EUROPEAN

POLICYBRIEF

CONSUMER SENTIMENT REGARDING PRIVACY ON USER-GENERATED CONTENT SERVICES IN THE DIGITAL ECONOMY (CONSENT)

Researching the use and development of social networks and user-generated content services and examining how consumer and commercial practices are impacting users' fundamental right to privacy

16 November 2013

INTRODUCTION

A key change 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. Have these recent changes to consumer and commercial practices developed in such a way that consumers are (in)voluntarily signing away their fundamental right to privacy? The CONSENT project sought to answer this research question from a multi-disciplinary perspective, providing a means to develop the appropriate tools and mechanisms to ensure consumer protection.

EVIDENCE AND ANALYSIS

The state of protection when using social networks and user-generated content services is of low quality and consumers desire stronger mechanisms through which they may reasonably protect their personal data. Through analysis of the services, the law and consumer sentiment, the project has identified gaps in the legal enforcement of the protection of user data and lack of standards in protecting personal data in social networks. While European Union law provides a solid framework for such protection, it remains unrealised due to a number of factors, notably lack of appropriate enforcement tools and education. Due to this, users using the current services feel vulnerable and dissatisfied of the differing and incomplete levels of protection. Thorough analysis of the technical realities and the application of law have provided a foundation from which to devise recommended tools and actions in order to fill the enforcement gaps.

The policy implications and recommendations identified in the next section are based on a status quo analysis of the current policies and practices of 107 European and international user generated content (UGC) service providers. The project mapped the privacy settings and fair processing of information identifying common purposes for which providers collect use and disclose their users' personal data. In the process, it identified current practices (including contractual and technological practices) that service providers employ in order to obtain users' consent and current policies and practices employed by services providers in relation to the interoperability of UGC and SNS services. This study was complemented by a review of the legal framework and current legal developments including the Commission proposal for a General Data Protection Regulation.

CONSENT compared the practical and theoretical status quo with consumer attitudes to privacy when using UGC services. A pan-European questionnaire was answered by 8,641 individuals from 26 countries. This was followed by more than 131 interviews for a more in-depth understanding of consumer attitudes. Cultural differences in the concept of privacy were taken into account in the analysis too.

Based on the evidence found in the status quo and consumer attitudes analysis, together with best practices identified during the process, the project prepared a toolkit aimed at policy makers, corporate counsel of UGC services and users. The Toolkit brings together a number of measures that if taken can improve many of the practices that were found lacking in the analysis. The key recommendations are addressed in the next section.

The following are the key findings that have important policy implications:

Consent and Privacy Policies

1. Only 24% of all respondents claimed to have read privacy policies often or always. A further 23% claimed that they sometimes read privacy policies.
2. There are 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 (e.g. Slovakia, Romania, Bulgaria) who showed the highest portion of non-readers, but Ireland and the UK – countries with a more established internet literacy.
3. Only 11% of privacy policy readers claimed to fully understand the privacy statement or policy they had read.
4. 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.
5. 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.
6. Some smaller UGCs have no privacy policy at all; others just refer the user to the national data protection legislation
7. 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!)

Data Protection Legislation

1. 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.
2. In general data protection authorities do not have enough legal powers and resources to enforce European data protection laws.

3. 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.
4. 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.
5. 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.

Data portability and interoperability

1. 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.
2. Interoperability between international players and national players absent.
3. Some smaller UGCs lack interoperability options citing technical difficulties.
4. Some sites allow interoperability to be turned on and off contextually but this also means more complex services and more difficult to understand sites.
5. The vast majority of sites contain simplified interoperability in terms of the ability to log in with other credentials and/or cross-post content
6. 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
7. In most cases it is not transparent what private information is being transferred and for what purpose
8. 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
9. UGC websites do not explain what happens with information when accounts are disconnected

POLICY IMPLICATIONS AND RECOMMENDATIONS

The Findings of the CONSENT project have several policy implications for legislators, policy-makers, service providers and consumers. Below are recommendations for actions to improve data protection from legal, policy, education and technical perspectives. The recommendations below are divided into five options that build upon one another. These recommendations cover more than law and policy but include strategies

This section identifies key findings of the CONSENT project that have important policy implications and makes recommendations on how each should be address. Given that not all recommendations are of equal importance, we have 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).

