Title session

Privacy and Citizenship

Responsible caretakers:

Jim Clarke, Nick Wainwright, Volkmar Lotz, Michel Riguidel

Other contributors to session organisation:

Peter Ljungstrand, Demosthenes Ikonomou, Roger Torrenti, Peter Stollenmayer, Magnus Erikson

Name of Chair/Moderator/rapporteur

Overall Chair: Jim Clarke, Waterford Institute of Technology, IRELAND
Panel Moderator: Peter Ljungstrand, Interactive Institute, SWEDEN
Rapporteur: Nick Wainwright, HP Labs, UNITED KINGDOM and Jim Clarke, Waterford Institute of Technology, IRELAND

Session objectives

To introduce the session, Chair Jim Clarke described the setting that led us to this topic. During FIA Bled through FIA Valencia, the trust and security sessions have concentrated heavily on trust and e-Identity. However, there were always strong underlying discussions in these sessions on the topic of privacy of the citizens. Moreover, in the open Trust and security caretakers session in FIA Stockholm, a large number of attendees strongly voted that privacy and links with citizens should be covered in a future FIA event.

There have also been quite a significant number of key items, reports, events, projects and initiatives dealing with these topics in the recent past, including the following:

- RISEPTIS Report[1], Trust in the Information Society, October 2009.
- Trust in the Digital Life[2]
- Conference on Trust in the Info Society[3], 10-11 February 2010, León, Spain.
- PRIMCluster and FP7 ICT projects Think-Trust[4], INCO-TRUST[5], PrimeLife[6], PICOS[7], FIDIS[8], TAS3[9], TA2[10], SWIFT[11], ….

[1] http://www.think-trust.eu/riseptis.html

[2] http://www.trustindigitallife.eu/

[3] https://trustworthyict.inteco.es/

[4] http://www.think-trust.eu/

[5] http://www.inco-trust.eu/

- ICT 2010[12], 27-29th Sept. 2010 in which both the necessity for innovation in the EU was stressed while at the same time the protection of fundamental rights to privacy were mentioned time and again.

As the session was two hours long, the session was broken over two topics related to Privacy and citizenship. These two selected topics were: Topic 1, User/Citizen issues related to privacy and Topic 2, Economics of privacy. The keynotes and panelists were selected accordingly with expertise in these topics. Full descriptions of the topics can be found in the Terms of reference of the session at the FIA Ghent web site[13].

The objectives and expectations of the session were highlighted, including giving the FIA a opportunity to lead the "enlightening" of the community on privacy matters, giving the impetus to push for what the citizens need in terms of privacy and supporting the ability of the users to make the right choices and not just blindly continue to hit the accept button. The session could also bridge the gap between all of the various stakeholders on this vitally important topic of the Future Internet. The various stakeholders include research communities (not only trust and security but also software and services, networks, Internet of Things, RWI, etc.), industrial, who need to ensure they have innovation whilst protecting the fundamental rights of their customers, legal/policy/regulatory communities and most importantly, citizens themselves. We need to discuss ways in which we can involve them better and empower them to have more control and rights over their own data usages. Additionally, an expectation of the session was to enable a balancing between innovation strategies and adherence to privacy, which goes both ways: privacy policies that are cognizant of business benefits and business models that are cognizant of privacy needs. The session could provide an opportunity to build a clear strategy and goal for progressing on implementation within the EU FI R&D communities by providing input for the various FIA Working Groups: Architecture, roadmap, standardisation, international cooperation, and others. In summary, the main objective of the session was to optimise the enlightening of

[6] http://www.primelife.eu/

[7] http://www.picos-project.eu/

[8] http://www.fidis.net/

[9] http://www.tas3.eu/

[10] http://www.ta2-project.eu/

[11] http://www.ist-swift.org/

[12] http://ec.europa.eu/information_society/events/ict/2010/index_en.htm

[13] http://fi-ghent.fi-week.eu/files/2010/12/Privacy_session_pres1.pdf

the FI projects and other relevant communities working together to assure citizens of their fundamental rights whilst enjoying the benefits of ICT in their daily lives.

