WORKSHOP ON
"PRIVACY PROTECTION AND ICT:
RESEARCH IDEAS"

WORKSHOP REPORT

21st September 2011 - BRUSSELS
# TABLE OF CONTENTS

1. INTRODUCTION ................................................................................................................... 3  
2. SCOPE, MOTIVATION AND GOALS .................................................................................... 3  
3. AGENDA ............................................................................................................................. 4  
4. PRIVACY AND ICT: RESEARCH IDEAS ............................................................................ 5  
   4.1 Lifecycle management of users – the weakest link? .................................................... 6  
   4.2 Geo-privacy: Geo-location and privacy ................................................................. 7  
   4.3 Privacy and ID management in context aware (including commercial) environments ............................................................................................................................... 7  
   4.4 Privacy and Social Networks ....................................................................................... 7  
   4.5 Alternative economic models based on social concerns ....................................... 8  
   4.6 EU research approach for privacy – should we follow the AIRBUS model? ............. 9  
   4.7 Privacy and Innovation ............................................................................................... 10  
   4.8 Privacy and BIG Data! ............................................................................................... 10  
   4.9 Privacy and security in mobile environments using biometrics ......................... 11  
   4.10 Privacy by Design – the silver bullet? .................................................................... 11  
   4.11 Privacy on centralised vs. de-centralised systems ............................................... 13  
   4.12 Policy driven approaches for Privacy ..................................................................... 14  
   4.13 Legislation and Regulatory approaches .................................................................. 16  
   4.14 Addressing the conflicts with Privacy ................................................................... 18  
   4.15 Privacy and Trust ..................................................................................................... 19  
   4.16 Counter-profiling ..................................................................................................... 19  
5. SUMMARY ......................................................................................................................... 20  

ANNEX 1. ATTENDANCE LIST .................................................................................................. 22
1. INTRODUCTION
The Unit F5, ICT Trust and Security research, of DG INFSO organised a workshop held on 21 September 2011 in Brussels. The aim of the workshop was to have an open discussion and exchange of ideas on the challenges and research ideas relevant to the thematic field of "Privacy Protection and ICT".

The workshop highlighted many future research topics and the discussions enabled further elaboration on these topics and this is included in the report.

2. SCOPE, MOTIVATION AND GOALS
Jesús Villasante, European Commission Head of Unit of F5, ICT Trust and Security research, of DG INFSO welcomed all the participants and set the scene and highlighted the objectives of the meeting, which are to discuss important research ideas within the areas of privacy protection and ICT for the short, medium and long term.

These types of workshops will lead to the fulfilment of the goal of the unit to have excellent research projects producing scientific results and to have a more influential trust and security community in the EU and beyond. It is also essential that our results should support a competitive industry in this area, not only on trust and security areas but also ICT industries at large. It is crucial that the industry is conscious of the need to implement privacy measures; otherwise, they will lose the trust of their customers and their competitiveness.

The workshop was designed to include a mixture of presentations, questions and answer periods with an emphasis on interactive discussions where the participants could participate openly while exchanging their views on the necessary research topics related to privacy protection and ICT and the technologies necessary to solve the many issues on data protection and privacy.

The workshop results would be used for the following purposes: providing inputs toward the future programs, which would undoubtedly have an element on trustworthy ICT including Horizon 2020, for which the European Commission will make a proposition before the end of this year to the Parliament including inputs from this workshop.

The workshop was divided into 4 sections, each with a dedicated chair. These included

- Usability and socioeconomic aspects of privacy
- Technology for privacy in the Future Internet (in the cloud, in the mobile systems, in the Internet of Things, etc.)
- Policy for preserving privacy in the information society
- Security, privacy by design, trust and accountability

A wrap up took place at the end of the workshop.
3. AGENDA

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:30</td>
<td>Welcome and introduction</td>
</tr>
<tr>
<td></td>
<td>Jesús Villasante, European Commission</td>
</tr>
<tr>
<td>10:00</td>
<td>Usability and socioeconomic aspects of privacy</td>
</tr>
<tr>
<td></td>
<td>Johan Van Hove, Sebastian Gambs, Andreas Albers, Jean-Marc Dinant,</td>
</tr>
<tr>
<td></td>
<td>Evangelos Markatos (Chair)</td>
</tr>
<tr>
<td>10:40</td>
<td>Questions &amp; Answers</td>
</tr>
<tr>
<td>11:05</td>
<td>Coffee break</td>
</tr>
<tr>
<td>11:20</td>
<td>Technology for privacy in the Future Internet (in the cloud, in the mobile systems, in the</td>
</tr>
<tr>
<td></td>
<td>Internet of Things, etc.)</td>
</tr>
<tr>
<td></td>
<td>Mika Lauhde, Rigo Wenning, Dimosthenis Ioannidis,</td>
</tr>
<tr>
<td></td>
<td>Claudia Diaz (Chair)</td>
</tr>
<tr>
<td>12:00</td>
<td>Questions &amp; Answers</td>
</tr>
<tr>
<td>12:30</td>
<td>Lunch break</td>
</tr>
<tr>
<td>13:30</td>
<td>Policy for preserving privacy in the information society</td>
</tr>
<tr>
<td></td>
<td>Mike Osborne, Luis Velasco, Alan Hartman,</td>
</tr>
<tr>
<td></td>
<td>Svein Johan Knapskog (Chair)</td>
</tr>
<tr>
<td>14:10</td>
<td>Questions &amp; Answers</td>
</tr>
<tr>
<td>14:35</td>
<td>Coffee break</td>
</tr>
<tr>
<td>14:50</td>
<td>Security, privacy by design, trust and accountability</td>
</tr>
<tr>
<td></td>
<td>Demosthenes Ikonomou, Demitrius Klitou, Mireille Hildebrandt,</td>
</tr>
<tr>
<td></td>
<td>Dario Avallone, Yos Samuel Martin,</td>
</tr>
<tr>
<td></td>
<td>Michael Waidner (Chair)</td>
</tr>
<tr>
<td>15:43</td>
<td>Question and Answers</td>
</tr>
<tr>
<td>16:05</td>
<td>Wrap-up</td>
</tr>
<tr>
<td></td>
<td>Jim Clarke</td>
</tr>
<tr>
<td>16:20 – 16:30</td>
<td>Closing by European Commission</td>
</tr>
</tbody>
</table>
4. PRIVACY AND ICT: RESEARCH IDEAS

The workshop was supported by the following presentations made by researchers engaged in Privacy protection and ICT research.

