REGULATION AND SELF-REGULATION OF ONLINE ACTIVITY

BLOGS AND ELECTRONIC SOCIAL MEDIA

Spiros Tassis

21/5/2011

Fourth International Conference on Information Law and Ethics

Thessaloniki, May 20-21, 2011

Contents

1. Regulating online behavior – Is it of any use? 2

a. Do we need regulation? 2

b. How much regulation? 5

c. Basic Regulation in EU affecting online social networks and blogging. 6

d. Main elements of the new reform (valid from 25 of May 2011): 7

2. Self Regulation 10

a. What is Self-regulation? 10

b. Is Self-regulation effective? 11

c. Terms of Use (or Terms and Conditions) as self-regulation schemes 13

d. Is self-regulation still an option? 17

Conclusions 18

1. Regulating online behavior – Is it of any use?

a. Do we need regulation?

Some years ago I was asked, which is the best way to preserve freedom of speech in Internet and my answer was … self regulation!

Indeed is common knowledge that freedom in online activity is a fundamental issue and as big as the governance of the online resources[1]. The typical reaction is that Internet must be free and open[2]. Everybody agrees this this is, probably, the last (virtual) space where everybody is able to freely express himself and many are those who actively defend this option.

The motto from the early period was going like this:
«Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather[3]».

What is defined, though, as regulation? Regulation is a rule, principle, or condition that governs certain procedures or behavior and in most of the times it

[1] For a list of methods to oppress freedom of online speech see a relevant report by the "Committee to Protect Journalists" http://www.cpj.org/reports/2011/05/the-10-tools-of-online-oppressors.php.

[2] *There are hundreds of organizations declaring that Internet means freedom of speech. As most of them say "There is no freedom of information without* Internet freedom".

[3] John Perry Barlow: «A Declaration of the Independence of Cyberspace». 1996. American poet, founder of the EFF and activist for the freedom of speech in Internet. He introduced the term "cyberlibertarian".

is generated by the legislative authorities such as the parliament, the respective ministry or the relevant NRA. This intervention is formed to rules and limits in rendering or/and using the relevant sources (both scarce and not) and services. Thus, the regulation turns to form at least a base line of rules for any online activity.

But do we, really, need any specific regulation for online activity or should we leave the stakeholders alone to form the rules of this "sui generis" environment? The traditional legal texts are not just enough?

Studies say that only in EU more than 107 million users will be active in online social networks by year 2012. The relevant risks are enormous[4]:

1. ***No oblivion on the Internet:*** **The notion of oblivion does not exist on the Internet.** Data, once published, may stay there literally forever - even when the data subject has deleted them.
2. ***The misleading notion of "community":*** Many service providers claim that they are bringing communication structures from the "real" world into cyberspace.
3. **"*Free of charge" may in fact not be "for free*"**, when users of many social network services in fact "pay" through secondary use of their personal profile data by the service providers, e.g. for (targeted) marketing.
4. ***Traffic data collection by social network service providers***, who are technically capable of recording every single move a user makes on their site; eventually sharing of personal (traffic) data (including users' IP-addresses which can in some cases also resemble location data) with third parties (e.g. for advertising or even targeted advertising) and law enforcement agencies with less protection than in the country of origin.

[4] As categorized by the "International Working Group on Data Protection in Telecommunications" in its published "Report and Guidance on Privacy in Social Network Services - "Rome Memorandum" - 43rd meeting, 3-4 March 2008, Rome (Italy)". The Working Group consists of representatives from the national data protection su-pervisory authorities and from international data protection organisations, as well as of independent scientists, representatives from industry and other specialists in privacy and telecommunications.

5. ***The growing need to refinance services and to make profits*** *may further spur the collection, processing and use of user data*, when they are the only real asset of social network providers. Social network sites are not – while the term "social" may suggest otherwise – public utilities but are run by major international players entering the market need to create and maximize profits.

6. ***Giving away more personal information than you think you do****:* For example, photos may become universal biometric identifiers within a network and even across networks. Furthermore, "social graph" functionalities popular with many social network services do reveal data about the relationships between different users.