Option 0 – No action – Status quo

0.1 Data ownership:

The notion of data ownership is a much debated topic and one with many intricacies and components. There are at least two distinct elements with ownership over content: copyright and profiled information. There is no foreseeable concerted will to create new personal data ownership rights, and to revise current intellectual property rules and regulations in order to cater for a concept of data ownership by the individual. This could also have serious consequences for other rights, particularly Art. 10 (Freedom of Expression) of the European Convention of Human Rights.

0.2 Definition and scope of 'consent':

A legal tradition on the notion consent is present and defined in each of the national legislations throughout the European Union, albeit these are not necessarily harmonised. The current Directive provides that consent be free, informed and unambiguous. However, this concept of consent has not always been transposed word for word at national level. The draft Regulation proposes to substitute unambiguous for explicit, which would only strengthen the concept as applied to data protection.

Option 1 – Limited update/revision of existing legislation and policy funding schemes

1.2 Giving consent and readability of privacy policies:

1.2.1 The definition proposed in the draft Regulation on data protection should be maintained. However it should be made clear that a long and unreadable privacy policy should not be the basis for consent. Research has shown that users rarely read privacy policies and when they do they do not always understand what is in the policy. This raises issues on how far one could claim that the consent obtained from users on this basis is informed. To counter issues of 'informed consent', three levels of protection are suggested:

1.2.1.1 'Medicine Warning' labels model: Oblige services to use standardised messages – similar to health warnings – placed in a prominent manner on page asking for users' consent (at the start of the service relationship and whenever consent for continued use of personal data is required during the provision of the service).

1.2.1.2 Privacy policies written using clear and simple language: Privacy policies are not required at a European level and this should be implemented. A further requirement would be for authorities to set out best practice guidance will create certainty in the SNS/UGC services market place and help create dialogue with enterprise and government to find simple, non-legal solutions to issues. SNS/UGC services should be encouraged to collaborate with appropriate authorities (e.g. data protection authorities, consumer protection authorities, Article 29 Working Party) to adopt a statement of best practices on how to best explain the data use by the service as well as user privacy to users.

1.2.1.2.1 These standards should focus on approachable, non-legal terminology, presented in a manner that is accessible for the widest range of audience types, including minors.

1.2.1.2.2 Increasing access to comprehension of privacy policies and data use: There are a variety of means by which to convey to the user. This has been done in certain instances by larger companies and is a practice to be encouraged and boosted.

1.2.1.2.3 Machine readable privacy policies: Encourage the use of machine readable privacy policies, where the user can then set its browser to alert him/her every time the privacy policy of a service provider does not match the preferences of the user.

1.2.1.2.4 Taken together, these means will provide a greater transparency for data use policies of SNS/UGC services, without the need to reduce the freedom of individuals to consent

to a wide range of situations. This item does not seek to shape a definition or scope of privacy or data protection, but to ensure that individuals are empowered with sufficient knowledge to make choices that fit their own preferences.

1.2.1.3 Certification schemes: Users are more likely to trust a service and the privacy practices of a service if an external body has checked the practices of the service provider and issued a seal of approval. European data protection compliant certification schemes exist (e.g. Europrise[1]) and should be encouraged to develop further and their services promoted as best practices.

1.3 Standard Form Contracts/Consumer Protection:

1.3.1 The services provided by SNS/UCG operates should come under the scope of consumer protection law.

1.3.2 The protections under this sort of legislation would address issues of post-contract formation, exclusion clauses, jurisdiction and other related matters of importance to consumers. Therefore, the services would not be able to exclude liability or coerce users into unfair contracts due to economic disparity and inability to negotiate fairer clauses.

1.4 Education and Awareness

1.4.1 Education and awareness programmes may be integrated in social education in schools, adult computer skills education as well as bolstered by public campaigns. The focus should remain on understanding how personal data is processed by online services and the degree of control and responsibility given to the individual. These programmes may be divided into (i) a short-term multimedia publicity campaign (such as those started in Nordic countries e.g. Denmark and Sweden within the Safer Internet Plus Programme information campaigns on child protection online) and (b) long-term education in schools and community centres.