Session 1. Usability and socioeconomic aspects of privacy
- Johan Van Hove, CA Technologies: “Human Behaviour and IT Security no longer needs to be in conflict”
- Sebastian Gambs, University of Rennes: “Show me how you move and I will tell you who you are: Geolocation and privacy”
- Andreas Albers, Goethe University: “Privacy and ID management in context-rich Personal Data Ecosystems”
- Jean-Marc Dinant, University of Namur: “Searching for a privacy Ontology”
- Evangelos Markatos (Chair), FORTH: “Privacy and Social Networks”

Session 2. Technology for privacy in the Future Internet (in the cloud, in the mobile systems, in the Internet of Things, etc.)
- Mika Lauhde, Nokia: “Cyber security and privacy protection, EU in global playfield”
- Rigo Wenning, W3C: “Privacy and BIG Data!”
- Dimosthenis Ioannidis, Informatics and Telematics Institute / Centre for Research and Technology: “Privacy and Security in Mobile Environments”
- Claudia Diaz (Chair), COSIC, KU Leuven: “ICT developments and privacy protection”

Session 3. Policy for preserving privacy in the information society
- Mike Osborne, IBM Zurich: “Policy for preserving privacy in the information society”
- Luis Velasco, European Data Protection Supervisor (EDPS): “Challenges for ICT within the review of Data protection directive”
- Alan Hartman, IBM Haifa: “Users, Providers, spies and governments: Privacy - an ongoing conflict”
- Svein Johan Knapskog (Chair), Centre for Quantifiable Quality of Service in Communication Systems, Norwegian University of Science and Technology (NTNU): “Policy for preserving privacy in the information society”

Session 4. Security, privacy by design, trust and accountability
- Demosthenes Ikonomou, European Network and Information Security Agency (ENISA): “Future research ideas related to privacy and trust”
- Demitrius Kliou, Leiden University: “Research for Privacy protection and ICT”
- Mireille Hildebrandt, Institute for Computer and Information Sciences (ICIS), Radboud University Nijmegen: “Getting out of the filter bubble: Transparency by design”
- Dario Avallone, Engineering: “Research ideas for Privacy protection and ICT”
- Yos Samuel Martín, Universidad Politécnica de Madrid: “Beyond-Privacy and Identity Spam: What others say about us”
- Michael Waidner, Fraunhofer (Chair): “Research topics for Privacy and ICT”.
Based on the presentations given and lively discussions at the end of each session, a significant number of research items for Privacy protection and ICT were elaborated by the participants. These are summarised here.

4.1 Lifecycle management of users – the weakest link?

Research is needed on how to protect applications and information with a layered approach where each individual transaction of the user is monitored across the key metrics user, device and data. For this, there is a necessity to have a content aware lifecycle management system of users under full control and the provision of access control – how to access and monitor access.

Privacy challenges are usually seen in one direction only. A person’s privacy is adjudged to be attacked from the outside, whereas, in reality, over 80% of the successful attacks are linked to human errors in the receiver organisation / personal behaviour. Therefore, whatever technologies are deployed, individuals are often at the source of providing information themselves. This happens because users usually don’t understand the impact of them providing information and they are solicited to provide information and then are not aware that this is very often an “attack”. This leads to three key challenges on privacy and ICT:

1. Education – we need to show rather than say it is dangerous. Even after an attack, users often don’t understand how it happened. There is a need for online simulation/ visualisation environments that can be operated by citizens – moving from simulation to visualisation of an attack / a threat.

2. Privacy in the context of cyber-security – needs to be addressed across all dimensions including networks, mobile devices, “intelligent” devices. Increasingly, cyber-space is using personal information often without the user knowing or being involved. An example is localisation services. We need to develop processes and methodologies to actively involve the user in privacy. This must require the user giving permission to a requesting service based on the “need to know” and an increased transparency of usage of privacy (move from an initial agreement to sign to dynamic management of privacy) that supports fine-grained “circles of privacy”.

3. Privacy certification - From previous processes, introduce certification of service providers linked to privacy management providing multi-level “privacy” certification process and enabling users to select service providers based on the level of certification.

There is a need for research in user oriented approaches for the privacy technologies. In human communications, there is a distinction between “giving off” information and “giving” information. An example of “giving off” information is that you are a man or woman and there is a need for theoretical research to understand the mechanisms that are able to understand normal human controls in the new environments in order to make the online life the same or similar to real life.

In summary, there are many challenges in privacy and ICT but technology overlooks that the “weak link” is often a human being. As researchers, we need to develop supporting tools and approaches to create personalised education on privacy, involve the users in managing his/her privacy across the entire cyber-space, through dynamic approaches and introduce certification based on levels of privacy.
4.2 Geo-privacy: Geo-location and privacy

Geo-location associates a geographic location to an object such as a cell phone, a computer or a Global Positioning System (GPS)-equipped vehicle. Geo-privacy seeks to protect the location data of individuals and prevent any unauthorised entity from learning the past, current and future location of an individual. Research needs to be undertaken on what it means to have good preservation of privacy in a geo-located context.

Future challenges of research include the sovereignty of geo-located data enabling the individual to keep control of their data. Another research challenge is defining metrics of privacy for geo-located data.

