DiPLO
www.diplomacy.edu

Internet Governance Capacity Building Programme

Research project summaries for EuroDIG 2011
30/31 May 2011, Belgrade, Serbia

Contents

Security risks of the social networks

Masa Kojic
Faculty of Law, University of Novi Sad, Serbia

Nowadays, we are witnessing an extreme proliferation of social networks, which can be seen as an expansion of social networks websites, but also as an increase in the number of people who are starting to use them. This phenomenon is accompanied by a number of risks that users are exposed to each time they create an account or leave information on some social network website. The problem becomes more serious bearing in mind that most of the users are not aware of these risks. This situation goes in favour of those who are willing to abuse other people's information.

Security risks of social networks can vary, but are mostly connected with the user's privacy. The term 'privacy' in this paper is used in its broadest sense, including not only the user's personal data, but also all other data concerning the user's movement, activities, likes, plans, etc.

Another important question with regard to security risks of social networks is the question of responsibility for those risks. It could be concluded that both the users and the social network providers are responsible for the user's security on the social networks. However, in order to hold somebody liable for the users' security, this liability should be proscribed and presented to the users before they start to use social network websites. Today, we have Privacy Policy rules or some other rules, but not all security risks are included in those rules. Those rules are proscribed so that social network providers can distance themselves from possible abuse, but do those rules really help users to be safe?

The issue of security on social networks is very important for the European region. Protecting communication is considered a priority for policy-makers in the EU. There are many directives on EU level which deal with security and privacy issues, but, in my view, they are not being applied in the world of social networks. I stand on the position that, in the future, there should be a legal framework concerning social networks, not only the privacy rules brought by the social networks providers. On the European Commission's website there is a section *Information Society - Thematic portal*. One of the issues which this portal deals with is the future of the Internet. The future of the Internet is strongly connected with the social networks and the security on them. It provides many opportunities, one of which is:

> ***Empowering you through networking and sharing –*** *Social networking has turned the Internet into a place where people can truly interact. This is also helpful for businesses. They can for instance take advantage of crowdsourcing to delegate a task to groups of people on the web using the mass collaboration enabled by the Web 2.0. The public may be invited to develop a new technology, carry out a design task, or help analyse large*

> *amounts of data. The outcome will be a product or service which is closer to the needs of the users and produced at lower cost for the company (European Commission, 2011a).*

Here, the question of security becomes even more important.

I believe that this issue is also connected with the Information Society Policy *Exploiting the Benefits of the Information Society* (European Commission, 2011b). Social networks are one of the benefits of the information society, but each benefit has its drawbacks, too, and if we want to increase the number of people who use these networks, we should think about the security issue the most.

References

European Commission (2011a) *A future Internet full of opportunties*. Available at: http://ec.europa.eu/information_society/activities/foi/opps/index_en.htm [11 January 2011].

European Commission (2011b) *Exploting the benefits of the Information Society*. Available at: http://ec.europa.eu/information_society/tl/policy/exploit/index_en.htm [11 January 2011].

Social media use in the workplace: how to protect employees' privacy rights while securing companies' business interests

Legal and policy issues in the European Union and suggestions for practical privacy-protective measures

Cédric Laurant
Cédric Laurant Consulting, Brussels, Belgium

General objective

This research project aims at providing companies with legal and policy information that will enable them to address the advantages and drawbacks, risks and opportunities of the use of online social networking (OSN) tools in the workplace. In particular, it will advise employers on how to improve the ways in which they can protect their business assets and confidential information, while at the same time preserve their employees' privacy.

Short description

The increasingly prevalent use of OSN sites by employees in the workplace is creating a new tension between, on the one hand, the need for companies to protect their business interests (control over their brand and reputation, confidential information, business assets, and employees' productivity) and, on the other, the increasing reliance by workers on those sites, to communicate, exchange information, make new contacts, network with new colleagues, and build new collaborative relationships. The growing use of OSN by people in the workplace is also creating new opportunities, risks, and challenges for businesses and employees. A company may be tempted to use social media to gather information about job candidates and employees. In turn, employees now access their favourite OSN sites during working hours and with company-provided equipment, making many of them less productive, or increasing the risk of information security breaches. Some interact online with colleagues after work by using their private profile, upload business-related pictures, and tag them with colleagues' names; others write status updates revealing critical business information or 'friend' business competitors. Others even create gripe profiles to criticise their employers or customers. All of those activities create new security and privacy risks for employers and employees alike.

