Final Report

Publishable Summary

Executive Summary

One of the key changes in societal trends and lifestyles witnessed over the past few years has been the move on-line of many consumers and the way they have become increasingly sophisticated in their media consumption habits. These real, rapid changes in market dynamics and consumer consumption require urgent evaluation of consumer consent as a fundamental aspect of the value systems on which the European market economy is based. The CONSENT project sought to examine how consumer behaviour, and commercial practices are changing the role of consent in the processing of personal data. While consumer consent is a fundamental value on which the European market economy is based, the way consumer consent is obtained is questionable in popular user-generative/user-generated (UGC) online services (including sites like Twitter, YouTube, Google Apps and Facebook), whose commercial success depends to a large extent on the disclosure by their users of substantial amounts of personal data. This project studied and analysed the changes in consumption behaviour and consumer culture arising from the emergence of UGC online services and how contractual, commercial and technical practices and other factors affect consumer choice and attitudes toward personal privacy in the digital economy.

The project aimed at and achieved the following objectives:

1. Analyse the evolution of commercial, technological and other practices employed by UGC service providers to obtain users' consent to the processing of their personal data.
2. Identify the impact of policies and practices employed by UGC service providers on community values like data protection, consumer protection and competition.
3. Explore the awareness, values and attitudes of users of UGC services towards privacy. Key findings here suggest that levels of awareness about certain UGC practices are low, and even where they are higher there is a marked gap between public awareness of service providers' use of personal data and the public's acceptance of such practices.
4. Establish criteria for fairness when obtaining personal data on the basis of users' consent and develop a best practice approach for the use of consent by UGC service providers. This includes a proposal to use new laws to make increased choice for UGC users mandatory especially by requiring that means of revenue such as direct payment be used as an alternative to making provision of service conditional to giving personal data
5. Develop a toolkit for policy-makers and corporate counsel to implement and promote the best practice approach.

The project's impact started building up thanks to the way it engaged with stakeholders in annual Policy Workshops and the Final Conference. Its impact continues to grow even after the project formally closed since the project findings and its Policy Brief continue to be reported upon in the media and discussed in various fora and policy makers including members of the LIBE Committee of the European Parliament and other MEPs. The Policy Brief was also communicated to the Council of Europe's Consultative Committee on Data Protection as well as the European Commission.

Summary Description – Project context & Main Objectives

One of the key changes in societal trends and lifestyles witnessed over the past few years has been the move on-line of many consumers and the way they have become increasingly sophisticated in their media consumption habits. This has not only taken place in a context of globalization where international borders and traditional jurisdiction are increasingly blurred but also in one where leading market research firms describe economic activity as occurring within "complex on-line ecosystems". Typically one notes that [A] web landscape that once required people to go to specific web destinations for content has evolved to one in which content is pushed to consumers, where and how they want to consume it. This dynamic was pioneered by, and is commonplace among, Web 2.0 leaders such as MySpace, YouTube, and Facebook[1]. These real, rapid changes in market dynamics and consumer consumption require urgent evaluation of consumer consent as a fundamental aspect of the value systems on which the European market economy is based. The EU has differentiated itself from other markets and especially the US market by stricter regulations involving consumer consent including areas like data protection[2], distance-selling[3] and, spam[4]. Yet all these efforts at predicating consumer protection on the principle of consent may now be seriously undermined by recent changes in globalised on-line media industry and consumption trends.

The CONSENT project sought to examine how consumer behaviour, and commercial practices are changing the role of consent in the processing of personal data. While consumer consent is a fundamental value on which the European market economy is based, the way consumer consent is obtained is questionable in popular user-generative/user-generated (UGC) online services (including sites like Twitter, YouTube, Google Apps and Facebook), whose commercial success depends to a large extent on the disclosure by their users of substantial amounts of personal data. This project studied and analysed the changes in consumption behaviour and consumer culture arising from the emergence of UGC online services and how contractual, commercial and technical practices and other factors affect consumer choice and attitudes toward personal privacy in the digital economy.

The nature of UGC services as a social tool

[1] Steve Dennen, 2009: The Epoch of Extended Web Content, ComScore Voices, 16 December 2008, last accessed 8 January 2009 at http://www.comscore.com/blog/

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[3] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The Internet has become a central feature in modern contemporary society. There are few activities, if any are left at all, that are conducted wholly offline. Being online, communicating with others, shopping, reading, watching movies etc. increasing all form part of the everyday reality of western societies.
Within this context UGC services play a very important role as a social tool. What has become evident during the course of the CONSENT project is that UGC services attract users of all ages and of varying backgrounds. It is mistaken to think that UGC services (and online social networks in particular) are the space for teenagers and young people only. Recent statistics show that the fastest growing demographic on Twitter, Facebook and Google+ is the 55–64 year age bracket. This demographic has grown 79% since 2012.[5]

Use of UGC services supports a trend that can be traced from the 1970s of an increased self-disclosure. Arguably, self-disclosure is a key feature of contemporary societies and can be recorded in every sphere of social life (personal relationships, intimacy, media, politics, language, lifestyles, etc.). However, the internet and in particular the variety of UGC services reinforce this orientation in many ways and degrees and multiplies the impacts of self-disclosure-oriented behaviours in terms of size (i.e. the number of people concerned) and intensity (i.e. the strength, depth and duration of the consequences related to self-disclosure).