7. ***Misuse of profile data by third parties***: This is probably the most important threat potential for personal data contained in user profiles of social network services together with the hijacking of profiles by unauthorized third parties (id theft).

8. ***Use of a notoriously insecure infrastructure****:* These incidents include well-known service providers like Facebook, flickr, MySpace, Orkut and the German provider "StudiVZ".

9. ***Existing unsolved security problems of Internet services*** A recent position paper by the European Network and Information Security Agency (ENISA) inter alia lists SPAM, cross site scripting, viruses and worms, spear-phishing and social network-specific phishing, infiltration of networks, profile-squatting and reputation slander through ID theft, stalking, bullying, and corporate espionage (i.e. social engineering attacks using social network services). According to ENISA, "social network aggregators" pose an additional security threat.

10. ***The introduction of interoperability standards and application programming interfaces*** (API; e.g. "open social" introduced by Google in November 2007) to make different social network services technically interoperable entails additional new risks: They allow for automatic evaluation of all social networks websites implementing this standard.

In all the above we should add the persistent effort to minimize privacy in online activity pushed by several governmental agencies across the world, which impose pro-active control of all data, aiming to control and check information that may relate to potential criminal behavior or terrorism and, of course, the notion of monitoring the employee's use of online services (such as the electronic social networks) during working hours[5].

These efforts mean two things: first, we do need specific regulation for electronic communications and second, regulation is not always depressing the freedom of speech. On the contrary, the appropriate regulation, very often helps users avoid serious risks and hazards to our privacy and other fundamental rights. The enemy of proportional regulation is … over-regulation of online activity. Proportional regulation of online activity should result to protecting online privacy and promoting net neutrality.

b. How much regulation?

Regulation should intervene where users should be protected, not only from the government or the big companies but also from other users who misuse internet. That means regulation relevant to activities that creates a big public interest (as e.g. the online gambling, e-commerce, online financial services and protection of minors) is usually welcome and accepted - as soon it stays within the limits of respect for the human rights. On the other hand any regulation aiming to protect an indefinite "public interest" or from generic social groups seen as "public enemies" is being treated with suspicion, because it simply leads to more surveillance and less privacy and overall to

[5] http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf.

less respect to fundamental civil rights. This regulation often remains ineffective in practice.

c. Basic Regulation in EU affecting online social networks and blogging.

- **1987**: Commission Green Paper on the development of a common market for telecommunications services.
- **2002**: EU agrees need for new regulatory package (Telecommunications Framework 2002)
- **2007**: Commission presents a new telecoms 'package' of reforms
- **2009**: A new framework for the electronic communications is created (Electronic Communications Framework 2009)

  The existing 2002 regulatory framework for electronic communications networks and services in the European Union is comprised by five directives, which altogether are referred to as "the Framework Directive and the Specific Directives". More specifically these directives are: (a) Directive 2002/19/EC of the European Parliament on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), (b) Directive 2002/20/EC of the European Parliament on the authorisation of electronic communications networks and services (Authorisation Directive), (c) Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), (d) Directive 2002/22/EC (Universal Service Directive), and finally, (e) Directive 2002/58/EC (Directive on privacy and electronic communications). Directives 2002/22/EC and 2002/58/EC were amended by Directive 2009/136/EC and Directives 2002/19/EC, 2002/20/EC and 2002/21/EC were amended by Directive 2009/140/EC.

d. Main elements of the new reform (valid from 25 of May 2011)[6]:

Protecting citizens' rights relating to internet access by a new internet freedom provision: Following the strong request of the European Parliament, and after long negotiations on this point, the new telecoms rules, in a new Internet freedom provision, now explicitly state that any measures taken by Member States regarding access to or use of services and applications through telecoms networks must respect the fundamental rights and freedoms of citizens, as they are guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and in general principles of EU law. Such measures must also be appropriate, proportionate and necessary within a democratic society. In particular, they must respect the presumption of innocence and the right to privacy. With regard to any measures of Member States taken on their Internet access (e.g. to fight child pornography or other illegal activities), citizens in the EU are entitled to a prior fair and impartial procedure, including the right to be heard, and they have a right to an effective and timely judicial review.