Presenters/title/organisation

Presenter	Title	Organisation
Mr. Peter Hustinx,	Perspective of the European Data Protection Supervisor	European Data Protection Supervisor
Mr. Innocenzo Genna,	Perspective from the European ISP	ICT Independent expert, AIIP Director, EuroISPA Council Officer (European Internet Services Providers Associations)
Mr. Gabriel Yoran,	Perspective from an Industry – Social Networking	Founder, Head of Social Network, aka-aki networks GmbH.

Summary of presentations

Presentation 1. Perspective of the European Data Protection Supervisor

Mr. Peter Hustinx, European Data Protection Supervisor

Mr. Hustinx observed that there are an increasing number of news stories focusing on privacy and the media and politicians recognise this. People rely now on ICT in their daily lives more so to work, interact, etc. In doing so, they provide data more or less voluntarily, and sometimes in circumstances without their full knowledge or awareness.

There are some negative effects to this behaviour:

1. A seemingly insatiable hunger for data, to collect data, covered recently in a report in The Economist entitled “The Data Deluge”. There is uncertainty over whether all this data is needed, but it is gathered because it is technically possible.
2. An individual’s ability to know, or control, the data is diminishing. There are technological functions incomprehensible to the average user. There is a real lack of understanding by the average user. Privacy policies are difficult to read and to understand.
3. Massive collection of data is not accompanied by sound Information Practices. Information managers are not in control of their data. Arguably there is not a “high standard of care” being exercised by information controllers over this data.

Whilst this is being driven by innovation creating new products and services, this innovation should not be at the expense of human rights. The question to be addressed is “what should be done to ensure that individual privacy is respected as we go forward?” The EU Data Protection Directive is under review at this time. Further action is required in this area which addresses an individual’s ability to know, and consent to, what happens to that data. This is covered in Articles 10 and 7 of data protection directive.

There is a need for greater transparency in data management practices. We should clarify what “informed consent” means and when it should be obtained. Oftentimes, “implied consent” is inferred, or just a presumption, for example, as a notice as to when data will be gathered. An example is Google Streets cameras, where notice is given and if someone goes for a walk at that time, it’s presumed that he/she has consented to having their picture taken and uploaded to the Internet. Consent may also be inferred from silence or inaction and failure to tick a box declining consent may be deemed as consent. According to the European Commission, consent must be informed, and specific and, taken in context, it must be unambiguous, so there is no doubt that the individual has in fact consented. However, this is not what happens in practice on the Internet, and there are even business models built on this presumption of consent. This model of consent must be clarified and shared across the EU. The Article 29 working party is addressing this and will provide a comprehensive communication on it within the next months. The solution to this will require creativity by regulators and data managers. We also need to look at where ‘express consent’ must be used. For example, for “sensitive data”, this must be expanded but this must be done with care.

Putting users in control is only part of the solution. The principles of the data protection directive are still very relevant. They require data is kept secure, prohibit use for different purpose from that for which it was gathered, and require that people are given access to that data. There is a now a need for a more proactive approach. There is a need to integrate data-protection and privacy from the inception of new technologies – i.e. Privacy by Design. In this regard, we must ensure that systems are designed to use minimum of data. Privacy by Design also calls for ‘privacy by default’, and for the implementation of the necessary tools that will give citizens control over the data. It will empower users and give them more control over their data. It’s an example of good data management practices. The principle of privacy by design should be included in new policy in this area, and this is the view of the Article 29 working group.

The principle of accountability should also be reflected in a future framework. This requires data controllers not only to comply with the principles but also to take measures on putting procedures in place to ensure compliance, and to be able to demonstrate compliance. They are responsible from the beginning to ensure that things go right, not just when they go wrong. This will put privacy into practice, not just a theory, and data managers must have policies that will be put into practice in any processes. Data controllers should be able to demonstrate that they are implementing these practices, through documentation and assurance services. This will help them minimise mishaps, negligence, and help authorities implement the rules.