1.5 Systems to protect special groups (including minors):

1.5.1 Protection for minors: The draft Regulation on Data Protection recognises that minors are a class of individuals that require more specialised safeguards. While in literature and other jurisdictions (e.g. the United States under the Children's Online Privacy Protection Act (COPPA)) age verification mechanisms have been introduced, the reliability and effectiveness of these systems is questionable. Cooperation is recommended with the countries like the United States, Japan, Canada, Australia as well as with service providers, and further research and analysis is needed to identify better ways to protect the needs of children online.

1.5.2 Protections for other vulnerable groups: Minors are not the only groups needing further provision in online services. Other groups, such as those with special needs may require further safeguards and protections for such services. Further research and analysis is needed in this regard to understand the current challenges and to provide future proposals.

1.6 Data Portability and Interoperability:

1.6.1 Data portability should be implemented as a strong feature in relation to SNS/UGC services. This concept should remain in the draft Data Protection Regulation and further guidance should be sought from regulators and industry cooperating on open standards.

1.6.2 Requirement for online services to adhere to open standards with regards to data storage and processing to enable users to move their data from one service to another.

1.6.3 These standards themselves may be set through self-regulation of services but enforcement of compliance should be allocated to an independent body working closely with DPAs.

[1] https://www.european-privacy-seal.eu/

1.6.4 Service providers should be encouraged to develop standards for interoperability of services.

1.7 Better protection of European citizens online

1.7.1 Given the ubiquity of the internet and many of the activities on the Internet, the territorial scope of European law often does not offer enough protection to European citizens online. More research on viable legal and technical options to address jurisdiction and enforcement issues, the provision of effective legal remedies and other difficulties European citizens encounter online is highly recommended.

Option 2 – More substantial update/revision of existing legislation and higher level of funding for complementary measures i.e. Option 1 as well as the following:

2.8 Data ownership:

2.8.1 This involves further rights than those solely on data protection: personality rights and copyright. This requires consideration of multiple legal issues to resolve rights over information. This would require a concerted effort within the European Union (and potentially beyond) to establish a clearer demarcation of where data is 'owned' by an organisation (e.g. in the instances of aggregate information contained within a database for mining purposes) and if and how the user may remove his/her own data from such database.

2.9 Changes to privacy policies/Renewal of consent:

2.9.1 Renewal of consent when changes in processing takes place: When the data processing is based on consent, any change of purpose of processing and changes in the privacy policy imply that there is no longer consent. In such cases, particularly when the purposes for the data processing have changed, the user should be informed of the changes and renewal of consent should be required for the continuation of the processing.

2.9.1.1 All changes (and not only major changes as proposed in the Regulation) to the privacy policy should be notified to the user following a medicine warning label model in for example a pop-up screen.

2.9.1.2 Any change in the privacy policy requires a new, informed consent. If not consented, then the user is automatically opted-out after a set time period and the service deletes the personal data. Concurrently there would be a period allowing users to export their data to file for their own records or to port to another service.

2.9.1.3 For services that have followed a certification route, changes to privacy policies also need to be certified.

2.10 Education/Awareness campaign:

2.10.1 Funding Europe-wide awareness on data protection: The topics would include data portability, withdrawal of consent and the fundamentals of data processing. This would require a concerted effort to run campaigns on an EU-wide level. Similar to what was noted in 1.4 above these programmes may be divided into (i) a short-term multimedia publicity campaign and (b) long-term education in schools (e.g. be inclusion in national curricula across the EU) and community centres.

2.10.1.1 Withdrawal of consent: Users should be made further aware of their rights to withdraw consent to a service and have their personal data removed. An increase in awareness will have an impact on creating a market force which would influence services to ensure compliance with best practice and the law.

2.10.2 Funding Europe-wide awareness on privacy: The focus is slightly different than above. Here the focus would be on educating users about privacy in an effort, not only to educate themselves regarding the services, but also regarding information of other individuals. This would combat challenges such as offensive behaviour, 'leaking' of personal information/media and related matters.