The UGC services business model

UGC service providers have built a business model that relies on users' orientation towards self-disclosure. UGC service providers build profiles of their users based on the personal information shared (or gleaned from) users. Based on these profiles advertising is sold. Indeed the predominant business model of UGC service providers is advertising: 'classic advertising', behavioural advertising, and contextual advertising.

Advertising is the primary business model, though during the course of the project one could trace an increase in business models based on paying customers, or on the offering of mobile apps or web apps or a combination of all these business strategies. It remains to be seen whether there are other alternative models but it is indicative of services seeking to wean themselves away from a sole source of revenue.

The value of personal information to the business model has led to businesses being set up to link up available information from public, semi-public domains and to de-anonymise data to develop profiles of consumers with personally identifiable data labels.

UGC services and privacy

Having an orientation towards self-disclosure does not automatically mean that

[5] http://thenextweb.com/socialmedia/2013/11/12/10-surprising-social-media-statistics-might-make-rethink-social-strategy/?fromcat=all accessed 13 November 2013

privacy and the enjoyment of a private space is no longer a value of a modern society and users of UGC services.

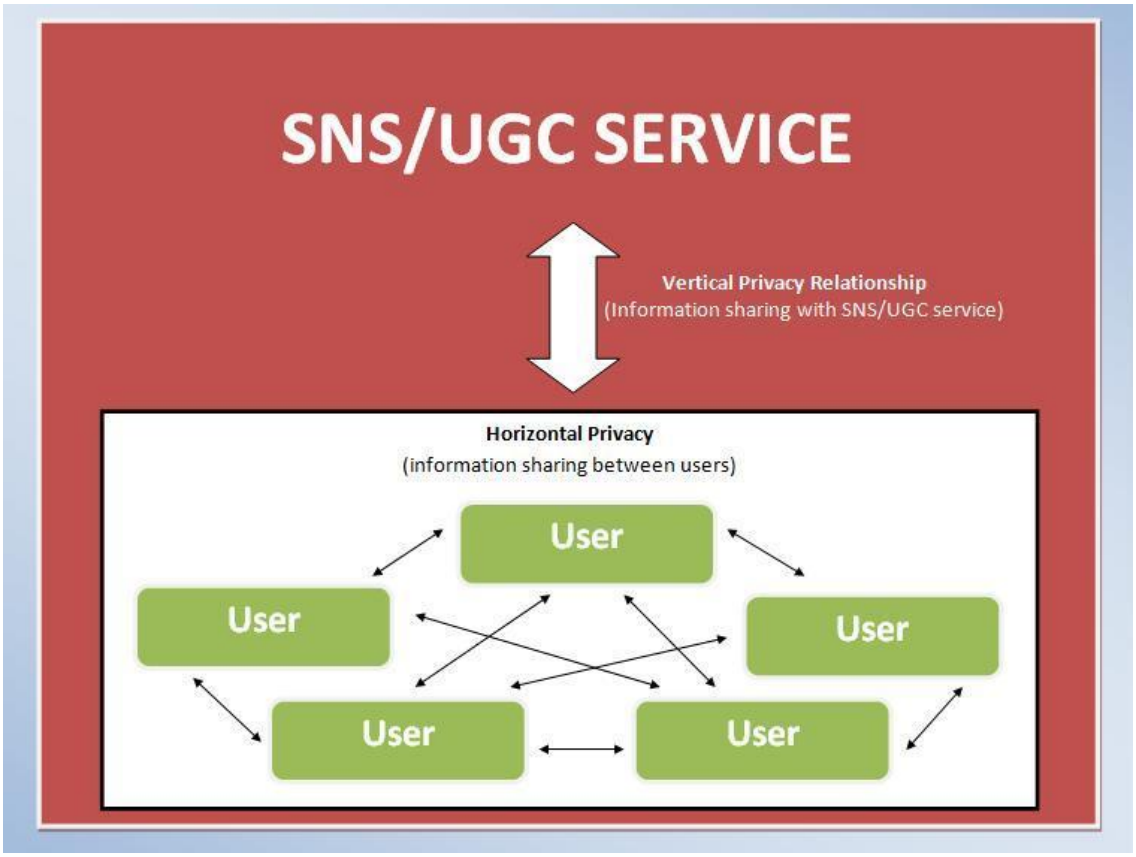
Research has shown that users still regard privacy as an important issue (even if they neither read privacy policies nor take action to prevent misuse of their private information).