In conclusion, these are the necessary steps to ensure that ensure that we implement the processes to bring ICT in line with fundamental values and rights.

Presentation 2. Perspective from the European ISP

Mr. Innocenzo Genna, ICT Independent expert, AIIP Director, EuroISPA Council Officer
(European Internet Services Providers Associations)

Mr Genna described the relevant data protection frameworks (see slide). The main directive, 95/46, is under review and there is a consultation in process now. There is also interaction with Directive 2000/31 on electronic business.

The ISP/Telco industry produced a joint position paper from a coalition of industry organisations including. Cable Europe, ECTS, GSM Europe, EuroISPA, ETNO, which identifies areas where there needs to be more debate on these topics (see slide)

There are two main categories of ISPs: Access providers (providing data transportation), and Hosting Providers (hosting data and managing platforms). This distinction may be clear to us but to non-technical persons, this sometimes is confused and sometimes how this is addressed varies by jurisdiction. To clarify:

- Access providers are not liable for the data they carry (mere conduit principle);
- Hosting providers are not liable, unless they have actual knowledge of illicit content or activity, at which point they have a 'removal obligation'

Mr Genna illustrated this with four case studies:

Case 1: Spam. In many countries this is prohibited by law in some countries. ISP's can put anti-spam filters, which may require intrusive inspection of communications. There is a large difference between spam filtering and any other kind of filtering because the ISP can obtain the users consent, it addresses only one service – email which is only a small fraction of the content, and email is managed by hosting ISPs, not by the access ISPs. Spam is a good example of filtering, but we should note that it is not extensible to other services, something which non-technical people may not be clear about.

Case 2. Hosting. The Vivi Down case in Italy. Google was found responsible for a video posted that breached privacy rules. Google removed the video, but Google was not sufficiently accurate in informing the user about the privacy risk. The speaker regards this decision as 'a bit weak' on the privacy side. Google did make an agreement to prevent future incidents in the future. This is a good example of self-regulation

Case 3. IPR Infringements. Access providers are required to cooperate and fight piracy through activities that may conflict with privacy rules, e.g. monitoring usage which may have been done in breach of privacy laws. This may use deep packet inspection by ISPs, which may be in breach of their legal obligations, and require disclosure of personal details linked to IP addresses, something which can and should be done through the courts. Lastly, ISPs are required to retain data for IPR enforcement, but this is not covered by data retention regulations as ISPs can only retain data for the purpose of running their business. An example is the Sabam-Scarlet case in Belgium, where an ISP has been required to implement some filtering, which may be unlawful, and technically not possible to implement all filtering required.

Case 4. Network management, traffic management, are licit when providing security or addressing congestion, but are controversial when used to discriminate between other companies / services. In order to block, you have to 'open the packet' which may be a problem with regard to privacy rules. Proper evaluation requires a case by case analysis. Courts and regulators have not been analysing this problem with sufficient detail to make the right decisions as to which activities are lawful and which not.

Presentation 3. Perspective from an Industry – Social Networking

Mr. Gabriel Yoran, Founder, Head of Social Network, aka-aki networks GmbH.

Mr. Yoran is the founder of two companies, previously Steganos, a company providing Privacy and data security software, and now aka-aki networks GmbH, a location based social network company founded in 2007 and based in Berlin, Germany.

The aka-aki service is simple - when two members meet, their phones ring and show mutual interest. aka-aki has 700,000 members in Germany and France. When this product was started, the company was not aware of the policy of "privacy by design", but this is, in fact, what they set out to develop anyway. Users can change privacy controls, but this is kept very simple. This is a consumer offering and it has to be simple, they don't do 'grouping users' etc. Users have to know which data is gathered and what is done with it. But offering too many ways to control and configure scares users away; you can't leave all the decisions to the users; you have to make some decisions up front.