Option 3 – Establishing a coherent legislative framework for UGC content / on-line use of consent – High level of investment in complementary measures i.e. Options 1 -2 as well as the following:

3.11 Mandatory Data Portability:

3.11.1 Data portability should be made mandatory for all service providers (processing the data of more than 500 data subjects per year). Regulators and industry should cooperate to develop open standards for data portability.

3.12 Mandatory machine readable privacy policies

3.12.1 Mandate the use of machine readable privacy policies (for services providers processing the data of more than 500 data subjects per year) , where the user can then set its browser to alert him/her every time the privacy policy of a service provider does not match the preferences of the user.

3.13 Launch voluntary certification schemes

3.13.1 Further from point 1.2.1.3, while European data protection compliant certification schemes exist (e.g. Europrise), for wider take-up of the certification process the market conditions for the development of the schemes, commitment to the scheme and cost to comply with the certification scheme need to be financially and politically supported.

3.14 Enforcement Mechanisms:

3.14.1 DPAs should more strongly enforce the current rules already in existence. The DPAs should check the privacy policies of the most used UGCs in their country/region and act accordingly to the legislation if it is not in line with the current law.

3.14.2 Monetary fines: Following what is proposed in the draft Regulation, data protection authorities need to be in a position to be able to impose substantially high fees on providers not compliant with data protection rules. Together with the ability to impose substantial monetary fines, they need to also have some discretion in their application. This is indeed very tricky as it can lead to forum shopping of least strict data protection authorities by service providers.
3.14.3 Standardisation of enforcement: experience has shown that different DPAs enforce similar situations differently. This may lead to a least strict enforcement forum shopping by providers, and may also lead to a reduced level of legal certainty for users. One way of reducing the differences may be by DPAs agreeing to standard enforcement procedures, shared training activities and the creation of enforcement checklists that can be followed by all the DPAs. This policy brief suggests that the standardisation process should be lead and coordinated by the European Data Protection Supervisor's office as this would fall within his supervisory mandate.

3.14.4 Mandatory data audits: Mandatory data audits can be another mechanism by which to investigate data protection breaches. These data audits should be carried out by certified, independent third party auditors and submitted to the relevant DPA for review. In this way, the DPA may receive relevant information about the types of services processing data in the jurisdiction, have pertinent information and make better use of resources for investigation and prosecution of breaches. The cost is borne by the service processing the data.

3.14.4.1 Articles 22 and 33 of the proposed Regulation for data protection create clear obligations for data controllers to have data audits. However there is no requirement that these

are performed periodically and by independent third party auditors. This is not enough. The legislation should include clearer rules on periodicity; who should carry out the audit and the fines that may be imposed where these audits have not be carried out or not been carried out well.

3.14.5 Registration: Currently (under the Directive) those organisations processing data must register with the relevant authorities. This registry can be made more accessible to users and with the data auditing proposal above, the DPA can provide a wealth of information to users about the data controllers using/storing/processing their data. The proposed Regulation has done away with registration. This policy brief recommends the re-inclusion of the registration rules.

3.14.5.1 This option does have certain drawbacks however as the external auditor may be then given access to information users not wished to have disclosed to third parties. There is also a significant trend in literature and discussion on abolishing such registration due to perceived inefficiencies and associated costs.

3.14.5.2 The Policy Brief therefore advises that these aspects of registration of data controllers are addressed as a wider issue in future investigations.

3.14.6 Funding of more human and technical resources for data protection authorities: A chronic problem of most data protection authorities is that they are understaffed for the amount of work that is required when carrying out an audit/investigations of large providers. Supporting the training and employment of more human resources is central for effective enforcement.

3.14.7 Cooperation between data protection authorities: since often multiple data protection authorities may have an interest in an investigation against a service provider, combining efforts may by a more effective way to carry out the investigation. However, for this to be legally possible, the legal basis and mandates for cooperation need to be included in the legislation. Furthermore, funding for cooperation activities need to be allocated to the data protection authorities.