4.3 Privacy and ID management in context aware (including commercial) environments

To date, the privacy research has been done without commercial industries on board. In order to be successful, there is a need to understand how privacy measures will impact the industry. Otherwise, the new privacy mechanisms will be developed in isolation and the advertising (or other commercial) industries will adjust their offerings around it. It is also important to establish methods for trustworthy personal data exchange between users and the industry if the user wants to give their data for some benefit. It is necessary to carry out an evaluation all of our research findings in an online advertising ecosystem as they would be the best area.

A summary of main research ideas include: make personal data flows more comprehensive for individuals; provide means and motivation for individuals to protect their privacy in this new evolving personal data ecosystem; and carry out research in cooperation with online businesses.

4.4 Privacy and Social Networks

Research on privacy should focus on the changing nature of social networks, as opposed to the original structure of social networks. Social networks used to be the place to socialise with friends. Nowadays, it has been redefined as the single sign-on authority on the Internet in which they now authenticate you on other web sites have, thus, become personalisation and location based services on the Internet mobile world.

What do we mean by single sign on in social networks? In other words, you can now log in to access social networking based sites via other sites (e.g. major online newspapers) to see what your friends are interested in or saying about these news items. However, the trade-off is not clear here as to whether the benefits are worth what you are doing and what the consequences are. It is not clear why you need to need to give out all this information and they sometimes end up sending unwanted mails, access your data, post on your wall, find out who your friends are, and other intrusive actions.

There are social plug-ins now such as ‘Like’ buttons are all over the place now. Web sites are using these social plug-ins as a growing trend. In 2010, 6% of web sites used these. In summer 2011, this grew to 20% of the most popular web sites use social plug-ins meaning there is no anonymous browser anymore. Web sites that use social plug-ins give me a personalised version of their site e.g. telling me what my friends say about the
news. At the same time, the social network gives out all the information to the sites that you are visiting. When talking about privacy and mobile social networks - is it OK for my friends to know where I am, even if it isn’t really my friend if their account is compromised?

Within social networks, there are considerable problems faced by users when others release information about them, which could include any number of variables including from leakage of original information to fabrication of bogus profiles. There are numerous motivations for this breach in privacy including careless sharing, gossip, libel, friends vs. enemy, etc.

Another problem is being caused by Identity Spam, where there is identity-related information in the social Web linking digital identifiers to real-world people and it is difficult to distinguish fake from original. This information is easy to create and can lead to a viral distribution (even push mode) and it is difficult to stop (Kournikova effect) and nearly impossible to erase (Right to Oblivion?). Moreover, social connections make spam more credible as we generally trust friends and it is difficult to control what a user says about others especially on federated, yet independent domains.

Research need to be carried out to better understand these new types of interactions within social networks have with privacy - how are they being launched? What is their impact? How do we stop it? And can we roll back and help users gain control of their data and protect them.

4.5 Alternative economic models based on social concerns

There is an enormous gap in the economics models of privacy. What is the cost and benefit of privacy? We need to figure out the current and future values of data.

There is insufficient or very little economic incentives for using Privacy Enhancing Technologies (PETs) and transparency enhancing technologies (TETs). In fact, it is the other way around whereby market forces favour the exploitation of personal information. Therefore, what is needed is to explain the benefits of privacy to individuals and organisations.

Research should be undertaken on how to enhance privacy by looking at alternative economical models where the internet is paid via permission based marketing or economic global compensation. We need to determine the economic value of privacy and how to gain money by respecting privacy.

From a social perspective, the education of the citizens on privacy is very important on accentuating the effect of privacy on netizens, marketers and web masters. Some research could be carried out on the social acceptance of the snoggle model (to sniff facts in between something). For example, would people be interested in a free taxi driver from the airport, in return for allowing them to search your luggage while driving you. Examination as to whether this is true social acceptance should be undertaken. In future research, we should evaluate the social effects of PETs. Are they being used? If not, why not? If yes, by who? Research needs to be carried out on the quantification of web bugs and interoperability of social networks/data portability.
4.6 EU research approach for privacy – should we follow the AIRBUS model?

During the presentations, there was mention of the EU research community taking an “Airbus approach”, whereby the EU should invest in their own industry taking into account the EU’s internal barriers and working specifically on proposals related to the research privacy agenda of the EU. With this approach, future privacy research would focus on our European assets and address the privacy legislation margins in order to reap the innovation rewards without compromising the citizen’s rights to privacy. Research should undertake to study the weakest link in terms of privacy, which is the tendency to trade what we have for other perceived benefits.

There were some concerns about this approach when trying to determine how an approach for a large company / infrastructure could be mapped with smaller IT companies / infrastructures that could even be one person shops. The difficulty presented to us in Europe is that the EU is a grid of countries and privacy would be a subset of a layer. When you look through this grid, everything is different across Europe and it is very difficult to harmonise and manoeuvre through the layers and grid to address the real issues on privacy and data protection. The question becomes how can we reform the situation in a way to empower our own industry? What kind of research should be funded? It should be a mixture of functional research, application research, and architectural research. However, from day one, they should be privacy compliant. It sounds like a dream but how can we do it in reality? We need to make sure there is allocated budget to carry this out.

As part of this “Airbus approach”, should we investigate a privacy compliant EU browser and carry out research on the interoperability of social networks and examine potential roles of ISP’s as an ‘informediary’ to protect the privacy of the individual from the network. Some dangers were pointed out about taking this approach - If we look at the current use of social networking plug-ins and try to bring EU solutions to it. This could be a mistake as we cannot influence other world power’s business policy and market. If our services are so unusable and hard to use, everyone will just start using the US based ones like Facebook. Therefore, should we tend not to discriminate between US and EU policy and market as we will have to look for international solutions.

