IDIS (2010) 3:397–404
DOI 10.1007/s12394-010-0058-7

Trust and privacy in the future internet—a research perspective

Dirk van Rooy · Jacques Bus

Received: 30 October 2009 / Accepted: 20 April 2010 / Published online: 18 May 2010

Abstract With the proliferation of networked electronic communication came daunting capabilities to collect, process, combine and store data, resulting in hitherto unseen transformational pressure on the concepts of trust, security and privacy as we know them. The Future Internet will bring about a world where real life will integrate physical and digital life. Technology development for data linking and mining, together with unseen data collection, will lead to unwarranted access to personal data, and hence, privacy intrusion. Trust and identity lie at the basis of many human interactions and transactions, and societies have developed legitimate concern for privacy being essential for freedom and creativity. The burgeoning development of the Information Society, particularly during the past fifteen years, transcended the societal readiness to respond to the transformational change evoked by ICT. We have reached the eleventh hour for the preservation of trust and privacy as elements that can be transposed into our digital future. Europe has been at the forefront in recognizing the importance of privacy protection in relation to digital data, witness the advanced European legislation in this domain. The European Commission recognizes that appropriate measures need to combine technology development with legal means, user awareness and tools supporting data controllers to comply with law in an accountable and transparent way, and that empower users with a controlling stake in managing their personal data. Activities are underway at many levels. European RTD programmes play their role in supporting research in trustworthy ICT, privacy enhancing technologies, privacy-by-design in service layers as well as in networks, enabling technologies such as cryptography, and in generalized frameworks for trust and privacy-protective identity management.

The views expressed above are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

D. van Rooy · J. Bus
EU Research programme on Information and Communication Technologies, Brussels, Belgium

D. van Rooy (✉) · J. Bus
DG Information Society and Media, European Commission, Brussels, Belgium
e-mail: dirk.vanrooy@ec.europa.eu

Keywords Trust · Privacy · e-Identity · Research · Technology · Future internet

Introduction—setting the scene

The Future Internet, broadly understood as a conglomerate of networks connected through the Internet Protocol with the Web as an information layer on top, will eventually include an Internet of Things and a Web of Services and will bring us a world with digital life fully integrated into "real" life. From a societal and historic perspective the Future Internet will be the next level of the transformational change that was initiated by the emerging Information Society, which really only started some decades ago, at most.

Trust and identity are concepts that lie at the basis of our existence and have been exercised through physical recognition and face-to-face communication. In a transformation to digital functions, it is vital to understand how the mechanisms of trust and identification can be maintained. Trust effectively facilitates human transactions and economic activities by reducing risks. There is factual evidence of a significant positive correlation between the level of trust in a society and its level of prosperity and economic competitiveness (Fukuyama 1995; Akçomak and ter Weel 2008).

Privacy has emerged in society as a concern to ensure liberty and creativity. The ability to control the release of personal information is a decisive factor for establishing levels of trust in society. Global principles of privacy are reflected in Article 12 of the United Nations Universal Declaration of Human Rights.[1] The EU has implemented a strong comprehensive legal framework on Data Protection and Privacy.[2]

Other elements in building societal trust include accountability and transparency to help ensuring respect of the rule of law and of democratic rights enshrined in law.

The prospect of an all-encompassing Future Internet forces us to consider in depth the consequences of digitizing many aspects of our lives. Massive data collection through social networking, profiling for business purposes, surveillance activities and the like create personal "digital shadows", which remain beyond the control of the affected individual. Management of direct and behavioural personal data will become increasingly difficult when every transaction and interaction is recorded, stored or used for profiling. Storage and processing, including linking and mining of this data, in particular in a future "Cloud", will create uncertainty, undermine trust in the use of eServices and might undermine the overall level of trust, thus threatening the full development of the Information Society.

Solutions must be found in research and technological development with the societal requirements and consequences in mind. Privacy, data protection, security, accountability and transparency must be included in the design of our networks, service architectures and infrastructures. To be effective in a globalised world we must cooperate internationally to ensure interoperability—organisationally, semantically and preferably also technically.

[1] http://www.un.org/en/documents/udhr/

[2] Directives 95/46/EC and 2002/58, respectively.

Privacy has many aspects—it relates to culture, history, morality, the position of individuals in society, public and private security, legislation, economics, technology etc. In many societies it is an important concern underpinning societal values, in particular for sustaining freedom and the ability to exert democratic rights and human self-determination. The concept of privacy is subject to change over time; it is contextual and cultural.

The challenges posed by the emerging digital world need urgent attention. We may currently witness the most massive and concentrated transformational pressure in known human history on the concept of privacy. It is essential therefore to work towards transposing these social characteristics into the digital space.

Legislation and policy, future challenges and technology

The European Union has since many years given focused attention to data and privacy protection, in legislation going back to the 1970s in individual EU Member States, in European-wide directives such as the Data Protection Directive [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*"] and in several policy documents, such as the PETs Communication [COM (2007)228 "*on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*"].[3]

The mentioned PETs Communication states that *"The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitate compliance with data protection rules."* The European Commission in its First Report on the implementation of the Data Protection Directive[4] considers that "*...the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection.*" The development of technology for privacy protection can help avoid data breaches and ensure compliance with protection rules.