The most exciting features on location based services rely on location data analysis. It contains extremely interesting and valuable information. Today, they match people by interests. If they wanted to match people by preferred locations, they would have to keep location data. To provide a valuable service, they would have to keep this data for over a year, and if they want to have third party applications provide additional services, then this data will have to be shared with them.

Current regulations limit creativity. In their experience, data protection authorities don't want people to share their location, but the users do want to share location. Privacy is about being transparent about what you do with your data, but not about protecting users from themselves. Mr. Yoran noted that the current spirit of regulators is not around innovation, and what users actually want, but more of a 'don't do it' attitude.

The issues are here today and the data protection goals interfere with the business. They conflict sometimes. For example, data protection requires that data is deleted, but police and law enforcers want data on a particular user to be kept and made available to them.

aka-aki is advertising-funded, and they would like to know the location of the user to provide better advertisements. The compromise in Germany is to provide only limited location, namely a zip-code. However, their advertising provider is an American company where they do whatever they want with this data and it is not restricted in this way. aka-aki also can't hand over device identifiers to identify individual users, something that would provide a better service to users, and which American companies can do.

For example, at this time, Google can do this with Latitude. As a result, many web-2.0 companies relocate to other countries. Mr Yoran wants to ensure that the dialogue with regulators is continued but they must take into account what the users are wanting.

Why are these US services more successful? They let the users decide who to trust. They seem to trust Google, and millions have decided to do this. This change is inevitable. Geo-location will not go away; it must be made easier for innovative companies to experiment with new offers. Mr Yoran gave "caller-id" as an example of how user behaviour is changing, and reminded us how people were concerned that their phone number would show up when making a call, and that now caller-id is expected so that the receiver can filter calls, putting the receiver is in control, not the caller. The key concluding message here was that user behaviour is changing!

Panelists/title/organisation

Panelist	Title	Organisation
Mr. Peter Ljungstrand	Panels Session moderator	Interactive Institute (Moderator)
Mr. Thomas Ruddy	Expert on topic 1: User/Citizen issues related to privacy	EMPA Swiss Federal Research
Mr. Magnus Erikson	Expert on topic 1: User/Citizen issues related to privacy	Interactive Institute
Dr. Nicola Jentzsch	Expert on topic 2: Economics of privacy.	German Institute for Economic Research (DIW)
Dr. Nick Papanikolaou	Expert on topic 2: Economics of privacy.	HP Labs Bristol

Summary of panelists interventions and discussions following

Each of the panelists were given an opportunity to make an intervention based on the keynote talks and their expertise in the area.

Mr. Ruddy enquired how accountability would be made to work in practice This might be in terms of a code-of-conduct, and standards. For example, in Germany, there is a state-run information Commissioner, which has developed a certification to have a transparent privacy policy. Regarding the ISPs, it is not clear what the ISPs want to see come about, and while there is a distinction between the difference between the access and service providers, the speaker did not declare what the real interest of the ISPs was. On the other hand, aka-aki was very clear about the position that they would like to see us move to, and the conflicts that they face. This really is talking about something very important for the future. And as we move to a mobile world, there are very real privacy risks from mobile from fixed, and this really is a ‘paradigm shift’.

Mr. Erikson pointed out that one of the major reasons why privacy has become a concern is that privacy has become ‘detached from the senses and the body’ of persons. Now it’s unclear what data is private and what it can be used for. Even those who aggregate it don’t really know what it can be used for. Data is generated that is beyond what is understood or known by the individual. Even if data sets can be anonymised, then there are still risks that they can be used in negative ways.