Privacy is a key issue in the UGC services sphere. Given the risk of massive and continuous privacy breaches, one can see that there is an increasing demand for privacy protection too. Recent events reported in the media e.g. the skirmish between Facebook users and Facebook about privacy issues and recent NSA revelations in news, remind us of the ongoing relevance of privacy issues in the UGC sphere.

In the case of UGC services, the risks and opportunities for privacy protection are often different to what one is traditionally used to in the offline world. The greatest threats to privacy are coming not only "from the outside" (i.e. from governments, bodies, and commercial entities and other users) but also but also "from the inside" (i.e. the individuals' strong propensity to reveal aspects of their own private life such as feelings, projects, physical characteristics, health information, sexual orientation, tastes, opinions, activities, etc.).

Traditionally, law has assumed that as long as the 'threat from inside' is based on the voluntary self-disclosure, then it is up to the user to take responsibility for the possible reduction in the enjoyment of one's private life.

For 'threats from outside' we need to distinguish between at least two forms of relations in UGC services that can give rise to issues to the rights to private life and data protection: vertical relationship: between the provider and the user (we can refer to this as vertical privacy); and a horizontal relationship: user to user relationship (we can refer to this as horizontal privacy).



So far, horizontal privacy has been deemed to be covered by the 'purely personal or household activity'[6] exemption. Following the opinion of Article 29[7], horizontal privacy in UGC services would in many cases fall outside the scope of European data protection legislation.

This is increasingly difficult to accept when one sees the consequences of the publishing of personal data on a horizontal level. Two more common consequences (reported in the media) are:

- The use of tagged pictures (persons 'identified' in pictures by others (when they have not uploaded pictures themselves)) is being used by UGC providers in increasingly sophisticated facial recognition systems.[8]
- Increase in use of 'information' on UGCs as evidence in court cases. It is reported that, e.g. in the United States, in 2011 alone 689 published cases

[6] Data Protection Directive 95/46/EC Article 3(2).
[7] Article 29 Data Protection Working Party (WP 163) Opinion 5/2009 on online social networking
Adopted on 12 June 2009
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf
[8] See for example Article 29 Data Protection Working Party (WP 192) Opinion 02/2012 on facial recognition in online and mobile services Adopted on 22 March 2012
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

used involved social media evidence.[9]

The complexity of the privacy protection on the Internet and developments that have occurred since the start of the CONSENT project.

Protecting privacy on the Internet is complex, nuanced and delicate. The complication arises from its lack of dependence on a single system of laws, answerable to a single, identifiable enforcement authority. The reality is that there exists a collection of rules and practices based on varying legal cultures, with differing approach and goals, as well as lacking effective enforcement mechanisms. The lack of central authorities is on the one hand a strength of the Internet and on the other hand makes it difficult for users to be able to obtain remedies for vertical privacy breaches.

In the preparation of this Toolkit (and during the project) the legal context has focused primarily on the European context - both at a regional level (Council of Europe and European Union Legislation) and a national level, looking into the legal developments of the European states members of the consortium.

During the course of the project, the European Commission presented a Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[10]. The text of the proposed Regulation and the discussions that ensued have informed and inspired some of the tools in this Toolkit. The legislative process was still on-going at the time of the conclusion of this Toolkit.

During the course of the project a large number of cases/actions were undertaken by data protection authorities around Europe against UGC services for alleged privacy breaches - for example the cases brought against Google Streetview by a number of German data protection authorities[11]; the close follow-up and questioning of the French data protection authority following changes to Google's privacy policy (and the finding that Google's Privacy Policy Violates EU Law by the UK, German, And Italian Data Protection Authorities[12]); the action started by Austrian students against Facebook before the Irish data protection authority[13].

CONSENT project objectives

---

[9] See "689 Published Cases Involving Social Media Evidence (with full case listing)" published at http://articles.forensicfocus.com/2012/04/16/689-published-cases-involving-social-media-evidence-with-full-case-listing/

[10] Proposed Regulation (25.01.2012. COM(2012) 11)

[11] http://gigaom.com/2013/04/22/google-fined-189k-by-german-privacy-authority-who-wishes-he-could-fine-more/

[12] http://safegov.org/2013/7/25/google's-privacy-policy-violates-eu-law-according-to-uk,-german,-and-italian-data-protection-authorities

[13] http://europe-v-facebook.org/EN/en.html

Against this background, the project aimed at achieving the following objectives to:

1. Analyse the evolution of commercial, technological and other practices employed by UGC service providers to obtain users' consent to the processing of their personal data.
2. Identify the impact of policies and practices employed by UGC service providers on community values like data protection, consumer protection and competition.
3. Explore the awareness, values and attitudes of users of UGC services towards privacy.
4. Establish criteria for fairness when obtaining personal data on the basis of users' consent and develop a best practice approach for the use of consent by UGC service providers.
   Develop a toolkit for policy-makers and corporate counsel to implement and promote the best practice approach.