New guarantees for an open and more "neutral" net (Net Neutrality): Another way to hinder freedom of speech and access on certain online social networks and non-friendly bloggers is the management of the internet sources in a way to limit bandwidth capacity or direct users to friendly services. The European Commission has repeatedly declared that it "will not put the achievement of the open internet at risk. Everyone in the EU should have the chance to enjoy the benefits of an open and neutral internet, without hidden restrictions or slower speeds than they have been promised"[7]. The new telecoms rules, according to the E. Commission, will ensure that European consumers have an ever greater choice of competing broadband service providers. Internet service providers have powerful tools

[6] http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm

[7] Neelie Kroes European Commission Vice-President for the Digital Agenda The internet belongs to all of us Press conference on Net Neutrality Communication Brussels, 19th April 2011.

at their disposal that allow them to differentiate between the various data transmissions on the internet, such as voice or 'peer-to-peer' communication. That is why, under the new EU rules, national telecoms authorities will have the powers to set minimum quality levels for network transmission services so as to promote "net neutrality" and "net freedoms" for European citizens. In addition, thanks to new transparency requirements, consumers must be informed – before signing a contract – about the nature of the service to which they are subscribing, including traffic management techniques and their impact on service quality, as well as any other limitations (such as bandwidth caps or available connection speed). This is a good example on how the Internet's economics (antitrust and unfair competition practices) may be helpful (even sideways) in supporting freedom and privacy.

Consumer protection against personal data breaches and spam: European citizens' privacy is a priority of the new telecoms rules. Names, email addresses and bank account information of the customers of telecoms and internet service providers, and especially the data about every phone call and internet session, need to be kept safe from accidentally or deliberately ending up in the wrong hands. Operators must respond to the responsibility that comes with processing and storing this information. Therefore, the new rules introduce mandatory notifications for personal data breaches – the first law of its kind in Europe. This means that communications providers will be obliged to inform the authorities and their customers about security breaches affecting their personal data. This will increase the incentives for better protection of personal data by providers of communications networks and services.

In addition, the rules concerning privacy and data protection are strengthened, e.g. on the use of "cookies" and similar devices. Internet users will be better informed about cookies and about what happens to their personal data, and they will find it easier to exercise control over their

personal information in practice. Furthermore, internet service providers will also gain the right to protect their business and their customers through legal action against spammers. The new EU Directive 2009/136/EC regarding the use of 'cookies' is imposing strict rules on website providers on the way in which cookies are used. According to this Directive website providers will need to receive explicit consent from users in order to store cookies on website users' devices so that the website can recognize the user's device in future. But as it became obvious the member states were not so enthusiastic about implementing these new stricter rules.

All these new elements try provide a more secure environment for users of the online social networks and the bloggers and at the same time try to motivate fair competition among the operators of these services. "Europe's competition frameworks and the EU Directives for electronic communications already guarantee the openness of the Internet and transparency for consumers while recognizing the need for innovation in networks and business models. With the fast increase in data traffic over fixed and mobile network, smart management of networks is essential for offering service quality to all end-users and for developing new innovative services"[8].

Two steps ahead and one beyond: On the other hand Europe recently introduced a really problematic directive regarding obligatory data retention. This new Directive (2006/24/EC) gave to many governments the opportunity to impose more privacy-free legislation as the French Government which recently defined data that must be retained "at the transmission or modification of online content, by the hosting companies, including video sharing and blog hosting services allowing for the identification of any person having contributed to the creation of online content". In Greece the said

[8] Luigi Gambardella, ETNO Executive Board Chairman (http://pr.euractiv.com/press-release/open-internet-maintaining-openness-internet-and-supporting-new-and-innovative-business).

Directive combined with the interpretation by the public prosecutor of Supreme Court that the external data of communications should not be treated as confidential as the content of the communication has led to a significant increase of the police's demand for disclosure of internet related data from the operators.

2. Self Regulation

Regulation can cover many aspects of the online activity but it sets only the basic principles. The details of each online service and community must be respected by all stakeholders through a self-restriction scheme.

a. What is Self-regulation?