This is why businesses may no longer ignore the OSN phenomenon, regardless of their size or sector of activity. Even if a company chooses not to engage in social media activities, it will be increasingly difficult to maintain an online presence without getting engaged in some way with them. Businesses may actually benefit from enlightened use of OSN tools to create good will, promote their brands, and interact with their customers. Being social-mediasavvy should not, however, allow those tools to gather information about job candidates and employees, or become a surveillance or tracking device in employers' hands. The latter should learn how to use social media advisedly, and a company's policy on social media use may prove to be a valuable first tool in that regard, and enable it to tackle some of the major risks of OSN.

Up to now, many companies have been left clueless about how to craft an adequate policy to use OSN tools, mostly because many specialists in the area, from social media, labour law or privacy lawyers to company CSOs, COOs or CTOs, are still learning the ropes and also because there are not many examples available from other businesses that have attempted to draft and implement one.

The good news is that, just as some centuries-old laws were interpreted to apply to the Internet, the bulk of laws and regulations that may cover the use of OSN come from rules already at our disposal. Neither in common law countries, nor in civil law countries do we necessarily need to come up with new OSN privacy laws.

One of the solutions to address the delicate balance between protecting employees' rights in the workplace on the one hand, and business performance and company interests on the other, could be found in a policy that goes beyond 'copy-pasted' boilerplate or standard clauses, and is carefully crafted to meet the business's specific needs. But it is only once companies will have learned how to interpret and apply current laws to OSN, that they will be able to draft and establish adequate social media use policies, and implement and enforce them effectively inside the organisation.

Essential elements

- **Research area:** law and policy issues surrounding the use of OSN tools and websites in the workplace by employers and employees.
- **Main research question:** can the right balance be found between protecting employees' rights in the workplace and a company's business interests, thanks to a company-tailored social media use policy and the integration of privacy-protective business workflows and practical measures?
- **Short justification** for the choice of question and the gaps in available research: industry guidelines regulating the use of OSN tools are lacking today. There is an urgent need for general guidelines intended for company's human resource managers, general counsels and other company executives. Guidelines are necessary in particular because:
    - they would diminish legal uncertainty for both employers and employees;
    - they would anticipate the need for specific legislation or rules that might be imposed by the legislator by coming up with a blueprint for future action; and
    - they would help CTOs, CSOs and COOs to review some of their business workflows and security measures so that they are designed from the very beginning to protect employees' privacy and company assets at the same time.

- **Main research objectives**
  - Draft the essential elements of a company policy that would apply to the use of OSN tools and websites in a business by employers and employees alike in order to find the right balance between protecting employees' rights and businesses' productivity, assets, confidential information and related interests.
  - Establish the practical measures that companies and their employees should adopt, i.e. privacy-protective business workflows to incorporate into their operating processes, and practical measures to incorporate into their business operations in order to protect employee privacy and preserve the security of their business assets.
- **Key audiences:** company general counsels; privacy, data protection, information security and corporate lawyers; companies' chief technology officers, chief operating officers and chief security officers; information security professionals, consultants and auditors; public policy experts and academics working in the converging fields of privacy, data protection, information security and labour law.
- **Research methodology:** research project will start with legal and policy research following a pre-defined timeline, followed by various more practice-oriented elements (online survey of professionals active in the field, interviews with general counsels and attorneys working in the area, and case studies) that will be included into the research report. A strong communication element will then follow in order to inform interested audiences (industry, government, and academic) using cutting-edge communication tools (visualisation tools, graphic design, Web 2.0 instruments (blog, online survey and polls) in various settings (academic conferences, industry conventions, government hearings, and roundtables).
- **Project outputs:** research paper including interviews, the results of an online survey, case studies, and guidelines; blog and online poll; conference presentations.
- **Evaluation:** of the impact of the research project, conference presentations, and other project outputs.