Dr. Jentzsch addressed the desire of organisations to collect data for profit motives, and raised the example of Google-street-view cars collecting Wifi data, noting that there is a patent pending by Google on how to identify people from wifi networks and to locate them geographically. In general, she said, companies gathered personal data to predict willingness to pay and, of course, to better meet the needs of customers, but this puts them in a position of power with respect to the customer. Dr. Jentzsch drew parallels between the credit reporting industry, which collects credit information on individuals that lets them better predict risk and data collection on the Internet that lets companies predict how consumers are making decisions. She stressed that it was important to understand how consumers make decisions and asked whether there are plans in the European Commission to make available funding for research projects on the behavioural economics of privacy. Finally, Dr. Jentzsch does not agree that the innovators are stifled by the regulation, calling on the companies to innovate within the regulations. Also, Dr. Jentzsch does not agree with the industry argument that consumers should always obtain what they want. She drew parallels to the sub-prime loan market in the US, where consumers wanted house loans, which they could not afford and that turned out to be bad loans.

Dr. Papanikolaou pointed out that it is likely users will start caring more about privacy than before. This is the flip side of the often heard view that ‘privacy is dead’. Actually, users are becoming more and more informed about the consequences of sharing data and users will care more about privacy and will expect not just to consent, but to be able to ‘revoke’ and reverse consent. Consent is not static, it is dynamic. You consent to something, and then you should be able to change your mind and make sure your wish will be respected (and your privacy enforced). You should be able to delete personal data that concerns you, anonymise it, amend it; As we know, anonymisation is very difficult in practice: this was demonstrated in the recent examples of the Netflix prize database, which was released publicly for research purposes and was successfully de-anonymised, and the ‘Facebook Places’ feature which is very controversial as it’s enabled by default and allows Facebook users to track each other’s physical location. Now that we have the technical capability to provide revocation, deletion, and some form of anonymisation, users will expect to be able to delete, to hide, to revoke their data. So the issue is not just about giving users the ability to grant consent for processing of personal data, but about providing the ability to reverse, change, revoke that data as and when required.. Maybe you change your mind about the purposes, and you should be able to do that also. We must put users in control.

Each of the panelists/keynotes were then given an opportunity to respond to the interventions of the panelists.

Mr Yoran, in response to” innovating within” the regulations. In the case of aka-aki, they have done everything that is allowed in Germany, but they are competing with the US and other countries that don’t have these restrictions. Most of their users ask for their service to be more precise about location sharing, and they can get this from US companies.

Dr Jentzsch replied that all international companies have to comply with national/local regulations and she wondered about competition with US companies while being based in Germany and being subject to national laws. Mr Yoran asserted that some larger well known companies already do not, in fact, comply with the German regulation / European minimum standards.

Mr Hustinx observed that we are on the eve of a review of the modernisation of the current data protection framework. This recognises the need for uniformity and of elimination of unhelpful diversity in regulations. These principles are also being applied in a global context with OECD. Mr. Hustinx noted that the Federal Trade Commission in the US has also issued some thinking that has similarity with the European position.

Mr Hustinx observed that where consent is given, we also need to be able to roll back. On the other hand, if consent is part of a contract, then we need to take this into account. On location data, the guiding principle is that the client decides. Finally, on the fundamental question of privacy vs. economics – there are some tensions. Behavioural economics is practiced on the Internet (this was covered by a recent OECD workshop in Jerusalem, Oct. 2010). Markets operate under rules, and privacy is an issue where some rules need to be imposed as there are some market failures. We have to think about how we enforce the principles. We will have to move privacy from theory to measureable practice. Responsibilities must be taken seriously and, if not, there will be strong sanctions, which will give a strong incentive to comply. Certification, which begins by articulating what responsibility is, who is responsible, and the consequences of non-compliance, is one instrument. Accountability ensures that the responsible person can demonstrate that this is done. This works for other areas, for example, the environment and it can work for privacy.

Mr Hustinx said that the EU has decided to distinguish between privacy and data protection. This later applies whenever data applies to, or has an impact, on someone, and this the starting point where we will move to consistency across Europe to scale markets and to build trust. We will see more transatlantic convergence over the next five years; in the meantime, we will see more focus on compliance with the regulations that we have. The market for location data is a cutting edge area where the discussion around privacy is developing and there is space to innovate within the law.

