social behaviour in the private, public and privatised space.

We have seen that societal trust – the level of trust citizens have in other parties and the societal organisation as a whole – is an important condition for economic growth. European society has a relatively high level of social trust. Ensuring the continuation and enhancement of this in digital life is also likely to have a strong beneficial effect on the digital economy.

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.

However, as argued strongly in this report, technology development on its own, without strong regard for the societal context, economically, socially and legally, will lead to the loss of trust and this will be reflected in less economic opportunities and prosperity.

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[36] 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. Many EU Member States are currently in the process of developing their own ID card systems. The STORK[37] project is working towards achieving interoperability (organisational and semantic interoperability, but where possible technical interoperability also). In parallel to this, we see industry sectors (e.g. banking) developing their own IdM systems and within web-based services, there is an emergence of interoperable or federated clusters of systems (e.g. Information Card Foundation[38], Liberty Alliance[39]).

Europe needs a common framework that allows federation and forms of interoperability (organisational interoperability providing business interfaces; semantic interoperability in the form of common definitions and standardisation of data and meta-data, etc.) between all these systems. Formal identification as a citizen of a Member State should be possible throughout the EU, with the State of citizenship being the claim provider. To open a bank account, electronic identification with the "citizen ID token" should be facilitated. Access to health and other public and private services could be enabled throughout the EU with any token that one has obtained for that purpose, anywhere within the EU.

This common framework should encompass a design that guarantees the principles of privacy, minimal data disclosure, proportionality and other general principles laid down in the EU legal framework.

At the same time, we need to ensure reasonable instruments for forensic analysis are available, which will not only provide possibilities for the traceability of illegal behaviour, but also for proving one's innocence (e.g. when a botnet downloads illegal content on a PC of a citizen without their knowledge). The eIdM framework must include regulations and tools for anonymity, accountability, transparency, auditing and law enforcement.

The Commission has proposed the development of European Large Scale Actions, on e-Identity, in its Communication[40]. Members of RISEPTIS have developed a roadmap

[36] http://trustindigitallife.eu/Home%20Page.html

[37] http://www.eid-stork.eu/

[38] http://informationcard.net/

[39] http://www.projectliberty.org/

[40] COM (2009)116: A Strategy for ICT R&D and Innovation in Europe: Raising the Game

which details actions to be taken to achieve a common European framework. This will be presented in a follow-up report on 'RTD and Infrastructures' and will be based on the Think-Trust Working Groups results. The importance of such a framework for the successful development of a trustworthy Information Society can hardly be underestimated and should be given high priority.

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[41], mandatory data breach notification has already been extended. Researchers[42] 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. For the future, one might need to bring in further elements that can strengthen the accountability of data controllers and develop tools to enhance transparency in data processing. The relationship with other policy frameworks must hereby be taken into account; in particular, the relationship with consumer law and liability for products and services that collect and process data (web community services, personalised services, identification devices, reputation systems, etc.), as well as Art 3.3 of Directive 1999/5 [Directive on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, 1999/5/EC, OJ L 91, 7.4.1999, p. 10]. The relationship with COM(2007)228 [Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM(2007)228] on Privacy Enhancing Technologies should also be considered, as well as the international context, applicable law, jurisdictional problems and cross-border data flows (especially in relation to the developing Cloud).

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. It should lead to the creation of an environment of technology-embodied law for a digitised constitutional democracy, stimulating the development of technical tools and instruments to support implementation and acceptance by both industry and citizens. Continuity, usability, trustworthiness and user-centric privacy protection are essential parts of such policy.

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. Its current level of long-established social trust, its scientific and technological capacities and its well-developed industrial and service structures all provide an excellent starting

[41] Proposal for a Regulatory framework for Electronic communication networks and services

[42] Rannenberg, K. Royer, D. and Deuker, *A The Future of Identity in the Information Society*, Springer 2009

point for large forward momentum. However, substantial and coherent European large-scale projects, which take full advantage of these European strengths, need to be targeted. The previously mentioned common framework for electronic identity management is one example that needs strong commitment from all Member States and industrial stakeholders. There are also other instances – for example, European citizens are very active in social networks on the Web and further development of these networks, paying full attention to privacy requirements and interoperability and developing business models that stimulate the creation of services in such networks, would fit well into European culture and expertise.

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. Relevant topics to start with could be: European data processing in the Cloud; a services platform with the EU's legal framework and governance infrastructure; next-generation social networks, taking account of interoperability and privacy; EU-wide, legally accepted electronic documents, usable on different media, including paper. There will also be others, related to innovative services and aiming at broad inclusion of all societal groups in Web activities.

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. For these to be most effective it is necessary to consider the global consequences of the actions taken in Europe. 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.

The world currently comprises (blocs of) nations with their own jurisdictions, and with agreements on the movement of persons and the exchange of data and goods from one nation to the other. For example, international or bilateral agreements exist on the acceptance of passports satisfying certain data formats, goods that are compliant with import/export law, etc. Geopolitical power prevails on the basis of existing frontiers and international law, with this recognition being critical for global stability. The Internet, however, introduces political and business entities that do not adhere to these rules. Electronic (business) transfers can easily go from one country to another without consideration of any change in jurisdiction and often with the consumer being unaware of such activities. Law enforcement in the digital world is hampered by an inability to bring the concerned parties to court. In addition, the information stored on a person's mobile device in one country may be considered illegal if the person is in another country. The spread of the virtual personal space over various geopolitical and judiciary entities leads to problems which are not yet sufficiently thought through.

Introducing geographical and temporal information in digital space may be part of the solution, but international and bilateral agreements between states will be the main tools which will create semantic and organisational interoperability between national policies and infrastructures. It is important in this search for solutions not to break the Internet/Web infrastructure into separately controlled pieces, since this would lessen its role as a global information network, as well as lowering its potential for innovation.

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.