E-democracy examples: Citizens 2.0 and Gov 2.0 in Western Balkans countries

Valentina Pellizzer
OneWorld – Platform for South East Europe, Bosnia Herzegovina

How does the Western Balkans understand e-democracy? Is it a challenge or an opportunity? An obligation because of the European accession process or an internal priority?

Are governments ready to provide access to data and transparent data? Are public officers using online tools for consultation and direct communication with their citizens? Are citizens aware of what access to information and open data means? What are the challenges, the issues and the cost of e-democracy in the region? What is the role of international organisations, academia, civil society organisations, and the ICT community?

This research will provide an overview of the current status of e-democracy in four Western Balkans countries (Bosnia Herzegovina, Croatia, Montenegro, and Serbia). Based on the emerging practices, the research will deliver a case study of Gov 2.0 and Citizens 2.0 practice/service. It will provide elements for government and elected officials to communicate policy issues to the wide and diverse audience of citizens and vice versa.

The research is intended as secondary research which will start from a literature review integrated by a qualitative approach to document analysis (content analysis). Internet search will be the key for the identification of platform, tools, eservices, and websites belonging to the e-democracy space.

The literature review will focus on four countries: Bosnia Herzegovina, Croatia, Montenegro, and Serbia. Based on the findings of the literature review, two concrete e-democracy examples will be analysed for the case study.

Current studies are investing in the analysis of infrastructural investment and the necessity of building knowledge into the system; this research will show how elements of e-democracy are already present and can be used with relatively small financial investment but with a high return in terms of direct communication between citizens and politicians.

The research will offer an overview of what is going on in the area of e-democracy with reference to government but also civil society. It will help identify best practices and lessons learned that can be of help for further developments. Eventually it will open a space for dialogue and discussion among government and non-state actors. It will contribute to the popularisation of the issue and will provide information on what is happening regarding regional and national policy processes.

Open data, a European policy issue

The European policy agenda considered e-democracy as one of the key features in its i2010 policy document:

> *ICT has great potential to involve large numbers of citizens in public debate and decision-making, from municipal to European level... The interface between democracy, new technologies, new forms of social organisation and governance is what eDemocracy is about. Nevertheless, many questions and concerns still need to be addressed, from inclusion to the quality of decision-making (European Commission, 2005).*

This vision has been restated and reinforced in *The Digital Agenda for Europe* (European Commission, 2010) and mentioned the Malmö Declaration (2009) which says that:

> *European Governments are committed to making user-centric, personalised, multi-platform eGovernment services a widespread reality by 2015.*

South-eastern Europe is a larger political/policy space where Bosnia Herzegovina, Croatia, Montenegro, and Serbia are bonded together by the international community for the purpose of a transversal approach to developmental issues and the European integration process, too. All governments of the selected four countries are signatories of common initiatives in the ICT sector that explicitly refer to EU policy as the guiding policy for south-east Europe and for their own national policy.

Binding documents are the Ministerial Declarations of the eSEE Agenda+ for the development of the Information Society in south-east Europe (2007–2012) which mention e-participation and e-democracy, too.

On the other side, civil society and citizens are more aware of European policy issues for the ICT policy agenda with reference to security and control issue (biometrics passport, war on terrorism, child safety) than about policy which focus on establishing conditions to provide e-services, e-government and last but not least develop policy favourable to e-democracy, enhancing and strengthening citizens participation, access to information and transparency.

References

European Commission (2005) *I2010: A European Information Society for Growth and Employment 2005*, CEC COC (2005) 229. Available at: http://europa.eu/legislation_summaries/information_society/l24226j_en.htm [20 January 2011].

European Commission (2010) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Digital Agenda for Europe*. Brussels COM (2010) 245. Available at: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf [20 January 2011].

Internet censorship: rationale, declared purposes, tools (obvious and hidden), their efficacy and adequacy to rationale

Oksana Prykhodko
European Media Platform, Ukraine

The case of WikiLeaks clears up a lot of issues around Internet censorship - such as rationale, declared purposes, variety of tools, and their efficacy. This is good news. But now efforts to introduce censorship will be more purposeful and sophisticated. And this is bad news.