As a counterpoint, it was argued that if you manage to get a system running in EU that is privacy compliant, it will run in the entire world. For example, the Primelife project produced real privacy related engines that generated a lot of interest in the US markets. Therefore, significant emphasis on the EU approach and research funding should be made to these innovations that are EU based to get them up and running and they will be bought up by other countries. The culture of research and the culture of innovation is different and it is based on the cultural norms of the countries. For example, students in the US seem to have a more view on how innovations can make money whereas the EU students don’t seem to have that perspective. People from around the world value the Framework programmes of research but the administrative overhead and reporting is hurting everyone. A suggestion was made that there could be a situation where people with experience are shepherding others e.g. European Technology Platforms (ETPs)/ Future Internet – Public Private Partnerships (FI-PPP) and the further use of like-minded clusters should be supported.

Although no consensus was reached on this topic, a number of participants expressed an opinion that an Airbus approach is probably not a good example for Internet based...
companies as it is a long term solution. They felt if you tried this in an Internet based company, they more than likely would not survive. However, even if it is not the correct model for the research community, we should explore the idea as to whether it is more productive to have smaller projects fragmented or to have a more ambitious program with the strong support of industry. Since the nature of the problems addressed in the area of Privacy & Trust are addressing many different fields of expertise, the point was made a number of times there is a need for projects with multi-disciplinary skills. In this context, it appears that longer term projects (e.g. IPs) are probably better suited to address such challenges. It was recognised that other regions may develop at certain moments with different flavours. With this in mind, we should consider a joint message conveyed to the decision makers by large industry players (e.g. equipment vendors, network operators, service providers, regulators, …) regarding the need of support for this long term multi-disciplinary approach.

4.7 Privacy and Innovation

We need to focus more on why Privacy Enhancing Technologies (PETs) are not achieving so well. It is necessary to make a more level playing field in which there is a focus on privacy compliance and not legislative compliance, and then the EU players can be more motivated and innovative. If you can change the incentive structure in the EU, you may get innovation that is natively privacy compliant.

As mentioned during the presentations, privacy also has a political element – people need security and privacy urgently. If we could provide technologies that will aid the citizens with their privacy aspects, this would create innovation. There is also a strong possibility of spreading democracy and protecting the citizens from their governmental regimes with these technologies. Policy and regulatory issues would be addressed in a cybersecurity strategy. Member states would have to address a binding level. The concept could have a value but must be structured well.

The EU should create a more supportive environment for innovative small companies. An issue in the EU is the difficulty in taking products to market in the current environment. Research projects have given good results but they are so large and they move very slow like mammoths. Within all research and technological development projects, there is a Work Package (WPs) called Dissemination and exploitation but these are not taken serious enough. In order to have more success in these WPs, you need venture capitalists involved in the projects. This brings difficulties as venture capitalists (VCs) generally wouldn’t get involved as their culture is different and funding high risk projects over the long term isn’t their preference. Regarding the size and duration of projects, from research to product development, it is usually 10 years time frame for any type of development in a multi-disciplinary project. What we need is a patient funding mechanism so you can have an innovation process going for as long as it takes to have a working product. If possible, the culture of research funding should move in this direction.

4.8 Privacy and BIG Data!

It is very clear that in the future internet, the scale of the amount of data on the web will be greatly increased. Furthermore, we will have technology that will enable the correlation of data from much larger sources. With semantic data, we can integrate semantically augmented linked data to integrate huge amounts of data where the data can be more easily correlated. This is what we call BIG Data. If you throw into this mix
the injection of false data and other forms of data manipulation, this will increase the need to look at the sources of the data. Industry and research have already come to W3C and said we need to know the source of the information as the trust in data needs provenance (known origin of source). But at the same time, provenance collides with privacy. How do we solve this conflict? Technology must play a role in the resolution of this conflict. We have to think ahead to solve the issues of big data and how to deal with it.

Future research needs to look at the reason for data protection limitations and the difficulty in handling real big data. Social networking and advertisements create even larger social graphs generating advantages and more power in the correlation of data.

Future research ideas include the exploration of data and usage control in big data, explore how to remedy the conflict between the trust and privacy needs in big data and integrate data usage control into provenance. We need to develop standards for unsharpness for big data and how to make data unsharp for local usage and research the societal the impact of entropy on society and ourselves and find a path between unsharpness and usefulness of data or correlations.

4.9 Privacy and security in mobile environments using biometrics

Privacy and security in mobile environments could be enhanced with research in biometrics in order to alleviate users fears of having the personal (including biometric) data unsecurely exposed to potential intruders. Two examples of research ideas were given:

1. Design and development of a novel, soft biometric driven multimodal cryptographic framework, whereby the traits are captured by the sensor network in an unobtrusive manner. This would introduce the concept of renewable and revocable “biometric keys” derived from multimodal soft biometric traits, without requesting the users to remember or carry any secret password.

2. Design and development of a secure m-commerce system using biometrics. This would need to address the shortcomings of mobile payments and transactions with the use of biometrics. It would address the lack of a reference biometric-enabled middleware implementation to support high security in mobile transactions (with or without near field communications (NFC)-based systems). It is essential that business to business (B2B) and business to consumer (B2C) transactions on the wireless domain need to be as secure as possible. Security enhancements of mobile platforms, embedded devices and privacy enabling technologies by the incorporation of emerging biometric-enabled frameworks for both high secure transactions and increased end-user data privacy, could help to address these shortcomings. The research idea would involve the development of secure online mobile payments and other m-commerce services using biometrics by delivering a cross-platform multimodal biometric Reference Implementation framework (BioMobile application programming interface (API)). It would be the first time research is carried out on the use of mobile-embedded devices (e.g. accelerometer for gait, camera for palm vein, etc.) for extracting discriminative features for reliable user authentication in order to introduce context-aware mobile biometric solutions.

4.10 Privacy by Design (PbD) – the silver bullet?
There are standards and legal requirements with regards to security and audit mechanisms thereof, but privacy is generally left out and ignored by manufacturers during the design and development stages of ICT products/services. The legal framework does not sufficiently and effectively regulate manufacturers when it comes to protecting privacy. There are increasing calls for this to change. While there is currently a legal basis for PbD, the technical emphasis, at present, found both in law and industry standards, is all too often focused on data security alone. The difficulty of keeping up with technology has caused doubt over the ability of lawmakers/policy makers to do something concrete to ensure privacy. This is where PbD comes in.