Mr Genna addressed the question of the motivation of the ISPs. There is a problem of applicable law and there is uncertainty as to which law may be applicable or not, as illustrated by the Google Italy case, the court couldn’t accept that the matter was outside its jurisdiction. However, the positive outcome was that Google set up new guidelines and practices. Dr Genna also addressed this point with regard to ‘Filtering’. On a platform (i.e. an application services such as email) this can work as there is a presumption of consent (which should of course be done in the proper way). But when we talk about filtering on networks (not servers), it is much more difficult as you can’t presume the consent of the users, and technically it’s more difficult to do this in the network. We must have some consistency in the law across all categories, and the ISPs must comply with consistent regulation, and not depending on the particular business that they are in.

Mr. Hustinx, in response to point about ISPs, stated that issues around implied consent emerge and we need to be realistic. We need to be clear what the rules are and stick to them.

Dr Jentzsch said that we need more ‘honesty’ in asking consumers for consent. For example, when companies are going to sell information to many other companies, they should say so. This is not the same as asking for consent to use information ‘to suggest new products to you’. She also raised the example of “security data breach notifications” and said that she was not aware of any field data on this. Mr Hustinx said that there is some evidence that security breach notification works if it is targeted well, and then we do not get ‘notification fatigue’ (refers to some work in the UK on this).

Thomas Ruddy returned to the question on what the EU would expect from transatlantic convergence, observing that Americans have more confidence in the private sector whereas we have more confidence in government. US citizens get services were they have to ‘opt out’ and in EU citizens get services when they ‘opt in’. Do we expect convergence to go further in the field of privacy? Mr Hustinx said that there is a long way to go, there is going to be ‘sufficient convergence to make this work but it’s not there yet.

At this point in the session, a number of questions were elicited from the audience.

Q1. The questioner drew a contrast with the plenary session speaker who spoke about innovation where many data sharing applications were described and also with the open data session that was going on at the same time as this session, and wonders how this is going to line up with what the regulators are doing?

Mr Hustinx responded that the US has put a lot of emphasis on the issues of ‘notice’ and ‘consent’ and they have taken on the idea that when you publish a policy and get a ‘tick’, then everything that follows is ‘consented to’. However, he noted that we are at the verge of important action in the US.

Q2. The questioner said that he was from Switzerland, and, therefore, not under as much protection from the data protection directive and he is actually happy with that! The debate is easily misconstrued as a debate between regulators protecting the citizen and commerce who want to exploit the users. He asked that we think about the users who want to publish data in order to communicate! He argued that privacy cannot be discussed usefully without discussing the freedom to have information published, i.e. what freedoms may we be losing out on?

Mr. Yoran responded that many consumers view it as a ‘deal’ – you give up some privacy, and you get something for it. At the moment, the deal is bad – you give much information and get little back in return. Of course, the user should be the person who decides whether the deal is bad or good. Most people don’t think of this as a privacy issue but one of expressing identity, by what they post and where you are. They should have the freedom to do it, but also to decide for themselves whether it’s a good deal.

Q3. In social networks area, the thing that is owned is jointly owned, e.g. in social network situations. We have laws that impose legal liability that are conflicted. We also know that competition doesn’t work to support privacy. The larger players have the least privacy controls, yet people don't choose suppliers based on privacy. Behavioural economics doesn't assume that individuals are completely rational but that they can be influenced. Since you can't see the use to which data can be put, people don't make informed decisions. He concluded that "We might need to be a little more paternalistic" in the future.

Dr Jentzsch responded by asking whether people really know, when making a choice, what they are actually choosing. The policies about what use the data will be put to change, and implicit agreement is assumed. It's often not clear what the consumer is opting for. We should not restrict the choices we give consumers too much, she asserted, but it's possible and necessary to give people better tools to manage those choices.

Dr Papanikolaou asked when something goes wrong, who do we go to? The information Commissioner (or equivalent) is the first place to turn to, but if we 'gave it away', then there is nothing that can be done as it's already done. Is revocation feasible? Yes, if enterprise complies, this would be part of good data management practices.