There are some countries, which admit censorship (including Internet censorship). And it's not only the worst enemies of freedom of expression, such as China, Iran, and Byelorussia. Canada, Finland, France and other countries with high democratic standards officially admit some forms of censorship. Instead in Ukraine, for example, censorship is prohibited by the constitution, but is widely used on different levels and with different purposes.

The English version of Wikipedia treats censorship as 'a suppression of speech or other communication which may be considered objectionable, harmful, sensitive, or inconvenient to the general body of people as determined by a government, media outlet, or other controlling body'. This article also provides us with five rationale for censorship - moral, military, political, religious, and corporate – and nine types of censorship – political, state secrets and prevention of attention, educational sources, music and popular culture, copy/picture/writer approval, maps, meta censorship, creative censorship, and Internet (Wikipedia, 2011).

The time of overenthusiastic perception of the Internet as censorship-free area is over, and now numerous researchers have revealed many examples of Internet censorship. It is easy to justify the blocking or filtering of child pornography, in contrast to political censorship. Methods of Internet censorship also differ: from that recommended by the Council of Europe's filtering of illegal and harmful content by Internet service providers (ISPs) to China's Great Firewall. So, how do we secure a safe Internet without infringing on freedom of expression? How can we balance the interests of different stakeholders on Internet censorship issues? And, generally speaking, what are their interests? Who has to take responsibility for Internet censorship? The proposed policy research can help to answer these questions.

Objectives

- Analyse attention of Ukrainian society towards different forms of Internet content regulation.
- Reveal examples of hidden or unlawful Internet censorship in Ukraine.
- Fulfil trustworthy polls of all stakeholders (legislators, lawyers, regulators, ISPs, media experts, journalists, educators, social media activists, human rights activists).

- Define ‘ceiling’ for governmental interference and ‘floor’ for self-regulation.
- Elaborate clear standards of admissibility and inadmissibility in Internet regulation.
- Work out practice policy recommendations to balance a safer Internet with freedom of speech.
- Raise awareness and to lobby this new policy.

Key audiences

Legislators, lawyers, judges, media experts, journalists, social media activists, human rights activists, Internet users, youth (digital natives).

Methodology

After reviewing the literature and analysing existing Ukrainian legislation in this sphere, it is necessary to work out some sets of questionnaires for different multistakeholders. A representative poll for Internet users and the Ukrainian community at large must be based on more general questions, while questions for ISPs and law enforcement officers should be more specific.

The main purpose of these questionnaires is to reveal the differences and commonality in the attention of different stakeholders to Internet content regulation. More clarity in understanding genuine and declared rationale of censorship, as well as understanding different tools of censorship will help to guarantee a safer Internet without impinging on free speech.

References

Wikipedia (2011) *Censorship*. Available at: http://en.wikipedia.org/wiki/Censorship [11 January 2011].

E-participation in decision-making: the *Europa.eu* model

Roxana Georgiana Radu
Center for Media and Communication Studies, Central European University, Budapest, Hungary

Executive summary

Civic online participation garnered much interest during the last few decades relative to the transformation of the concept of democracy in a move from representative to participatory. Reshaping public administration to deliver qualitative, less bureaucratic, and more effective services has also been on the agenda of governments worldwide for the past decade. Moreover, the types of online opportunities for citizen empowerment have diversified tremendously with the advancement of ICT, while their number has increased substantially. This has been complemented by easier access to new technologies and a diminished digital gap between developed and developing countries. Standing at the crossroads of politics, public policy, and ICT evolution, the present study undertakes an original stance in the research of online empowerment mechanisms and their challenges by employing an interdisciplinary approach aimed to cover both theoretical and practical aspects.

The present proposal investigates the mechanisms enabling participation in policy shaping at the level of the European Union (EU) via the portal Europa.eu, a one-stop shop not only for obtaining information, but also for enabling civic empowerment. The age of 'pseudo-participation' (Verba, 1961), meant to create the feeling that participation is possible, was said to have come to an end when digital platforms allowed for active engagement and offered increased opportunities for facilitated consultation and deliberation. Full participation, defined as 'a process where each individual member of a decision-making body has equal power to determine the outcome of decisions' (Pateman, 1972), became one of the guiding principles of interactive platforms such as *Europa.eu.* From a similar point of view, Macintosh *et al.* (2002) explored the citizens' role in setting the agenda for policy-making, but emphasized their move from consumers of policies and top-down decisions to their emergence as producers of information and policy initiators.