Main S & T results / foregrounds

The research in the CONSENT project was carried out in the context of four distinct, but interdependent project streams:

- A Status Quo Analysis covering an analysis of current UGC services policies and practice and the legislative framework,
- Consumer Attitudes,
- Criteria for Fairness and Best Practice. Cultural differences in the concept of privacy were taken into account and analysed in a special work package.

In its first 18 months (01-05-2010 - 31-10-2011) the project carried out a Status quo analysis of the current commercial, technological and other practices employed by service providers and the existing legal framework within which those providers operate.

CONSENT collected three complementary sets of data:

- **Data on existing services:** CONSENT has put together a list of individual service providers offering services to a particular target group in each participating country (WP2).

- **Data on current policies and practices, including:**
  o A mapping of service providers' privacy settings and fair processing information with a view to identify common purposes for which providers collect use and disclose their users' personal data (WP3).
  o Identifying current practices (including contractual and technological practices) that service providers employ in order to obtain users' consent (WP4).
  o Identifying current policies and practices employed by services providers in relation to the interoperability of UGC and SNS services (WP5).

- **Data on the legal framework** operating in participating countries governing both the interoperability of services and obtaining consent (WPs 5 and 6).

The main findings here include:

a. Fair processing practices are generally weak. E.g. only few of 107 UGCs reviewed:
   - - Use a separate registration stage for explicitly expressing consent to processing personal data;
   - - Enable user's online status to remain invisible to other users;
   - - Allow deletion of sources of posts (and/or the posts themselves) placed on profiles of others by an individual who has removed an account;
   - - Have a formal complaint procedure;
   - - Provide users with a clear and direct message on updates of the privacy policy (or choice to opt-out of the updates);

- - Require an explicit consent to process personal data for commercial purposes and allow users to withdraw this consent without a need to remove the account.

b. Privacy Policies
    - Finding a copy of the privacy policy is not always possible. Various reasons may lead to this - link not evident on the web-site, or link not working properly.
    - Some smaller UGCs have no privacy policy at all; others just refer the user to the national data protection legislation
    - Readability of privacy policy varies greatly between providers -
    - Language - complex language/terminology; in 40 services that offer more than one language option, often the profile interface languages differ from the languages of policy documents.
    - Style - different styles
    - Length (from shortest of 45 words to longest of 7500 words!)

c. Data portability and interoperability
    - While research has shown that there are no major obstacles to interoperability (as long as data protection, competition, intellectual property regimes are followed) there is no coherent policy (apart from inclusion in Digital Agenda) in favour of or promoting interoperability.
    - Interoperability between international players and national players absent.
    - Some smaller UGCs lack interoperability options citing technical difficulties.
    - Some sites allow interoperability to be turned on and off contextually but this also means more complex services and more difficult to understand sites.
    - The vast majority of sites contain simplified interoperability in terms of the ability to log in with other credentials and/or cross-post content
    - Most websites do not allow their users to select which information is accessible to which interoperable sites, i.e. the only option is to opt in or out
    - In most cases it is not transparent what private information is being transferred and for what purpose
    - Interoperability is in a vast majority of cases declared but either not properly explained or explained with the use of complicated technical and legal jargon
    - UGC websites do not explain what happens with information when accounts are disconnected

The current European legal framework is insufficient in several ways:

- In practice Directive95/46/EC has been implemented differently in the different EU Member States. The differences in implementation lead to major differences in application and enforcement.
- In general data protection authorities do not have enough legal powers and resources to enforce European data protection laws.
- Since UGC service providers know the data protection authorities in practice has little or no power, UGC providers have no incentive to abide by law and give citizens the protections provided for in law.
- Reliance on the notion of informed consent as a safeguard for users is unreasonable given the disparity in contracting powers that exist between service providers and users. The proposals in the draft Regulation do not resolve this issue since they do not make mandatory those measures which are complementary to consent and which could make consent be more significant e.g. the obligation on the part of the provider to provide the SNS/UGC service even without the user granting of consent for profiling but against a reasonable payment as an alternative to giving up one's personal data and being subjected to profiling.
- There is a lack of requirements for availability, accessibility and readability of privacy policies. This gives rise to a large disparity of texts, where texts exist at all. Given that privacy policy is often the basis for informed consent clear rules are necessary to secure that users do obtain the right information upon which to base their consent.

In the second 18 months of the project (01-11-2011 - 30-04-2013) the project focused its attention to establishing the values and attitudes to privacy of users of UGC and SNS services. CONSENT used a combination of quantitative (WP7) and qualitative (WP8) methodologies to establish the values and attitudes to privacy of users of UGC and SNS services.