The development of technology for information and network security has been going on for many years. Examples of RTD in trustworthy ICT include areas such as cryptography and trusted computing to protect information in storage, transit and processing; security principles for the engineering of networks and systems; methodologies for software assurance; identification and authentication.

Cybersecurity and privacy

Developments in computing capacity and networking during the past decades have led to profound changes in the digital landscape. It has enabled complex computer tasks and image processing, but also cybercrime to become organized and extensively equipped. This has resulted in an "arms race" amongst those developing and deploying protective measures for software and systems on the one hand, and the cyber-criminals trying to break them on the other. Successes in hardening the

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF
[4] http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf

basic layers of the infrastructures, such as operating systems, against attack have led to new attacks directed at weaker, higher level links of the cyber chain, in particular browsers and applications. At the same time patching, quick emergency repairs and insufficient testing give rise to new vulnerabilities in the cyber systems.

Although cybersecurity, eIDM, trust, privacy and data protection are conceptually different, they conflate. The use of purloined identity attributes enables fraud and/or the evasion of law enforcement. Respecting privacy essentially means that parties that are not supposed to access personal information, actually do not get such access. Security breaches are incompatible with the protection of personal information as understood in the corresponding EU legal framework. Effective cybersecurity for electronically stored, transmitted and processed personal information is a necessary but insufficient condition for such compliance. If for example terrorists or cybercriminals are able to assume other identities, not only will that capability enable them to evade detection, but moreover this will likely result in falsely accusing individuals, which might result in forceful measures being taken against innocent persons whose identities were compromised.

Reality is that we cannot design and operate widely used networked information and communication systems from which theft and data breaches will never happen. This translates in a plea for offering people tools for identification with security and presentation of data proportional to the offered service, rather than using full-blown governmental eID cards in every situation. The use of formal governmental eID tokens for simple matters may also be felt as sensitive and emotionally not acceptable. Solutions have emerged from various industry initiatives, such as Open ID cards or Info Cards, which enable flexible user control of ID attributes for many common situations that require some form of identity attributes to be presented. If such tokens are somehow compromised, other ID tokens remain in place and mechanisms to revoke and replace the compromised token can be readily put in place. User-control in personal data management helps minimizing the potential violation of privacy and identity of individuals. But user-control must be facilitated by usable tools, and has to go hand in hand with transparent compliance with data proportionality and minimization rules on the service provider side, with auditable accountability for processing personal data by data collectors and processors, and with adequate rules of law, including their enforcement through reporting, auditing and forensics.

The future internet

The Future Internet, in particular when extended with the Internet of Things, will encompass physical and virtual entities requiring identification. These will operate in smart contexts, sometimes referred to as ambient intelligent environments, in a widely networked world. The introduction of the environment of “things” within the Internet will add a whole new dimension and multiple degrees of complexity to the relationship between the virtual world created with information technology and the physical world, and open up for entire new ways of using and abusing personal data.

Trust and privacy will be prominent themes within many usage scenarios in the Future Internet, and the ability to control our digital assets and the digital footprints

they leave behind will be a key enabler in realizing the potential of the coming digital world. Highly personalized information should only be shared with entities that we have chosen to interact with and only for the purpose and duration of the service we want to access. Nevertheless, our digital footprint will further increase. Technology is moving ahead; cloud computing, service mash-ups and advanced biometrics are further developed. To ensure a trustworthy future society we need to complement these developments with research into "privacy-by-design" in systems and services architectures and platforms. We also need to develop technology tools to support regulation and its enforcement, and assist regulators to understand the emerging technological world.

A major weakness in the Internet is the lack of a well designed and generally usable infrastructure for reliable and privacy respecting authentication of claims, including identity claims, when needed. Much of current Internet crime like spam, viruses, identity theft, phishing and pharming is possible due to anonymity of the perpetrators. Accountability, auditing and non-repudiation are currently developed at application level only.

Another consequence of authentication at application level is over-identification; often based on: provide all information that is asked for or don't get the service, effectively a denial-of-service approach. This could in the worst case lead 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. A trustworthy and privacy respecting identity claim management regime can ensure that the right people get to the right resources in a practicable way.

European research programmes

The rapid pace of change necessitates equally rapid responses to protecting personal information. To this end, many organizations are engaged in research into technological solutions that enable the provisioning of end user services while ensuring privacy protection, security and trust. The objectives of stimulating research related to privacy protection should take into account:

- Principles of privacy-by-design, providing the methods and tools to enable proper attention to privacy and security in the design phase of systems and services;
- Privacy-respecting authentication and claim management, and implementation of accountability and transparency.

The European Commission, in its ICT Programme for research and technology development in the field of Trust and Security, gives significant attention to the area of privacy protection, with projects and actions being funded for more than a decade now.