By examining the extent to which it allows for extensive engagement of citizens in decision-making, this study will inform both current and future policy-makers in Brussels, as well as in the 27 EU member states about the degree of interactivity and public outreach that is provided in the *Europa.eu* framework. Additionally, it aims to provide recommendations for further improvements, while taking into account the specificities of the multilevel governance model. By focusing on citizen participation in deliberations mediated by the use of information and communication technology (ICT) in a transnational environment, it will provide an analytical framework and empirical evidence for comparing the latest developments in the EU

to inform citizens, policy-makers, and analysts about the current approaches towards e-participation by taking into account the degree of interactivity and public outreach it enables.

Since the creation of *Europa.eu* in 2004, the paradigm shifts occurring in the digital era have influenced all aspects of e-government. However, this long-term impact has remained under-studied. The present study aims at addressing this in a comprehensive manner and analysing in depth the constraints emerging from electronic participation and the degree to which citizens are interested in using online communications as a means for making their opinions heard. Consequently, the research question to be explored here is: To what extent is *Europa.eu* enhancing real e-participation? This question stems from the need for assessing the impact of a single-point of access for 27 EU member states and its effective service delivery. Additionally, it aims to take into account the civic participation in decision-making that goes beyond what websites enable by default. A mix of qualitative and quantitative methods will be employed for revealing the complexity of these dynamics. The methodology relies on a score for interactivity – as a measure of ownership transparent information, reachability, and timely responses – and another score for public outreach, which comprises foreign language translation, the presence of search engines, the existence of privacy and security policies, and the availability of e-petitioning. Upon the availability of data, an assessment of participation on *Europa.eu* (number of users, most requested services, frequently asked questions, rate of involvement in policy deliberations, participation in online surveys, e-citizen profiles) may be considered. The evaluation of the current EU strategy for enhancing civic empowerment by online means will provide additional information for what can be followed in a different pattern of implementation. Moreover, it would allow for an informed decision as to whether there are aspects that need to be modified within the current functioning of the *Europa.eu* portal.

The practical relevance of this endeavour consists in shedding light on the extent of civic engagement at the highest level of decision-making by taking into account the stimuli and the constraints in effective online participation throughout Europe. Accordingly, different policy recommendations and facilitation mechanisms will be considered when evaluating the real challenges behind a more inclusive e-governance project, as well as the barriers in terms of its efficient implementation. These would be based, prima facie, on the most influential factors affecting the e-citizens' willingness to become meaningfully involved and the perceived benefits of online engagement.

References

Macintosh A *et al.* (2002) *Technology to support participatory democracy*. In Gronlund A (ed.), *Electronic Government: Design, Applications and Management*. Umea University, Sweden: Idea Group Publishing

Pateman C (1972) *Participation and democratic theory*, Cambridge: Cambridge University Press, p. 70–71.

Verba S **(**1961**)** *Small groups and political behavior***.** Princeton: Princeton University Press, p. 220.

From conflict to cooperation in cyberspace: the case of the Western Balkans

Ana Rankovic
NGO Fractal, Belgrade, Serbia

The team and organisation that I have the pleasure to work with, NGO Fractal, has as its mission: *Improvement of communication, trust and cooperation of people with different backgrounds*. This mission is especially challenging in ethnically divided and post-conflict contexts, where social complexity and behavioural options are often limited and where confidence-building initiatives take place against the scenery of continuous tensions and adversarial positions.

With a recent past marked by nationalism, division, and violence, a common opinion is whether this can be transcended with the EU integration process, as it provides a common ground and a shared objective in the region. However, despite the existing cooperation-facilitating framework, cooperation in the Western Balkans remains challenging and weak. There are divisive lines between different ethnicities, backed up by negative stereotypes of the 'other' side, mutual misunderstanding, distrust, unwillingness to meet 'the others', and often a lack of channels for enabling connections between ethnic groups.