PbD provides practical measures in the form of technological and design solutions aimed at bolstering privacy/data protection law, better ensuring or even almost guaranteeing its compliance, and minimising the privacy intrusive capabilities of the technology concerned. Technological-based solutions and architectures are critical for minimising the threat to privacy. Experts and policy makers generally agree that PbD is a vital approach for improving the trust of consumers/citizens. PbD is especially critical for protecting privacy in a world of increasing cross-border data flows, for example, as a result of cloud computing and online social networking. This problem is especially accentuated, since different legal jurisdictions have different degrees of adequacy in data protection rules. PbD can better ensure the protection of personal data, regardless of geographic location, technology or legal jurisdiction concerned or the adequacy of the legal framework.

Privacy by Design is receiving support by data protection policy makers (e.g. Federal Trade Commission (FTC), European Commission Communication on ‘A comprehensive strategy on data protection in the European Union’). PbD advocates privacy taken into account from the systems development stage; however, it is not clear how this can be translated into network design. However, we also need to accept the existence of a plethora legacy networks (3G, 4G, WiFi, GPRS, etc.). The new technological landscape provides with computing power that opens advantages to do things in a new way that is not mimicking the physical world. For future research on privacy and data protection, we should focus on technology rather than processes and organisational measures and make sure we do not ignore the (good and bad) properties of digital systems when digitising services.

Privacy by design methodologies are heavily one sided in the balance between the legitimate right to privacy and the protection of society. When balancing Privacy by Design with safety of the users, while it is necessary to catch the criminals, it is very dangerous to use this argument that could result in a situation where back doors could be built for obtaining data. This could result in a situation that fosters additional surveillance, which is the incorrect direction. If you put surveillance in place, it may not work on the smarter criminals and you could end up with a never ending cycle of more surveillance and the innocent suffering. It is a difficult research issue but if you design privacy tools too well, there could be some abusive behaviour. There has to be a separation of Privacy by design and abusive privacy. This is a difficult research area that needs to be addressed by the PbD community in a coordinated way.

There is a need for better coordination of activities related to PbD as there are currently no established best practices/standards on the way privacy protection can and should be built into ICT, nor any established policy options on implementing PbD. The necessary coordination among researchers, engineers, designers, manufacturers/industry players,
and legal/social/privacy experts and privacy advocates is needed. Their efforts are often too fragmented. Coordination is needed to bring together the various actors involved and to coordinate and integrate their activities and research, in order to collectively determine and agree on how to move forward, and clarify what is needed, where, when, how, why and from whom (in terms of PbD). The potential impact could be increased societal acceptance and confidence in advanced ICTs, greater development, deployment and take-up of the latest technologies; Enhanced protection of privacy/personal data; and necessary action at the political level- i.e. amendments to the Data Protection Directive (incorporating PbD provisions) or the adoption of comprehensive PbD legislation.

What is interesting about Privacy by Design (or Default) is that it is NOT about a technical solution for a social problem, it is NOT paternalism BUT it is going beyond naïve voluntarism giving people the opportunity to opt out or opt in based on informed consent. It is enabling awareness of the implications of technical defaults and anticipating the consequences at the design stage involving the public and the legislator. It will have implications for Identity Management systems (IDM), cryptography, data minimization and credentials.

Most PETs focus on consent for access/capture of personal data and few focus on the right to check, delete and correct personal data. There is a need to focus on consent for processing AFTER capture: for sale, for change of purpose, for anonymisation, for data mining. But, in the light of the “Filter Bubble” (Pariser 2011), this does not make a real difference: what does consent mean if you don’t know what profiles your data will match? This is a core research question.

Before we get to Privacy by Design, it was asserted that we need Transparency by Design (TbD) (by default also!). This is a novel challenge and you need lawyers & computer scientists & designers to develop TbD/TETs to discover what profile or patterns you match. There are two ways to do this in future research:

Type I: In the EU Directive, you already have the right to Information about or Access to the ‘logic of processing’ (art. 12 D 95/46/EC); and

Type II: Another important research issue is Counterprofiling the environment to anticipate the consequences of sharing or leaking your data. In other words, users themselves have their own data mining technology to monitor what the environment is doing with your data.

There was a suggestion that research should be undertaken on the development of practical approaches to Privacy by Design. We need to be able to put theory into practice in shorter time periods than the typical duration of 10 years. There are wonderful technologies already in place that could be utilised (e.g. portable identities, data minimisation techniques, crypto advances) and examples of simple things should be considered e.g. mandatory expiration dates for social networks data that could be mandated in Europe that would put pressure on implementing these applications.

4.11 Privacy on centralised vs. de-centralised systems

More research is needed on advanced privacy technologies – including crypto techniques – for both centralised and de-centralised systems. If we are going to have
centralised systems, data can be centralised but in a protected (encrypted) form that still allows limited processing. We should also research in how data can be stored and processed locally e.g. road pricing ensuring integrity properties of the system. There are opportunities with anonymous authentication (credentials) using advanced cryptographic protocols. It is very important that anonymity is possible in the lower layers of the communications stack. We also need to need to consider traffic analysis threats and carry out research on mobile devices/location privacy.

4.12 Policy driven approaches for Privacy

The setting is that our planet is getting more instrumented, interconnected and intelligent and as researchers, we have an opportunity to think and act in new ways - economically, socially and technically.

When we look at the intermixing of instrumentation and privacy policy where there are sensors across entire ecosystems that are pervasive and location aware, there are a number of challenges to address in terms of privacy and security. First and foremost, in this scenario, the ultra low cost models wins market share and they generally are characterised by fulfilling no privacy or security. In addition, the multiplicity of small intelligent devices distributes even more information. Therefore, the technology has to become power efficient with a small footprint consisting of crypto algorithms that are computationally efficient, privacy protocols that have efficient bandwidth and latency. The necessary goal is to balance requirements on Performance/Security/Privacy/Cost with the advent of appliance like sensors that require a minimum configuration with a centralised policy definition sensor gateway utilising a policy distribution model and sensor adaptation as required. In order to accomplish this, future research is required in the development of policy engines and policy enforcement models.