The quantitative phase of the research measured current levels of awareness of privacy issues, beliefs on privacy practices, evaluation, and current user practices. A web-based questionnaire was used for the quantitative part of the research. The pan-European questionnaire was answered by 8641 individuals from 26 countries. Fourteen countries had respondent numbers which were sufficient for a meaningful quantitative analysis by country. Some key findings include:

- Disclosure of personal information online was considered as generally rather risky – mostly between 5 and 6 in all countries on a scale of 1-7 (1 being the lowest risk and 7 being the highest risk).
- The largest variation of perceived *general* risks between results in different countries occurred in respondents' perception of unexpected problems arising out of disclosure of personal information online (Netherlands: 4.44; Czech Republic: 5.89). This suggests different

levels of perceived control in different countries – although the overall high sample average (5.16) highlights a generally elevated perception of loss or lack of control.

- The average *general* awareness of personal information being used by website owners for a number of purposes was rather elevated (74%) – however, locally ranging between 60% (Ireland) and 89% (Germany).
- Regarding awareness of *specific* website owners' practices, on the one hand there was high awareness (72%-87%) and moderate levels of acceptance in the case of being contacted by email and the customisation of content and advertising. On the other hand, gathering in-depth information about users and making it available or selling it to others were less well known about (awareness 51%-61%) and largely seen as unacceptable even with financial compensation.
- Noticeably below-average awareness levels of all practices could be particularly observed amongst Slovakian respondents and, to a certain extent, with Bulgarian, Romanian and Irish respondents, where a lack of experience in UGC usage, and a lack of knowledge, may be assumed.
- The different awareness levels of website owners' practices in different countries mostly corresponded with respondents' online behaviour regarding technical protection measures in those countries. Ireland and the UK were an exception in this regard as technical protection measures appeared to be well known and commonly used, but awareness of some of the website owners' practices was rather low.
- Just above 50% of all CONSENT respondents indicated that they often or always change their privacy settings but country results varied between 77% in Germany and 38 to 42% in Italy, France, Slovakia and Romania.
- Only 24% of all respondents read privacy policies often or always. A further 23% claimed that they sometimes read privacy policies.
- There were considerable country-specific differences in the practice of reading, or not reading, website terms & conditions and privacy policies. However, it was not the countries with the highest assumed need of increasing awareness and technical protection knowledge (Slovakia, Romania, Bulgaria) who showed the highest portion of non-readers, but Ireland and the UK – countries with an established internet literacy.
- Only 11% of privacy policy readers claimed to fully understand the privacy statement or policy they had read.
- Less than half of all respondents answered that they ever decided not to use a website due to their dissatisfaction with the site's privacy policy.

This was then followed by in-depth personal semi-structured interviews for the qualitative phase. The interviews were conducted between May and July 2012 in the partner countries.

- Key findings from the 131 interviews carried out include that:
  - Most UGC users experienced an internal conflict between wishing to keep control of their personal data and a perceived need, or desire, to use UGC services. A number of different strategies were used for dealing with this conflict.
  - Interviewees in most countries were less willing to give personal information online than in offline situations. A majority outlined their uncertainty about what is happening to their personal data online and who is holding it and possibly sharing it with unknown others.
  - Being engaged in UGC usage did not necessarily go alongside a greater willingness to disclose information for commercial trade-offs, and being open to commercial trade-offs was not linked to a more "generous" disclosure of personal and private information on UGC sites.
  - The website owners' practice of sharing and selling personal user information to third parties was mostly deemed unacceptable due to a fear of losing control both at the point of first information disclosure and when using the website, but also through the uncontrollable use by third parties at any future point in time. This practice also went counter to the strong desire on the part of interviewees to be able to decide themselves which data would be shared or sold, when and to whom – even in the case of anonymized data. Rejection of this practice may also be linked with unease that users' perceptions of privacy may differ from those of website owners.
  - The most common measures taken to protect privacy online practice was to exercise caution in disclosing personal or private information online. More proactive measures varied according to the interviewees' levels of awareness and experience of possible data misuse, knowledge of the possibilities and limitations of changing privacy settings and the technical ability to do so.
  - The majority of interviewees in most countries stated that they usually do not read privacy policies. Reasons for not reading privacy policies can be divided into two categories: technical and content. At a technical level, privacy policies were not read because they are too long, written in text that is too small and too difficult to understand. On the level of content, interviewees did not feel the need to read privacy policies because they are "always the same", or because the contents would already be familiar due to discussions in the media.
  - Those who did read privacy policies viewed this as part of a learning process that is indispensable if one wishes to assume responsibility for one's personal information and be able to take adequate protective measures.

- A common perception amongst both readers and non-readers of privacy policies was that privacy policies primarily serve the purpose of protecting the website owners rather than the website users.