Cyberspace provides a valuable environment for meetings and interaction, enabling a diversity of modes of engagement. It can help build sustainable peace (UN ICT Taskforce, 2005) but as well provide an avenue for different forms of cyber-attacks and conflicts.

The focus of this research will be ethnically motivated cyber-attacks, or cyber-attacks carried out for ideological purposes, to support causes of one ethnic community, directed towards (members of) another ethnic community, by disrupting normal operation in cyberspace.

To best of my knowledge, ethnically motivated cyber-attacks in the Western Balkans region have been relatively low in number, scope, or impact; they have mostly included small to mid-scale denial of service (DOS) attacks and simple website defacement where the hacker/hacktivist infiltrates the site leaving behind graffiti – a message – throughout the site or on the main page. Although, this is not considered a particularly sophisticated activity within the larger range of hacking actions (Carr, 2009), even when the actual attack has little operational impact it can quickly gain the attention of the media and create a more significant impact. Furthermore, with shared commitment for eSEE Agenda (Regional Cooperation Council, 2011) in the region and gradual progress in digitisation, increasing dependence on ICT infrastructure will also increase vulnerabilities.

Since very little is known, I am interested in exploring what kind of measures if any, are undertaken to prevent or mitigate effects of ethnically motivated cyber-attacks on national and regional level, and how in turn this relates to a level of trust, sharing, and cooperation between countries in the region. Or, is the current framework for cybersecurity cooperation in the Western Balkans helping build confidence among different communities in the region?

The scope of this study does not include exploration of roots and causes of conflict and inter-ethnic distance in the Western Balkans region. Rather, the goal of this research is to examine how existing the legal and regulatory framework responds to ethnically motivated cyber-attacks, and whether anticipated cybersecurity risks and challenges, given their complexity and interdependency, serve as an incentive for countries in the region to identify common interests and concerns, and to engage and enhance cross-border cooperation. To do so, the following issues will be explored:

- Ethnically motivated cyber-attacks. Skype, frequency and impact of ethnically motivated cyber-attacks in Western Balkans. State and non-state actors response (Nye, 2010). Experiences and lessons learned from other post-conflict regions in cybersecurity.
- Passive or active defence (Carr, 2009). Transparency level of cybersecurity programme (Nojeim, 2010). Public support?
- Is regional cooperation in cybersecurity perceived as a risk, opportunity or challenge in countries of the Western Balkans? Common concerns and expectations in terms of cybersecurity. Incentives and constraints for cooperation.
- The relationship with EU policies and activities (Cornish, 2008)? Other cybersecurity cooperation frameworks.
- Tension between anonymity and security. Privacy and surveillance.
- ICT and peace-building. Cybersecurity and conflict transformation.

This research will examine cybersecurity and ethnically motivated cyber-attacks, focusing on the Western Balkans region as a post-conflict area with increasing interest in cybersecurity. The research will be conducted in three parts:

1. An examination of the type, frequency, perceptions and effects of ethnically motivated cyber-attacks; a review of measures and responses to ethnically motivated cyber-security challenges in each respective country of the region; similarities and differences.
2. A review of regional cooperation, procedures and agreements; also other multilateral initiatives to address cybersecurity.
3. A final paper with recommendations, based on findings and information collected in Parts 1 and 2 and further discussed with peace activists and conflict transformation CSOs in the region.

References

Carr J (2009) *Inside cyber warfare: Mapping the cyber underworld*. Available at: http://books.google.com/books?id=ip9bVYm64vQC&lpg=PA109&ots=zPDTAFtkUL&dq=jeffrey%20carr%20google%20books&pg=PA109#v=onepage&q&f=false [14 November 2010].

Cornish P (2009) *Cyber security and politically, socially and religiously motivated cyberattacks.* Available at: http://www.europarl.europa.eu/activities/committees/studies.do?language=EN [14 November 2010].

Nojeim G (2010) Cyber-security and freedom on the Internet. *Journal of National Security, Law and Policy* **4**(1). Available at: http://jnslp.com/read/vol4no1.asp [14 November 2010].

Nye J (2010) *Cyber-Power.* Available at: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf [14 November, 2010].