By self-regulation we define "when industry administers and enforces its own solution to address a particular issue without formal oversight or participation of the regulator or government. In particular, there is no *ex ante,* legal backstop in a self-regulatory scheme to act as the ultimate guarantor of enforcement"[9]. Self-regulation or self-restriction is the voluntary acceptance by all stakeholders to respect a series of norms agreed specifically for a certain online activity.

More often the self-regulation rules are set by the operator of an internet service, thus the main forms of self-regulation are the Code of Conduct and the Terms of Use. Both instruments rely on the user's good intentions to respect them and its fair use of the respective services.

[Self-regulation has also been promoted and encouraged by the legislators such as the EU through several Recommendations issued:

- Recommendation (2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new

[9] As defined by Ofcom at www.ofcom.org.uk

communications and information services) which strongly suggests the creation of principles and mechanisms concerning self-regulation and user protection against illegal or harmful content on new communications and information services by establishing Self-regulatory organizations, Content descriptors, Content selection tools, Content complaints systems, Mediation and arbitration procedures, and securing user information and awareness.

- Recommendation 2006/952/EC which calls for a further step to be taken towards establishing effective cooperation between the Member States, the industry and other interested parties as regards the protection of minors and human dignity in the broadcasting and Internet services sectors. It supplements Council Recommendation 98/560/EC on the same subject, taking into account recent technological developments and the changing media landscape.]

b. Is Self-regulation effective?

Self-regulation was always the preferred method of online activity governance. It started at the mid 90's as the preferred mean of setting rules for online activity and from the very beginning became apparent that if some basic rules could not followed the self-regulation schemes would not be able to lead to an open and fair virtual world. But it is not easy to find out how effective it is unless it is tested for many years and within a certain cultural and economic environment.

Bertelsmann Foundation gave a clear answer on this question: "For a public response of **Self-regulation of Internet content** to be effective, it must be integrated, systematic and dynamic, sensitive to public needs and national differences within a framework that encourages robust communication. Only such a systematic approach – bringing technological potential together with the energies and capacities of government, the Internet industry and the

citizenry – has the promise of success in meeting what often seem to be competing goals. Given the global and borderless architecture of the Internet, such a systematic approach requires not only coordination at a national and regional level, but its scope must be international. Codes of conduct should be adopted to ensure that Internet content and service providers act in accord with principles of social responsibility. These codes should meet community concerns and operate as an accountability system that guarantees a high level of credibility and quality. As part of the codes of conduct, Internet providers hosting content have an obligation to remove illegal content when put on notice that such content exists. The procedure for such notice and take-down – while laid down by regulation – should be reflected in codes of conduct and should specify the requirements for proper notification of service providers"[10].

More than 15 years after we are in position to tell that as long the technology is progressing and the online business is flourishing, the internet is turning to a real battlefield for financial wars, where the self-regulation schemes turned to be inadequate and very often misused. "The concept of self-regulation is now being used in a way that extends far beyond its initial meaning to cover activities that are neither "self-" nor "regulation" but devolved enforcement, surveillance and extra-judicial punishment of allegedly illegal activities"[11].

On the other hand it is true that being self-restricted when it comes to privacy may deteriorate your position in the market. "It costs to be proactive on privacy. Companies concerned with privacy may turn away from business practices their less principled competitors jump at, or devote significant resources to supporting self-regulatory or technical programs. Regulatory actions (self or statutory) are not cheap. The cost of privacy when placed in

[10] Self-regulation of Internet Content, Bertelsmann Foundation, Gütersloh 1999

[11] EDRI "The slide form self regulation to corporate censorship" (http://www.edri.org/files/EDRI_selfreg_final_20110124.pdf).

the broader context of user satisfaction, fraud reduction, and user confidence in the Web is worthwhile, however the cost is uncertain and poorly distributed"[12].

c. Terms of Use (or Terms and Conditions) as self-regulation schemes

Online social networks and blogging services providers have implemented the majority of the regulatory principles in their terms of use. As a user you cannot join in without have agreed to these terms and conditions which are a take-it-or-leave-it legal document.