Other outcomes - The creation of a Toolkit

Based on findings found in the CONSENT project, a Toolkit was produced in the form of a document which focuses its attention on four main themes:

i. Promoting User Consent
ii. Fair data collection and processing practices
iii. Adequate User Control
iv. Safety and Security

Within each of these themes a number of issues are identified and addressed. Once a theme is identified, the document lists appropriate strategies to be followed to improve or remedy the conditions noted in the issue. Appropriate Tools and Actions to achieve the strategy and address the issues are then listed and explained. The Tools and Actions are arranged according to the three target groups identified earlier (legislators and policy makers, corporate counsel and UGC service providers, user groups). No Tool is planned as a complete stand-alone. Indeed, no one tool alone will solve the ensemble of issues identified in this Toolkit or a particular issue. For change to be most effective, the Tools need to be taken together.

The toolkit includes a large set of tools including:

- legislation (directives, regulations, decrees, decisions, laws, subsidiary legislation, etc.);
- best practices (including the way of making them known - public recognition-oriented initiatives, awards, quality marks, public display of best practices, etc.);
- communication and awareness-raising activities (information campaigns, information desks, ads, social events, newsletters, brochures, etc.);
- education and empowerment (training courses, school curricula, guidance packages, etc.);
- lobbying and negotiation (public agreements, joint committees, cooperation schemes, quality networks, etc.);
- Standardisation (standard setting initiatives, agreed standards, self-regulation practices);
- Privacy-by-design (new technological options including privacy enhancement technologies, etc.);
- research-based tools (observatories, studies, annual reports, quality assessment exercises, etc.).

Other Outcomes - Distilling the findings and analysis into a Policy Brief

Parts of the toolkit were discussed (as part of the discussions on the Policy Brief) with a broader audience including relevant stakeholders from amongst others academia, the European Commission, the European Data Protection Supervisor, national Data Protection authorities and Information Offices, the Council of Europe, Civil Society, business and many other stakeholders during the CONSENT Final Conference held 20-21 March 2013 in Malta. During the Final conference: 'Online Privacy: Consenting to your future'

The project consortium has identified a graded set of policy implications and actions that can be taken by policy makers. These are contained in the policy brief attached. This information will allow policy-makers to assess whether the current regulatory framework governing the use of consent conforms to consumer perceptions and expectations in relation to the level of control they feel that they should be able to exercise over their own personal information.

The S & T Findings of the CONSENT project indicated above have several policy implications for legislators, policy-makers, service providers and consumers. The Policy Brief translates these into recommendations for actions to improve data protection from legal, policy, education and technical perspectives. The recommendations are divided into five options that build upon one another. These recommendations cover more than law and policy but include strategies.
Given that not all recommendations are of equal importance, the project research team in the Policy Brief followed an ascending importance rule: starting from issues that though having some policy implications do not require any further action (Option 0); to issues requiring limited update/revision of existing legislation and policy funding schemes (Option 1); increasing to more substantial update/revision of existing legislation and higher level of funding for complementary measures (Option 2); to measures establishing a coherent legislative framework for UGC content / on-line use of consent and requiring a high level of investment in complementary measures (Option 3); escalating to recommending new mandatory obligations for UGC providers and maximum level of investment in complementary measures (Option 4).

Following the presentations and discussions held during the Final Conference, the CONSENT Policy Brief has been further developed for publication and distribution to a wide variety of stakeholders among which the LIBE committee, the Council of Europe and several Civil Society organisations (e.g. ISOC and EFF).

Description of Potential Impact

The project findings from CONSENT provide policy makers with:

- An overview of the current practices employed by online service providers across the EU for obtaining consent from users to the processing of their personal data. This will enable policy makers to establish whether there are substantial differences between the practices used by providers in different EU member states, by providers in different markets segments and by providers which target different population groups. They should therefore be able to evaluate the extent to which a differentiated approach is required to any issues which may be borne by the research carried out as part of the CONSENT project.

- An overview of the current policies and practices employed by UGC and SNS service providers in relation to the interoperability of services. It allows policy makers to establish any differences in the policies and practices used by providers in different countries with a view to making a policy decision on any harmonising measures that may be required in order to ensure development of a competitive market for UGC and SNS services across the borders of individual member states.

- The results of in-depth empirical research into
    - the awareness of users and non-users of UGC and SNS services of practices (defined above) used by those services
    - the values and attitudes of those users to privacy and
    - the way in which their awareness and attitudes influences their consumption behaviour.

Dissemination Activities

At the start of the CONSENT project the coordination team together with the dissemination team has developed the Dissemination and Communications Strategy (DaCS). The DaCS aimed to cover all dissemination processes. Its main aim was to identify each target audience and outline how it will be reached. A number of possible target audiences together with relevant issues were identified and reviewed following consultation with European Commission officials responsible for advising on communication and dissemination.