Regional Cooperation Council (2011) *Agenda for the Development of the Information Society.* Available at: http://www.eseeinitiative.org/ [12 January 2011].

United Nations ICT Task Force (2005) *ICT4Peace*. Available at: http://old.ict4peace.org/articles/ict4peace_ebook1.pdf [14 November, 2010].

Introducing child safety in the Romanian school curriculum

Alexandra Vasile
'Dimitrie Cantemir' Christian University, Romania

At the present time, the only existing policy in Romania that is specifically dedicated to children concerns the prevention and eradication of child pornography (a law passed in 2003). While this is an excellent start, it does not cover the existing policy needs: as technology develops and more and more children spend time online, they are exposed to numerous threats, dangers, and potential abuse. In order to ensure that children have a positive and enriching online experience, we must not only focus on recommendations that cater to the children during their online activities (such as software that filters content), but also on preparing them before they go online and when problems arise (sometimes after they are online). Children need to learn how to behave online, how to critically assess their activities online, and how to act accordingly. That is why introducing a policy in this sense would involve introducing an initiative which encourages being smart online and being prepared to surf the Internet and avoid its dangers.

Implementing such a policy initiative would involve four aspects:

1. Dedicating space in the school curriculum for online safety education.
2. Training teachers in how to teach the curriculum.
3. Finding funding for this supplementary education.
4. Encouraging initiatives that have educating children about safety online as their main goal.

Up until now, a number of initiatives that deal with child safety online have either taken place (or are still taking place) in Romania. They have mostly been organized by Save the Children Romania, in partnership with various organisations. On a European level, an initiative that is connected to child safety online and Romania is Memo/10/200, put forward by the European Commission 19 May 2010. It draws out the plan for a so-called European Digital Agenda. Its purpose is to ensure that the EU is making full use of ITC in order to form the basis of a sustainable digital future. In essence, the Agenda identifies the aspects that the EU needs to focus in the future. Online safety ranks high on the list of the priority areas on the Agenda. However, the only mention of how this will be accomplished is the suggestion of collaboration between EU countries in order to organise courses in online safety (Memo/10/200).

It is obvious from looking at the existing initiatives that they are disjointed, and lack clear focus and organisation. Current efforts are weak and dispersed: not all schools or educational institutions are being offered courses in child safety online. In terms of the proposal put forth by the European Commission as part of the Digital Agenda (in Memo/10/199 and Memo/10/200), while the ideas are good in theory, it will be very difficult to put them in practice in a timely manner. Because the EU is formed of countries with their own individual style of teaching and educational systems, implementing a uniform system of teaching online safety across all countries without having a deep and sound knowledge of how child safety online is tackled throughout the European Union would be extremely difficult.

While some research in the field of child safety online exists in Romania, it is mostly reduced to short articles or newspaper pieces that lack depth when analyzing a specific issue. That is why this research project centred on introducing online safety training in the formal education system that would provide both the breadth and the depth necessary to create a basis for future, more extensive, scholarly work related to child safety online in Romania, especially in conjunction with educational tools and methods.

In this context, the research *Introducing Child Safety in the Romanian School Curriculum,* has four main objectives.

1. Research the need to introduce online safety in the Romanian primary and secondary school curriculum.
2. Analyse what methods could be employed for training teachers in delivering course content on the topic of online safety.
3. Assess how such a curriculum can be developed in Romania, given the current structure and content of the syllabus.
4. Identify, use and promote best practices from other European Union countries in order to improve the Romanian school curriculum in terms of online safety.

The research project will benefit from a three-pronged methodological approach. It will include:

1. questionnaires that will be administered to a diverse sample of children, parents, and teachers in order to assess their awareness of the dangers of child safety online;
2. focus groups with randomly chosen parents and teachers, in order to explore how they believe the introduction of safety notions should be implemented in schools and what the safety curriculum should contain in terms of knowledge useful for children; and
3. examples of other European Union countries' best practices and initiatives in the area of integrating safety in the school curriculum which will be taken into consideration, in order to analyse how these countries trained the teachers, developed the curriculum, and shaped the content and structure of the classes themselves.