"One cannot go online today without eventually being asked to accept a set of so-called Terms of Service (or TOS). These "terms" are actually purported legal contracts between the user and the online service provider despite the fact that users never get a chance to negotiate their contents and can often be entirely unaware of their existence. In the unregulated and unpredictable world of the Internet, such arrangements often provide the necessary ground rules for how various online services should be used. Yet TOS agreements also raise a number of concerns for the consumer, as they can be a vehicle for abuse by online service providers, as they tend to end up being one-sided in the service provider's favor, and are often designed to be beyond any judicial scrutiny[13].

- Users of "blogger.com" are obliged to accept several terms regarding fair use of the service: **"**Proper Use … the user agrees that he will use the Service in compliance with all applicable local, state, national, and

[12] *Joseph M. Reagle Jr.* reagle@mit.edu*, Resident Fellow, Berkman Center for Internet & Society, Harvard Law School,* http://cyber.law.harvard.edu/archived_content/people/reagle/privacy-selfreg.html

[13] https://www.eff.org/issues/terms-of-abuse

international laws, rules and regulations, including any laws regarding the transmission of technical data exported from your country of residence and all United States export control laws … By their very nature, Blogger.com and Blogspot.com may carry offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are otherwise deceptive. We expect that you will use caution and common sense and exercise proper judgment when using Blogger.com and Blogspot.com.

Google does not endorse, support, represent or guarantee the truthfulness, accuracy, or reliability of any communications posted via the Service or endorses any opinions expressed via the Service. You acknowledge that any reliance on material posted via the Service will be at your own risk.

Content Boundaries means that no adult content is allowed on Blogger, including images or videos that contain nudity or sexual activity and that Blogger has a zero tolerance policy towards content that exploits children. In addition other content not allowed is Hate Speech, Crude Content, Violence, Copyright infringement, disclosure of Personal and confidential information especially when these belongs to third parties, Impersonating others, Illegal activities (for example, encouraging people to drink and drive), Spam, Malware and viruses."

- Facebook declares and obliges users to declare, among others, that:

- "You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.
- We can remove any content or information you post on Facebook if we believe that it violates this Statement.

- If we remove your content for infringing someone else's copyright, and you believe we removed it by mistake, we will provide you with an opportunity to appeal.
- If you repeatedly infringe other people's intellectual property rights, we will disable your account when appropriate.
- If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.
- You will not post anyone's identification documents or sensitive financial information on Facebook.
- You will not tag users or send email invitations to non-users without their consent.
- You will not send or otherwise post unauthorized commercial communications (such as spam) on Facebook.
- You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our permission.
- You will not bully, intimidate, or harass any user.
- You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
- You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory".

Now, seriously, does anyone believe that all users of these services do respect the above terms? As we have seen these rules are breached many times by the users. Online bullying is often happen in social networks and the same applies with sharing or publishing not authorized content (IP protected, photos of persons with no consent etc.) not to mention that recent studies have revealed that some pedophiles have found a home for social networking on Facebook, where they can securely exchange their hideous

content, covered by the way the user groups are treated[14]. But Facebook assumes no legal responsibility for child pornography, according to Mexican journalist Lydia Cacho[15], which was the one to reveal that "when [Facebook] finds a page containing images of child pornography, it closes the account. The problem is that once the account is closed, it wipes away all traces of the user and any evidence that police could have used to prosecute him or her. In addition, she says, the user often opens a new Facebook page with the same content within a day".

And how the Facebook reacted on these accusations? According to the same source (www.baycitizen.org) "it had taken down the journalist's own Facebook page after she denounced those who post child pornography on Facebook. In response to that claim, Wolens wrote: "We will not comment on specific profiles for privacy reasons, however, we will disable any account found violation our Statement of Rights and Responsibilities".

And this is not the sole case where providers of such online services are using their Terms and Conditions in order to - suspiciously - ban organizations, groups or people. Facebook (again) recently took down 50 activist groups' accounts in UK for alleged breaches of the Terms and Conditions[16]. The problem with the industry self-regulation schemes is the fact that it is so difficult for commercial companies, implemented in online business, to be fair in balancing privacy with practices as spam and government pressure that eventually they step back. That is why the self-regulatory schemes and dispute resolution procedures established by service providers are, often,

[14] http://www.foxnews.com/scitech/2010/09/28/pedophiles-find-home-social-networking-facebook/

[15] Mexican journalist Lydia Cacho has taken on some of the most powerful figures in Mexico, from businessmen to politicians, who have colluded with child pornography rings. Now the women's rights crusader is going after a Bay Area-based company that she says is allowing sexual predators to operate with impunity: Facebook (http://www.baycitizen.org/blogs/pulse-of-the-bay/anti-child-pornography-crusader-takes/).