In the Analysis of target groups five important target groups were identified:

i. Policy makers - This target group includes:
- inter-party Committees and sub-Committees at national parliaments, at the European Parliament (e.g. LIBE) as well as the Parliamentary Assembly of the Council of Europe,

- parties at the European Parliament, local political parties, individual MEPs and MPs
- governmental bodies (e.g. EU and national data protection offices, consumer protection offices etc.),.
- Inter-Services Steering Group of the Directorates of the European Commission

ii. Research and academia - This target group includes universities, scholars, research groups and individual researchers.

iii. Industry - This target group will include various providers of UGCs, business units, industry associations, trade unions, rating agencies etc.

iv. Consumers - This target group includes consumer associations and subsequently individual consumers.

v. Mass Media - This target group is a means to an end (particularly reaching all other target groups) as much as an end in itself and includes individual editors, journalists and EU/governmental PR agencies.

The suitable way of communication is naturally very much dependent on the communication channels and preferences of the specific target group. The CONSENT project has attempted to address the identified target groups via the best suitable means of communication and dissemination.

In the CONSENT project's main dissemination events (and especially its two Policy Workshops and the Final Conference) invitations for participation were extended to the different target groups using different and tailored communication channels. The direct result of this hybrid communication and dissemination strategy was not just a relatively high number of participants in the dissemination events but it also guaranteed speakers, panelists and an audience from various relevant backgrounds.

The indirect result of this hybrid communication and dissemination strategy is the higher level of acceptance and impact of the project's results since the results have been discussed with a wide range of stakeholders at different stages in the project.

In the following paragraphs the project's main dissemination events and some of The highlights will be reflected upon. Of specific interest are the target groups and the specific stakeholders involved.

Dissemination event 1: Full Immersion Workshop – Rome, 13-14 January 2011

The full immersion workshop was held in Rome on 13-14th January 2011. The two-day workshop, consortium members as well as representatives from the

Commission, Ms. Marianne Paasi and Ms. Laura Corrado, and the external advisory group, Ms. Meryem Marzouki provided input and meaningful discussion on concepts of privacy and culture as well as on the development of the quantitative web-based questionnaire. The first day of the workshop was the presentation of by Dr. Luciano d'Andrea on the cultural differences of privacy. The second day included presentations from consortium members from post-totalitarian nations on the effect this era of history may have had on perceptions of privacy as well as a presentation by Dr. Noellie Brockdorff on the web-based questionnaire that will be deployed in WP7.

Dissemination event 2: The First Policy Workshop – Göttingen, 5-6 July 2011

The Policy Workshop was held on 5-6 July 2011 and hosted by the University of Göttingen. The two-day workshop brought together consortium members as well as representatives from the Commission, the Council of Europe, industry service providers, representatives from other research projects and members of civil society.

Keynote speeches were delivered by among others Mr. Kimon Zorbas, Vice-President of IAB Europe, Ms. Andreja Rihter, Rapporteur, Parliamentary Assembly of the Council of Europe, Motion on Privacy and the management of private information on the Internet and other online media, Mr. Giovanni Buttarelli, Deputy European Data Protection Supervisor and Prof. Uwe Hasebrink, Hans-Bredow-Institut für Medienforschung in Hamburg.

A Policy development Panel provided for an open discussion with panel members from European Commission Data Protection Unit, UGC Service Providers, Council of Europe T-PD addressing questions like '*What input should service providers and other stakeholders be giving to policy makers in Strasbourg and Brussels?'*

Furthermore, the findings of the CONSENT project were presented and discussed by attendees and panel members. The result was a robust discussion on the issues facing users and social networks spanning a wide range of sectors including law, technology and sociology.

Dissemination event 3: The Second Policy Workshop - Cluj-Napoca, 6-7 September 2012

The Second Policy Workshop entitled ***Perceptions, Privacy and Permissions: the role of consent in on-line services*** was held in Cluj-Napoca, Romania, hosted by CONSENT partner Babes-Bolyai University. The workshop was held over two days, 6-7 September 2012.

- The workshop was advertised via mail-out through the Lex Converge network;
- The conference was well attended by academics, practitioners, service providers from Europe and beyond including Mrs Renate Weber MEP, Prof. Eric Goldman from the High Tech Law Institute at Santa Clara University

School of Law, Christine Runnegar from the Internet Society (ISOC) and Rainey Reitman from the Electronic Frontier Foundation (EFF).

- During the Second Policy Workshop the (preliminary) results from WP6 and WP 7 and 8 were presented. These results were amongst many other things discussed in two panel discussion sessions with panels in which the different stakeholders of the CONSENT project were represented.

Dissemination event 4: The Final Conference – Malta, 20-21 March 2013

An important milestone in the final project period was the Final Conference held 20-21 March 2013 in Malta. During the Final conference: 'Online Privacy: Consenting to your future' (http://www.onlineprivacyconference.eu) the main results of the CONSENT project were presented to wide group of stakeholders from academia, the European Commission, the European Data Protection Supervisor, national Data Protection authorities and Information Offices, the Council of Europe, Civil Society, business and many others.