Option 4 – Proposing new mandatory obligations for UGC providers – Maximum level of investment in complementary measures i.e. Options 1-3 as well as the following[2]:

4.15 Mandatory certification schemes

4.15.1 Further from point 1.2.1.3 and 3.13, while European data protection compliant certification schemes exist (e.g. Europrise), to assure the maximum protection for users and the fairest market conditions for providers, compliance with the certification scheme needs to be a mandatory requirement.

[2]Historical note: the CONSENT Research Group in March 2013 considered the inclusion of the following additional action under option 4 "**Creation of a parallel European Internet**

- This option includes the creation of network based within the European Union, designed with technical features specifically to safeguard privacy and data protection features as well as allow for greater control mechanisms to enforce European law and principles in cyberspace. This option would require substantial investment and commitment technically, politically, legally and socially. Within this 'European Internet' the system could be engineered to cater for European ideals on data protection, privacy, commerce and a host of other matters; the technical feasibility is not in question. The challenge with this option comes with the potential walling off of users and services from the 'global' Internet, which has its own social and political consequences."
- The inclusion of this option as a formal policy recommendation was dropped at the time for the sake of prudence but at the time of filing of the final report, in a post-Snowden era when "parallel universes" and a "pan-European *Internetz*" are now being actively and promoted, especially by German commercial giants such as Deutsche Telekom, Brazil and other important actors, the consideration though not the adoption of such an option by the research group is hereby being recorded and communicated to policy-makers

4.16 Mandatory interoperability with open standards

4.16.1 All service providers (processing the data of more than 500 data subjects per year) should be obliged to follow open standards for the interoperability of services.

4.17 Use new laws to compel service providers to offer real alternative to personal data

The principle of informed and explicit consent should be complemented by a legal principle which ensures that the user of an SNS/UGC is not faced with a position of "take-it-or-leave it" where a decision not to give personal data would otherwise result in his or her being denied access to an SNS/UGC service. Therefore, wherever possible, the service provider should be compelled by law to offer the user a reasonably-priced alternative to obtaining access to and use of an SNS/UGC service without having to surrender personal data unnecessarily or be profiled for the duration of his/her use of the SNS/UGC. The requirement for consent could very usefully be complemented by other legal requirements e.g. the ability to use an SNS/UGC for a fee as a choice over giving away personal data in return for a "free service". This approach to the "privacy-benefit" trade-off would thus improve consumer choice and consumer protection without depriving the service provider of all income and instead provide an alternative revenue stream to advertising income lost by the inability to profile or otherwise use personal data from the user.

Research Parameters

Project Objectives

The CONSENT project sought to examine how consumer behaviour and commercial practices are changing the role of consent in the processing of personal data. Within this context, the project documented and analysed:

- changes in consumer online behaviour;
- behaviour and consumer culture;
- effects of contractual, commercial and technical practices on consumer choice; and
- consumer attitudes toward personal privacy

Methodology

The project was divided into 13 work packages, each with a cross-disciplinary focus in order to give a holistic view of the challenges and issues arising in social networking services and privacy:

1. Coordination and project management
2. Identifying and classifying UGC services
3. Mapping privacy settings
4. Obtaining consent
5. Analysis of interoperability of services
6. Impact of common policies and practices
7. Quantitative measurement of end-user attitudes towards privacy
8. Qualitative study of UGC users and UGC non-users attitudes towards privacy
9. Criteria for fair processing information and technical features
10. Toolkit for policy makers and corporate counsel
11. Evaluation
12. Dissemination and knowledge transfer
13. Cultural differences in the concept of privacy

The research and development work packages were carried out in the context of four distinct, but interdependent project streams: **Status Quo Analysis**, **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 (WP13). Separate work packages include project

management, the evaluation of the research methodology, the effectiveness of the project partners in executing the project and the quality of the project outcomes and dissemination of project outcomes.

Status-quo analysis
Focusing on 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 (WP2).
Data on current policies and practices, including:

- 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).
- Identifying current practices (including contractual and technological practices) that service providers employ in order to obtain users' consent (WP4).
- Identifying current policies and practices employed by services providers in relation to the interoperability of UGC and SNS services (WP5).