The European research is organized in so-called Framework Programmes. Major and noteworthy research activities focusing on privacy technology and identity management in the 6th Framework Programme (FP6, 2003–2006)

included FIDIS,[5] PRIME[6] and ECRYPT,[7] which were large-scale initiatives on identity management, privacy and cryptography, respectively. Those activities have put Europe on the global map as a place for high quality research in their respective areas. Other FP6 research in ICT trust technologies targeted areas such as multimodal and secure biometrics; electronic authentication; secure digital assets management; virtualization of security resources for advanced and seamless security.

Currently we are in FP7 (2007–20013), and specific privacy related research objectives in the current **ICT Work-programme 2009–2010**[8] in trustworthy ICT include:

- *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;
- *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. 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.

A number of projects have been started for more than a year (TAS3, PRIMELIFE, MASTER, TURBINE). More information about these and other activities funded by the European Commission can be found at http://cordis.europa.eu/fp7/ict/security/.

The road ahead

The vision of RISEPTIS

Other bodies and initiatives have also been advocating technological solutions in the area of trustworthy ICT. As it appears from the above, important RTD results have already been achieved in this area, but the rapidly developing digital world requires further consideration. The RISEPTIS board, short for "*Research and Innovation in Security, Privacy and Trustworthiness in the Information Society*", is an advisory board composed of high-level European research and industry experts, supported by the EC-funded action Think Trust.[9] In its report of October 2009 it emphasises the necessity for technology development to be connected strongly to the development

[5] http://www.fidis.net/
[6] https://www.prime-project.eu/
[7] http://www.ecrypt.eu.org/
[8] for the full text see: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10_en.pdf
[9] http://www.think-trust.eu/

of law and regulations and to research in societal acceptance and economic viability. RISEPTIS formulates in its report[10] six recommendations addressing:

RISEPTIS formulates a number of recommendations addressing the need for interdisciplinary research, technology development and deployment related to and security needs in the Information Society. In particular, it identifies a need for:

- Trust, privacy and identity management frameworks, including issues of meta-level standards as the first priority;
- Concrete initiatives that bring together technology, policy, legal and social-economic actors for the development of a trustworthy Information Society;
- Development of a common EU framework for identity and authentication management;
- Further development of the EU data protection and privacy legal frameworks as part of an overall consistent ecosystem of law and technology;
- Development of large-scale actions to build a trustworthy Information Society;
- Addressing the global dimension and foster engagement in international discussions.

These recommendations constitute important input to the planning of the ICT Trust and Security research agenda for the FP7 programme period 2011–2013 and beyond, as well as to related policy planning of the Commission.

A common European framework for user-centric e-Identity management

The Communication "*A Strategy for ICT R&D and Innovation in Europe: Raising the Game*",[11] adopted on March 13, 2009, proposes to support a set of large scale projects cutting across the research, innovation and deployment cycle for establishing modern pan-European service infrastructures. One of the candidate examples given is an electronic identity management infrastructure (eIDM), which would be in line with the above RISEPTIS recommendation.

The work in above mentioned EC funded RTD projects is very relevant to such an activity, as is the large trial project STORK.[12]

Currently the development of such a European Large Scale Action is in a reflection phase and possible modalities are the subject of debate at different levels of policy-shaping. Its provisional objectives are to ensure interoperability for trustworthy authentication across service domains of Member State public authorities, businesses and citizens. It should allow EU-wide trustworthy service provisioning in domains such as e-government, e-health, e-commerce, finances and social networks, and hence should support the provisioning of multiple identity instances from government-accredited to commercially accepted, ranging from strong identification to anonymity..

[10] http://www.think-trust.eu/riseptis.html
[11] [COM(2009)116], see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0116:FIN:EN:PDF
[12] http://www.eid-stork.eu/

Conclusions

With the advent of networked electronic communications and the accompanying immense capability to collect, transfer, combine and store data, enormous transformational pressures challenge the concept of privacy as we know it. Technology development needs to provide innovative architectures, systems, and services, security instruments and infrastructures for the effective implementation and enforcement of law, supporting privacy-by-design, aiming at user control, prevention, protection and recovery, and providing auditing and assurance. This has to go together with a well-conceived legal environment that allows an effective rule-of-law. And above all, appropriate procedures and organisation need to be installed, technology needs to be user-friendly and people need to be aware and adapted to life in the digital age.

Unless user-control and privacy concerns are taken into account early in the design process—i.e. privacy-by-design—, there is significant risk that we will end up with a very effective distributed surveillance system, a dream come true for the metaphorical big brothers, electronic stalkers and cybercriminals. User-control and personal data protection have to be part of the design of the underlying infrastructure, the e-services that run on top of it, and the governance and management structure to run it. In conceiving, designing and building a common European eIDM framework for the Future Internet, for digital life and economy, the challenge is to take the world from where it stands today—a mix of systems in a spectrum of global and mostly non-federated application dependent e-Identification systems—to European-wide or even global federated eIDM systems that provide user-centric and privacy protective identity management, and ultimately high trustworthiness.

References

Akçomak IS, ter Weel Bas. Social capital, innovation and growth: Evidence from Europe. Eur Econ Rev, Elsevier. 2008;53(5):544–67. http://ideas.repec.org/p/iza/izadps/dp3341.html.

Fukuyama F. Trust: social virtues and the creation of prosperity. NY: Free; 1995.