Mr Hustinx concluded that we need to explore the "right to be forgotten".

Conclusions

Privacy and Citizenship are intrinsically linked since these subjects are highly relevant as people are increasingly relying on ICTs where security, privacy and trust are key enablers. Tremendous amounts of data are being processed with the service based economies and there is an unprecedented hunger for data (or "data deluge"). It will become ever more relevant given that over last ten years, we have been dealing with more security issues – within both public and information security - with significant impacts on privacy.

When dealing with privacy and citizenship, we need to draw a careful balance:

- real security does not exit without privacy built in; and
- real privacy won't exist without security built in.

With regard to privacy vs. innovation, yes, we need to strike a balance but not at the expense of fundamental rights of citizens.

There are a number of challenges to build privacy policy as we move forward into the Future Internet:

- Individuals must know what happens to their data;
- Individuals must gain control over the processing of their data;
- There is a need for greater transparency on data processing;
- There is an urgent need to clarify what "informed consent" means and when and how it should be obtained; In addition, clarification on what "implied consent" means, which may be inferred by an action or inaction of the user, should be addressed urgently. The way in which consent is given should be unambiguous and there should be no doubt about whether the individual has consented. The legal regime should ensure that consent is full and we need to find new ways to inform people "up front". For example, there are some cases where expressed consent should be required.

- Putting users in control of their data is only part of the challenge. The principles of data protection and the safeguarding of data are very important. The collected data must be kept secure, and must ensure prohibition of uses (or mis-uses) of the data not compatible with the users wishes.
- Need for more proactive approaches to data privacy and integration at a practical level.

Building the right data protection framework goes hand in hand with technological developments. When dealing with privacy and citizenship, a clear view of what data is applicable is required, including all information on individuals and on objects that could have an impact on the individual. This has consequences, in particular, on new technologies. This brings us to the principle of "Privacy by design" – attaining privacy by building data minimisation and processing of the minimum sets of data required into the systems. An example of this would be within social networks, keeping an individual's profile information private as the default. If implanted from the outset, privacy by design would ensure the following attributes:

- Compliance – it would be instrumental in limiting the collection of data;
- Empowerment of user – giving users more control over who uses and to what uses of their data;
- Ensure best practices on data protection.

There are a number of instruments available dealing specifically with privacy and citizenship. For example, Article 29 deals with accountability and adherence to better data governance. It describes the data controls not only to ensure compliance and demonstrate compliance on request. It will map procedures to ensure binding data policies complying with data subjects. Providing adequate protection will give more effective controls over data collection and how it is carried and minimise mishaps with the data.

Rights and obligations have been defined for all those that data protection relates to and these are now laid down in article 8 of the data protection directive and forms part of the Lisbon treaty. There are a number of defined rights:

- the right to know,
- the right to access, whenever data relates to the person or has an impact on the person.
- The right to object,
- the right to consent.

Regarding consent, many think this is the heart of the matter as it is one of five or six of the legal grounds. However, consent is currently rooted on very loose grounds and doesn't mean very much. A point was made in the panel discussions that we should not get too hung up about it apart from ensuring that when talking about consent, it is true and real consent and not a false, implied or misinterpreted one as currently experienced today when users blindly hit the accept button. Therefore, it is urgent to deal with clarifying and defining the limits of what is meant by consent. Maximum empowerment of users is a very important part of the privacy and citizenship subject. A significant amount of technological support is needed for this. In terms of a timeline for this, 2010 and 2011 will consist of reviewing and conclusions drawn from the wide public consultations that have been undertaken, detailed discussions will be made in 2012-2013 and brought before the Parliament in 2013-2014. The end goal is to work on an effective protection framework from today and implementation from 2015 onwards. As a research community, the FIA research communities can all play an important part in this.

Links/additional info

The full set of slides will be available shortly at both the FIA Ghent official web site:

http://fi-ghent.fi-week.eu/program/

and the Trust and Security FIA wiki:

http://security.future-internet.eu/index.php/FIA_Ghent