The organisation of the CONSENT Final Conference to be held in Malta 2013 had been making progress since its inception at the Steering Committee Meeting held in León, Spain in January 2012. The Organising Committee (Dr. Clive Zammit, Dr. Noellie Brockdorff, Prof. Joe Cannataci, Prof. Jeanne Pia Mifsud Bonnici, Ms. Terezie Smejkalová, Ms. Bettina Zijlstra and Mr. Aaron Ceross) has been working closely together with the consortium partners, a local organising team of the University of Malta and many different stakeholders in order to achieve a high profile conference with a high impact.

As can be seen in the CONSENT Final Conference programme[14] (also attached to this report) a long list of stakeholders made presentations during the conference. These include a contribution by: Dr. Viviane Reding - Vice-President of the European Commission (as part of a video message); Mr. Peter J. Hustinx - European Data Protection Supervisor; Ms Lara Ballard - Special Advisor for Privacy and Technology in the Office of Communications and Information Policy at the U.S. Department of State; Ms. Sophie Kwasny - Head of Data Protection Unit, Council of Europe; Ms. Nevena Ruzic - Member, Consultative Committee of the Council of Europe Convention 108; Ginger McCall - Director of EPIC's Open Government Program and IPIOP Program; Ms Christine Runnegar - Senior Policy Advisor, Internet Society; Mr Andreas Krisch - President, European Digital Rights; Ms Rainey Reitman - Leader of Activism Team, Electronic Frontier Foundation; Mr Max Schrems - europe-v-facebook.org; Ms Kirsten Bock - International Coordinator at Office of the Data Protection and Freedom of Information Commissioner, Schleswig-Holstein, Germany; Mr Johannes Caspar - Commissioner for Data Protection and Freedom of Information for Hamburg,

[14] The CONSENT Final Conference 'Online Privacy: Consenting to your Future' programme can be found via http://www.onlineprivacyconference.eu/category/programme/

Germany; Mr Wojciech Rafał Wiewiórowski - Polish Inspector General for the Protection of Personal Data; Mr Ken Macdonald - UK Assistant Commissioner for Northern Ireland and Scotland. A draft copy of the CONSENT project policy brief was discussed in the panel sessions with these stakeholders and other stakeholders present in the audience. Indeed an important part of the programme was the panel discussions, but also the different papers and streams sessions in which selected papers and streams submitted in response to a call for papers were presented. The abstracts were published in the conference website[15] and a selected number of full papers will be published in book form as a single-volume special edition of Law Science & Technology published by *Edizione Scientifiche Italiane*.

Dissemination event 5: Press Breakfast with the European Data Protection Supervisor – Malta, 21 March 2013

In the morning of 21st March 2013 a Press Breakfast with the European Data Protection Supervisor, Mr. Peter Hustinx, was held before Mr. Hustinx delivered his keynote speech in the CONSENT Final Conference. During the press breakfast a speech was given by Malta's Civil Liberties Minister Helena Dalli and Mr. Peter Hustinx followed by a short panel discussion chaired by Prof. Joe Cannataci.

In summary the CONSENT project, in its Dissemination and Communication Strategy aimed at identifying its target groups and involving those target groups in its research via among other things its dissemination events in order to receive timely, topical and quality feedback and input from its stakeholders. We believe that the project has achieved this goal in not merely having large events with a high number of participants but rather having events with high quality speakers, panellist and audiences in order to allow for lively debates and discussions on the (preliminary) research results and developments in our fast-paced digital society.

By openly discussing the project's (preliminary) research results with the various stakeholders from policy makers to businesses to civil society organisations the feedback received could directly be integrated in the project's on-going research. An excellent example of this is the open discussion on the CONSENT Policy Brief during the CONSENT Final Conference. This discussion and the feedback received has been integrated in both the Toolkit and the Policy Brief, which we believe will be powerful tools aimed at the relevant stakeholders groups in order to achieve maximum impact.

Ongoing Impact

The project's impact continues to grow even after the project formally closed since the project findings and its Policy Brief continue to be reported upon in the media and discussed in various fora by policy makers including members of the

[15] http://www.onlineprivacyconference.eu/category/papers-streams/

LIBE Committee of the European Parliament and other MEPs, [16]The Policy Brief was also communicated to the Council of Europe's Consultative Committee on Data Protection as well as the European Commission. It is expected to inform part of the ongoing discussions about the European Commission's Data Protection Reform Package between 2013 and 2015.

[16]See various media reports on dissemination activities involving MEPS inter alia discussing CONSENT project results at
https://www.facebook.com/events/257690901045548/?ref=22
http://gozonews.com/42199/debate-highlights-need-for-more-awareness-on-online-privacy/