For interconnectivity and privacy policy, in which there is a significant amount of information usage, exchange and dissemination characterised with the potential of data linkage and control, the main challenges are controlling the flow of data across interconnected systems and preventing linkages of data from multiple sources and potential identity reconstruction. There is considerable complexity involved in that user privacy policy is still too complex for users leaving the less technical users at considerable risk. Simplification is required perhaps template approach with an agreement on default values for balanced of interests.

Regarding the intermixing of intelligence and privacy policy characterised by intelligent decision making / resource allocation based on data analytics, the challenges are enhancing analytics capability whilst increasing privacy and defining policy for aggregate data. Future research is required in privacy preserving analytics (data mining), which target same results with less intrusion of the data and research is needed on privacy preserving advertising as a linkage with advertising is a major driver for innovation within internet services. The goal is to provide the analytics in a privacy-preserving way. This would include clever use of technologies such as cryptography and efficient algorithms to achieve oblivious transfer resulting in the transfer of data without the database provider knowing what has been transferred.

There were a number of other policy related elements to privacy that should be examined in more detail by the research community. The first dealt with the costs associated with reading privacy policies, which if calculated would probably be quite
Companies collect personally identifiable information that website visitors are not always comfortable sharing. One proposed remedy is to use economics rather than legislative policies to address privacy risks by creating a market place for privacy where website visitors would choose to accept or reject offers for small payments in exchange for loss of privacy. The Federal Trade Commission (FTC) supports industry self – regulation for online privacy. In the late 1990’s, the FTC decided that the Internet was evolving very quickly and legislation could stifle growth.

Another important policy based approach is the World Wide Web Consortium’s (W3C) platform for privacy preferences (P3P)\(^1\), which lets web sites convey their privacy policies in a computer-readable format. Although not yet widely adopted, P3P promises to make Web site privacy policies more accessible to users. The Platform for privacy preferences specification has eight major components, most with multiple subcomponents and attributes:

- **Entity** lists contact information for the business, organization, or person who owns the site
- **Access** states whether individuals can find out what personal data a site keeps about them in its databases
- **Disputes** describes how to resolve privacy-related disputes with the site
- **Data** lists the kinds of data collected
- **Purpose** states how collected data is used and whether individuals can opt in or out of any of these uses
- **Recipient** states whether and under what conditions data can be shared and whether there is an opt in or out
- **Retention** states policies for periodic purging of collected data
- **Consequence** provides a human-readable explanation of site’s data practices.

There were several workshops held recently where the ontology of talking terms from P3P was retained. P3P is a protocol, privacy language and data format, some of which are no longer retained. As a direct result of Primelife, the ontology of talking terms of P3P was retained and still used as cutting edge state of the art. In terms of unsolved research, there is still a use for this tool. There is a transparency tool where service providers can contribute to the service. A number of questions were raised about P3P? Is a service provider rewarded for using P3P? Not technically but they are socially rewarded in value as they get a lot of extra traffic resulting in revenues. Is P3P enforceable? It is legally. How do you understand a big companies infrastructure in order to map into P3P? It would be quite difficult to do this but it is necessary for P3P to understand the particular attributes of data. When going back to inferences, how can you get an understanding from those attributes of data? Are companies going to show us how they make inferences? Usually, the companies are very keen on protecting these. These are the big research challenges. Note that the P3P sanctions are related to the commercial aspects and not research. The main point is that BIG data raises huge challenges to P3P and this needs to be addressed in future research.

It was pointed out during the workshop a number of times that privacy policies have the flavour of something that has been constructed to be as non-useful as possible to make users ignore them. Even legal people sometimes cannot understand the privacy policies.

With this in mind, how do we ensure that people understand what is meant by “informed consent”? It is not reasonable to make people have to remember many things. From a usability point of view, we can look at other technologies not as alternatives but as additional options for people to use eg. telephone vs. Facebook, ... In usability studies, if you have a continuous connection you didn’t trust, you could download everything and go off line and continue working in a trusted mode. Different patterns of use under the direct control of the user are important for future research. If we understood their use patterns better, researchers could better design the gatekeepers for the users of the future. Typically, the ordinary users don’t have a complete knowledge on how to use it so there is a big challenge to ensure there is informed consent of the users.

4.13 Legislation and Regulatory approaches

The European Data Protection Supervisor (EDPS) has taken a number of actions towards being involved and integrated within the EU’s Framework RTD programme’s including:

- Policy paper giving shape to the different forms of collaboration in Research initiatives² (especially within the FP7). June 2008
- Participation as observer in the "Research and Innovation for Security, Privacy and Trustworthiness in the Information Society think-tank" (RISEPTIS)³ 2008 - 2010
- Presence in relevant forum providing input e.g. Future Internet Assembly (FIA) session on Privacy and citizenship⁴. December 2010
- Specific opinions have been taken concerning research projects such as TrUsted Revocable Biometric IdeNtitiEs project (TURBINE)⁵ and ⁶ February 2011

The Commission has announced the intention to review Directive 95/46 on data protection in the light of the societal and technological evolution that has taken place from 1995 and also to fully reflect the changes introduce by Lisbon Treaty. In November 2010, the Commission provided in its communication to the EP and the Council some of the guidelines for the review. The EDPS is focussing on two of the guidelines:

1. Strengthening Individuals rights and increasing transparency for data subjects. It is necessary to give the user the ability to give ‘real’ consent in a user friendly and also making it effective. It is also necessary to clarify the so-called ‘right to be forgotten’ ie. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. The challenges for IT associated with this guideline include:

³ http://www.think-trust.eu/riseptis.html
⁴ http://security.future-internet.eu/images/1/1c/Privacy_and_citizenship_report1.pdf
⁵ http://www.turbine-project.eu/
⁶ EDPS, Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs), 14 p., also available at http://www.edps.europa.eu/EDPSWEB/edps/cache/offConsultation/OpinionsC/OC2011
• Establish mechanisms for (1) the data provided by the data subject (2) the data inferred by the controller from data subject activity (3) information about the data subject provided by third parties
• Interoperability, creation of standards that can be used by industry becomes of paramount importance
• Privacy by Design mechanisms - need clarification on what we mean by privacy by design

2. Enhancing the internal Market Dimension, which means enhancing the data controller’s responsibility. The challenges for IT associated with this are:
• It is necessary to progress in the harmonisation of tasks, competences and tools available for data protection officers across heterogeneous IT environments so equivalent levels of data protection is indeed a challenge. The measure tape must be the same!!!
• Data Protection Assessments should have a standardised way of being carried out so the risk can be assessed objectively. IT must provide the tools to carry such as risk assessments. Certification Schemas, Privacy seals for instance could be interesting.
• Although the term PET and PbD have been for a while around, it is still needed to progress in its definition, categorization and applicability.
• Data Protection Agencies cannot reach everywhere. Therefore, we must examine means of further encouraging self-regulatory initiatives including the establishment of sectorial codes of conduct aided by the necessary practical IT implementation is needed to ensure effectiveness of privacy regulation.
• Explore the feasibility of establishing EU certification schemes in the field of privacy and data protection.

IT has opened very important challenges for the legislators since IT has evolved a lot since the 95 Directive was created. The dimensions that IT is taking now: cloud computing, international data transfers, mobile internet, social networks,... could hardly be assessed at that time. Therefore, the new legislation aims to adapt to the challenges created by IT. This new EU data protection and privacy legislation coming in the next few months will quite likely incorporate some new principles and rights but, in general, will not give implementation rules and its practical implementation will need to be refined. And indeed, in the same way IT has created the challenges, it should provide the tools to give response to those challenges.

There is a lack of global regulatory frameworks for privacy that would work for everyone. There is also a lack of prototypes of new approaches (cloud computing, mobile computing) that work in the real world even with all of the funded research projects. These prototypes for real world should be highly scalable, high performance, usable prototypes with engineering methods used for privacy enhancing technologies. We need to work on closing these gaps. Transparency within organisations is needed because many organisations don’t know where there personal identifiable information is. There is a lack of metrics and privacy risk, impact assessment of technologies. There is no consistent way of looking at privacy. There is a lot of piecemeal work but nothing
pulling it all together.

There needs to be a closer harmony between legislative and regulatory approaches and the current business models of services e.g. social networking, which are based on the more information that you share, the more information that goes around and around. In fact, in most of these services, they are quite lacking in terms of how they define their privacy policy. But there should be a clear distinction between privacy violations and the way that these services present their privacy policy. A distinction should be made between those services that are storing information on things you want to keep private and those to which users knowingly sharing the information. To what extent is the mere risk of them having your data and sharing it in ways that could be detrimental a violation? It is a violation if they are storing information without your knowledge, without you knowing the object of their use of the data, without your consent and for longer than they should. It should be noted that Article 6 is about fair processing and Article 7 has the grounds including consent and you still have to satisfy everything in Article 6 also. Many people don’t realise that.

4.14 Addressing the conflicts with Privacy

The four basic rights to privacy were outlined:

- The right to protection from from criminal acts (Communications Assistance for Law Enforcement Act (CALEA) – 1994, PATRIOT Act - 2001)
- The right to promote legitimate business (Telecommunications Act (1996))
- The right to know (Freedom of Information Act - 1966)

These four basic rights are in conflict. On the one hand, you want to give the data to obtain particular services, and on the other hand, you want to protect your data to avoid harassment or terrorism. The actors involved are of various kinds and include innocent users, guilty users – thieves, terrorists, spies, data aggregators – Rapleaf, advertisers, search engines, social networks, legitimate service providers, and governments. All of these players play a part in this conflict and have different requirements based on their viewpoint and we need to decide what are the policies and technologies involving all the players.

There are research gaps in Privacy enhancing Technologies, which do not depend on the cooperation of service providers. Too many PETs are requiring 3rd parties and not the user to protect privacy and they need to have PETs under their control without any assumption of cooperation.

Another research gap being addressed to a certain degree in the Ensure project is on the need for anonymisation techniques, which maintain anonymity over the passage of time. When you are doing long term data preservation of clinical trials data, what happens to the data after twenty years?

Specific research questions include add the element of time to k-anonymity, and linkability algorithms. There is an issue that time is not taken into account. We also need to create a new business model for privacy, which is currently non existent. Finally, privacy with accountability (non repudiation) by design needs to be looked at in addition to just privacy by design.
4.15 Privacy and Trust

While ICTs are immensely beneficial for society and the economy overall, there are increased intentional and unintentional threats to privacy. The societal acceptance of the latest technologies is partly interlinked with the public’s trust that privacy is respected, and the societal acceptance is often a prerequisite for the deployment and use of the latest technologies. The further development, deployment and use of the latest ICTs is now being held back due to the opposition of consumer protection organisations, the lack of trust among consumers/citizens concerning the privacy/data protection issues and the hesitation of manufactures (likely due to these uncertainties and resulting investment risks). This lack of trust leads to missed business opportunities and stalled innovation. Therefore, privacy & trust need joint considerations of technology including the following elements - social science; economics, ethics; law and other disciplines. It also needs to be addressed from a pan-European perspective.

Research into privacy and trust should include the move to new ‘spaces’ (e.g. peer to peer (p2p) trust). Research is required on trust via rating sites, customer forums, P2P commerce, sharing, music producing, financing, collaborative knowledge producing, file sharing and social networks. There are dangers of potential security holes: false comments, false identities, phishing, social engineering and research must continue on enabling multi-identities, minimal disclosure and anonymity.