A review of the current legal framework operating in participating countries including the implications of the proposed Commission Data Protection Regulation and recent court decisions and decisions of data protection authorities in Europe involving UGC services (WPs 5 and 6).

Consumer attitudes
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 (Behaviour). A web-based questionnaire was used for the quantitative part of the research. This was then followed by in-depth personal interviews will be employed for the qualitative phase.

Criteria for fairness
The CONSENT project identified criteria for the privacy friendly use of fair processing information, privacy settings and technological features employed by UGC service providers to obtain user consent (WP9). The development of those criteria was based on the results of the Status-Quo Analysis and took into account existing criteria and best/good practices developed in other contexts.

Best practice
The CONSENT project developed a toolkit for policy-makers, corporate counsel and users to implement and promote a best practice approach based on the fairness criteria established during the previous phase (WP10).
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.).

PROJECT IDENTITY

PROJECT NAME

Consumer Sentiment Regarding Privacy on User-Generated Content Services in the Digital Economy (CONSENT)

COORDINATOR

Professor Joseph A. Cannataci, Rijksuniversiteit Groningen, Gronignen, The Netherlands j.a.cannataci@rug.nl

CONSORTIUM

Asociatia pentru Tehnologie si Internet –
Bucharest, Romania

Babeș -Bolyai University - Faculty of Law –
Cluj-Napoca, Romania

Consilio Nazionale delle Richerche –
Rome, Italy

Copenhagen Business School - The Law Institute –
Copenhagen, Denmark

Georg-August Universität Göttingen - Chair for Civil Law,Intellectual Property Law, Media Law and E-Commerce –
Göttingen, Germany

Laboratorio di Scienza della Cittadinanza –
Rome, Italy

Law and Internet Foundation –
Sofia, Bulgaria

Leibniz Universität Hannover - Institute for Legal Informatics –
Hannover, Germany

Masaryk University - IT Law Work Group –
Brno, Czech Republic

Queen's University Belfast – School of Law –
Belfast, United Kingdom

Rijksuniversiteit Groningen - Faculty of Law –
Groningen, The Netherlands

Universidad de León - Department of Management and Economics –
León, Spain

Universite Paris-Sud XI - Institute of Space and Telecommunications Law –
Paris, France

University of Leiden - E-Law –
Leiden, The Netherlands

University of Malta - Centre For Communication Technology –
Msida, Malta

Univerzita Komenského v Bratislave - Faculty of Management – Bratislava,Slovakia

Uniwersytet Wroclawski - Research Centre for Legal and Economic Issues of Electronic Communication – Warsaw, Poland

Westfälische Wilhelms Universität Münster - Institute for Information-, Telecommunication- and Media Law – Münster, Germany

FUNDING SCHEME

FP7 Framework Programme for Research of the European Union - Collaborative Project: FP7-SSH-2009-A - Socio-economic sciences and Humanities – Activity 8 – SSH-2009-3.2.1. - Changes in consumption and consumer markets

DURATION

May 2010 – April 2013 (36 months).

BUDGET

EU contribution: € 2,599,570

WEBSITE

http://www. http://www.consent.law.muni.cz

FOR MORE INFORMATION

Contact: Prof. Joe Cannataci, j.a.cannataci@rug.nl
Contact: Prof. Jeanne Pia Mifsud Bonnici, g.p.mifsud.bonnici@rug.nl

FURTHER READING

Cannataci, J. & Mifsud Bonnici, JP. (eds.) (2014) Online Privacy: are we consenting to our future? Explorations in current privacy issues. *Law, Science and Technology Series*. Edizioni Scientifiche Italiane. Rome [Forthcoming][3]

Custers, BHM., Calders, T. & Schermer, BW., Zarsky, TZ. (eds.) (2013) Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. *Springer Journals*. Heidelberg, Germany

Rogosch, PM. (2013) *Die Einwilligung im Datenschutzrecht*. Nomos. Germany

[3] This volume is a collection of 18 publications relating to the CONSENT project, covering a variety of disciplines and perspectives.