[16] http://wiki.openrightsgroup.org/wiki/FB_takedowns

seen as prejudiced and suspicious. Because, really, who wants a big corporation as Facebook and Google to judge whether his account will be blocked or his data will be disclosed to the authorities, based only on an alleged "breach" of the accepted (?) terms and conditions? And how many of us do firmly believe that all personal data stored in the servers of these providers are secured and not disclosed, mined or sold. "It's easy for us to imagine that laws and public pressure can hold corporations in check, and therefore this is the most important thing to do. In practice, holding corporations to account is very difficult, and power relations tend to hold the day[17]".

d. Is self-regulation still an option?

This continuous battle for governance of the Internet and the variety of the stakeholders involved led to a situation in which "the Internet is *de facto* co-regulated by National Governments — that intervene however without strongly co-ordinating among themselves — by professional entities — whose competencies overlap and which are not always legitimate — and instances of technical standardization — that are very dynamic, but that lack strong institutional roots. This present institutional framework is problematic for at least two reasons: it is partly inefficient in the sense that there are incompletenesses, conflicts and defaults in enforcement in the set of implemented rules; and the current processes used to establish these rules do not guarantee that the interests of all the stakeholders are fairly taken into account"[18].

[17] http://www.openrightsgroup.org/blog/2011/corporations-may-not-protect-your-free-speech-and-privacy

[18] Open Internet - Maintaining the openness of the Internet and supporting new and innovative business models to foster network development published by ETNO (www.etno.org) on Tuesday 19 Apr 2011.

All the above must have made Robert Madelin (Director General for the Information Society and Media) to say that "Self-regulation is coming under enormous scrutiny. Proof it can work needs to be brought to ripeness quickly[19]." For Madelin in order self-regulation to succeed it must be founded on three basic principles:

1. Transparency. All stakeholders must be involved from the start
2. Accountability. All the parties must set goals and agree the principles
3. Monitoring. Agreed metrics are vital

Conclusions

Freedom in internet and especially when it comes to social networks and blogging is still essential and a prerequisite for the existence of internet. After so many years though we have seen that the old days, when the online community was self-restricted and inspired by the pure ones (as the "cyberlibertarians" dreamed about) have long passed and gone. Even their successors "cyberutopians" cannot rigidly justify that having no regulation is the right answer even when we are talking about how the social media conveys the message (and the messages) for a revolution, as it happened recently in Arab countries. The "cyberutopians" support the idea (and actually seem to believe) that repressive regimes can be overturned in social media and networks. But I would have to agree that "The internet is neither necessary nor sufficient for a revolution. An outraged and unified population is both"[20].

Nowadays the online community services are owned by multinational companies aiming to gain more profit. On the other hand it is usual that the users of such services cannot understand the risk on their privacy and the impact their online activity may have on their real life. "In EU a quarter of children on social networking

[19] Speech on the 16th March, 2011. Crowne Plaza Hotel. Brussels.

[20] "Of Cyber-Skeptics and Cyber-Utopians – Debunking Myths and Discussing the Future" http://www.meta-activism.org/

sites say they have their profile open to public. One fifth of children whose profile is public say this profile displays their address and/or phone number. In 15 out of 25 countries, 9-12 year olds are more likely than 13-17 year olds to have public profiles. Only 56% of 11-12 year olds say they know how to change privacy settings on their social network profile. Older youngsters have better skills with 78% of 15-16 year olds saying they know how to change their privacy settings"[21].

Additional risks that children and teenagers will probably face include grooming (where adults can pass for young people with the intent of abusing children), accidentally finding inappropriate content, and abuse of personal or private information and cyber-bullying.