All three research methods complement one another, and they each add a new layer of information and depth of knowledge to the data that will be collected.

As stated before, the ultimate goal of the *Introducing Child Safety in the Romanian School Curriculum* research project is to look at the need for the introduction of child safety online as a component in the school curriculum, but also – in a larger sense – to also look at best practices in other countries, to learn from their experience but also from their past mistakes, so that European countries will not make efforts towards 'reinventing the wheel' and will –hopefully – at some point in the future look at reaching a common ground, a common set of rules that govern child safety online throughout the European Union.

Use of social media and Web 2.0 technologies to increase participation and engagement in Internet policy forums

Filiz Yilmaz
ICANN

Executive summary

This proposed study aims to explore Social Media and Web 2.0 technologies to discuss their usage and effectiveness in facilitating participation and engagement in Internet policy-making forums.

Internet policy-making forums have a multistakeholder profile. These stakeholders are numerous and diverse and include academia, governments, law enforcement agencies, civil society groups, technical community mostly serving in private sector and sometimes even regular citizens who feel that they have a say and interest in Internet and ICT policies. Getting feedback from such diverse groups on a particular policy issue in development or informing them about a concluded decision is often a mission.

One common denominator among these various stakeholders is that they often follow technological developments and Internet happenings, as these have a natural effect on Internet policy, too, or simply this is their core interest area. Nowadays there is a trend in the use of social media and Web 2.0 technologies. These tools have been developing tremendously recently and they have been proven to be popular among those people who are involved with Internet and so among those who are also involved with the development of Internet policy.

Various Internet communities today deploy bottom-up and transparent policy-making or development processes. The idea is that their multistakeholder communities contribute and participate in these processes to reach consensus on specific policy issues. Such processes can be time-consuming by nature. So far, these processes have been heavily supported by mailing lists or forums as means of main participation tools, which can be defined as ‘passive’, heavily depending on actions from the user. This does not help the processes in their efficiency in time. Social media and Web 2.0 technologies, on the other hand, seem to be instant and active compared to these conventional feedback collection and information dissemination tools.

Web 2.0 and social media tools are today bringing masses of people with similar interests together, enhancing their engagement and collaboration. Furthermore, Web 2.0 technologies especially are bringing their inherent collaboration aspect and this key point raises the question if such tools could fit into the policy-making environment where transparency, collaboration, and participation are essential.

Accordingly, the main questions in this proposed research are whether Web 2.0 and social media tools can also be used to facilitate participation and engagement of these various

stakeholders in Internet policy-making forums in a way that information dissemination and/or policy discussions are realised via these tools and even further whether they can replace the current main tools such as e-mail lists or forums to collect public comment or to promote participation and engagement to these processes. If they can be used as the main tools in such policy development processes, a further question is how their effectiveness or success can be measured.

If these questions about these new tools can be answered positively, the policy-making and development processes will benefit in effectively collecting feedback from their various groups as well as later on reaching them out to inform them about the developments.

The final result can be beneficial for both the feedback collecting body and the stakeholders who conveyed feedback as these tools seem to be easy to use and well-deployed, having a factor of fast spread of information.

Within a European context, there are several policy-making processes that could also consider usage of social media and Web 2.0 technologies. The European Commission today is very active in following various Internet policy-related forums such as IGF, ISOC, ICANN, and RIRs, as well as seeking input for various other topics. Some of the European governments and regulators are also looking into ways of deploying processes where they can receive public comment on policy issues more effectively. These may or may not be directly related to Internet policy but there are similarities in how the processes and usage of social media and Web 2.0 technologies can be adopted in national or regional policy-making processes where feedback collection, contribution, collaboration, and participation by various stakeholders are anticipated within the process. Furthermore, this study can be relevant to those institutions that are also considering concepts like e-government, Government 2.0 and Open Government.

Broad objectives of the proposed study

- Find out how Web 2.0 Technologies and social media can be used in an Internet policy-making or development environment with multistakeholders.
- Identify examples of such environments or forums that (could) deploy these technologies.
- Discover whether these tools can be used to collect feedback or should their role be more towards the direction of increasing participation and engagement. In either case, which example case studies can be produced?
- Assess/monitor their effectiveness.