There is a need for policy frameworks including user controlled trust policies, user perceptions of trust, user-driven definitions of trust and inclusion of dynamic trust. We need research in establishing trust based on observation in a privacy-friendly way in which trust parameters can be dynamically changed.

Future Internet (FI) applications introduce new challenges in terms of privacy (e.g. smart metering). In addition, research should be carried out on the socio-economics aspects including investigating the impact of different types of secondary use of data (related - unrelated, leakage) as well as the impact in terms of consumers /market behaviour of data breach notifications.

4.16 Counter-profiling

Counter-profiling is an approach where a user might use a data aggregator tool (e.g. Dashboard tool developed in Primelife) that collects and displays data that was collected about you. This tool could also be used for good reasons to make users more aware of their data and who is using it. Although it is fairly rudimentary, you can collect the data and then do an analysis with pre-constructed queries. For these tools, further research must be carried out on user interfaces.

There were some cautionary questions raised about counter-profiling including if you implement counter-profiling fully, isn’t it the same as carrying out profiling yourself? In any case, to solve this problem, you need to collaborate amongst peers and many stakeholders. A single person cannot anticipate the kind of profiles that are being built about others.
5. SUMMARY

The workshop on "Privacy Protection and ICT: Future Research Ideas", organised by the ICT Trust and Security research Unit on 21st September 2011 was successful in highlighting a significant number of future research topics across the four sessions:

Session 1. Usability and socioeconomic aspects of privacy
Session 2. Technology for privacy in the Future Internet (in the cloud, in the mobile systems, in the Internet of Things, etc.)
Session 3. Policy for preserving privacy in the information society
Session 4. Security, privacy by design, trust and accountability

The following table highlights and maps the findings of the workshop according to the session outcomes.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Lifecycle management of users – the weakest link?</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>2. Geo-privacy: Geo-location and privacy</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Privacy and ID management in context aware (incl. commercial) environments</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Privacy and Social Networks</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Alternative economic models based on social concerns</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. EU research approach for privacy – should we follow the AIRBUS model?</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Privacy and Innovation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>8. Privacy and BIG Data!</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>9. Privacy and security in mobile environments using biometrics</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Privacy by Design – the silver bullet?</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>11. Privacy on centralised vs. de-centralised systems</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
### Workshop Sessions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Policy driven approaches for Privacy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>13. Legislation and Regulatory approaches</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>14. Addressing the conflicts with Privacy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>15. Privacy and Trust</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>16. Counter-profiling</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

The workshop met its objectives to elaborate future research topics within Privacy protection and ICT that can be used for providing inputs toward the future programmes, namely Horizon 2020.
## ANNEX 1. ATTENDANCE LIST

<table>
<thead>
<tr>
<th>Family name</th>
<th>First name</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dinant</td>
<td>Jean-Marc</td>
<td>University of Namur</td>
</tr>
<tr>
<td>Wenning</td>
<td>Rigo</td>
<td>W3C</td>
</tr>
<tr>
<td>Diaz</td>
<td>Claudia</td>
<td>KU Leuven</td>
</tr>
<tr>
<td>Lauhde</td>
<td>Mika</td>
<td>Nokia</td>
</tr>
<tr>
<td>Waidner</td>
<td>Michael</td>
<td>Fraunhofer Institute</td>
</tr>
<tr>
<td>Knapskog</td>
<td>Svein Johan</td>
<td>Norwegian University of Science and Technology (NTNU)</td>
</tr>
<tr>
<td>Ikonomou</td>
<td>Demosthenes</td>
<td>ENISA</td>
</tr>
<tr>
<td>Osborne</td>
<td>Mike</td>
<td>IBM Zurich</td>
</tr>
<tr>
<td>Albers</td>
<td>Andreas</td>
<td>University of Frankfurt</td>
</tr>
<tr>
<td>Velasco</td>
<td>Luis</td>
<td>EDPS</td>
</tr>
<tr>
<td>Avallone</td>
<td>Dario</td>
<td>ENGINEERING</td>
</tr>
<tr>
<td>Gambs</td>
<td>Sébastien</td>
<td>University of Rennes</td>
</tr>
<tr>
<td>Podsiadla</td>
<td>Aneta</td>
<td>Tech America</td>
</tr>
<tr>
<td>Markatos</td>
<td>Evangelos</td>
<td>FORTH - Institute of Computer Science</td>
</tr>
<tr>
<td>Klitou</td>
<td>Demetrius</td>
<td>Leiden University</td>
</tr>
<tr>
<td>Hartman</td>
<td>Alan</td>
<td>IBM Haifa</td>
</tr>
<tr>
<td>Van Hove</td>
<td>Johan</td>
<td>CA Technologies</td>
</tr>
<tr>
<td>Hildebrandt</td>
<td>Mireille</td>
<td>Trust in Digital Life</td>
</tr>
<tr>
<td>Ioannidis</td>
<td>Dimosthenis</td>
<td>CERTH / ITI</td>
</tr>
<tr>
<td>Rosenberg</td>
<td>Duska</td>
<td>Royal Holloway University of London</td>
</tr>
<tr>
<td>Clarke</td>
<td>Jim</td>
<td>Waterford Institute of Technology - TSSG</td>
</tr>
<tr>
<td>Del Alamo</td>
<td>José M.</td>
<td>Universidad Politécnica de Madrid</td>
</tr>
<tr>
<td>Villasante</td>
<td>Jesús</td>
<td>DG INFSO / F5</td>
</tr>
<tr>
<td>Anton Garcia</td>
<td>Maria Concepcion</td>
<td>DG INFSO / F5</td>
</tr>
<tr>
<td>Scillia</td>
<td>Mario</td>
<td>DG INFSO / F5</td>
</tr>
<tr>
<td>Juceviciene</td>
<td>Vilija</td>
<td>DG INFSO / F5</td>
</tr>
<tr>
<td>Carvalhosa</td>
<td>Manuel</td>
<td>DG INFSO / F5</td>
</tr>
</tbody>
</table>