Therefore, children and teenagers need to learn how to be empowered, they need to manage their online identity in a responsible way by using the privacy settings offered by social networking services, selecting friends online that they can trust, publishing their own photos after thinking carefully about the potential consequences, and pictures of their friends with their permission[22].

We have to deal properly and with responsibility with the social networking sites and blogging services because these new services have changed the way we communicate and of course they have forced the introduction of new technologies to all the age groups and especially the young teenagers. As Evgeny Morozov says "Social media – by the very virtue of being "social" – lends itself to glib, pundit-style overestimations of its own importance. In 1989, the fax-machine industry didn't employ an army of lobbyists – and fax users didn't feel the same level of attachment

[21] Digital Agenda: children using social networks at a younger age; many unaware of basic privacy risks, says survey Reference: IP/11/479 Date: 18/04/2011

[22] http://ec.europa.eu/saferinternet

to these clunky machines as today's Facebook users feel toward their all-powerful social network"[23].

It is true that blogging has given voice to people and has allowed many of them to shout out their beliefs and ideas, the change to express their self and, consequently, a part of their generation. We must realize, though, that all these are happening in an era in which the perception of innocence it is not as it used to be. Childhood and social activity, even in the real world, are not as they used to be. Adolescent happens earlier and ends very soon. The electronic social media have changed the way we make friends, the way we are implemented in the social life, the way we find a job and make a career. At the same time being a member of such a community is far less innocent than being with the gang of school mates with whom we were hanging around when we were kids. Now our secret thoughts can be permanently stored and revealed, accidentally or not, to people and in time totally out of our control.

Blogging, which supposedly transfers the unbiased voice of some people, may often be used for hidden commercial and competition wars and secret public policy. All these simply mean that the defending freedom and anonymity of bloggers has also a side effect that is the lack of any control on postings notwithstanding the fact that often the impact of such online activity is that some people are losing their jobs, their friends or even their lives due to a blog posting or a careless conduct in online social networks. We have to make sure that there is adequate regulation in order to safeguard privacy and free expression and, at the same time, keep the online environment as safe as it needs. Social networks should - ideally - provide sociability. Blogging should mean the sharing of ideas and notions. We have to make sure that all legal instruments we use are aiming this target.

[23] In its Article "Facebook and Twitter are just places revolutionaries go" published online (http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians)

The lack of regulation cannot be the right way, for a democratic society, in addressing the social effects of this new social phenomenon. We cannot let the creation of a chaotic world just to preserve an undefined and unlimited freedom. As Morozov says "What if the liberating potential of the Internet also contains the seeds of depoliticization and thus dedemocratization?[24]"

The bigger the virtual world becomes the less the private space remains to individuals. The bigger the financial and political stakes implemented the less we can expect a– voluntarily – fair usage of the internet resources. We need both regulation and self-regulation but in quantities able to make them comprehensive and acceptable. Regulation can succeed when it does not lift barriers. Self- regulation can work as long as it is broadly accepted by stakeholders and provide for effective enforcement. These two vehicles may be combined and create other appropriate means of administering this virtual world and the conflicting powers. The most prominent of these new vehicles seems to be the co-regulation. The co-regulation schemes are an extension of self-regulation that involves both industry and the government (or regulator) are administering and enforcing a solution in a variety of combinations. "Thus the aim is to harness the benefits of self-regulation in circumstances where some oversight may still be required"[25].

Convergence is creating a new environment where users will be able to traffic their data in several communications markets at once. This kind of use of social media will be a necessity as these services improve and mingle with cloud computing and remote access facilities. Regulation turns to be crucial once again and that is a reality we need to accept and go forward by being careful but productive on how this regulation is formed and how to preserve all these fundamental citizen rights that exist in Europe for decades. "As a platform for free expression, for community, for

[24] Evgeny Morozov «The Net Delusion: The Dark Side of Internet Freedom», PublicAffairs (January 4, 2011).

[25] «A consultation proposing an incentive-based approach to self- and co-regulation in UK communications" www.ofcom.org.uk

business Internet may even be our most valuable communal asset. For that reason the internet must be managed carefully, transparently and lightly"[26]. We need to create a new generation of e-citizens that will be inspired by the traditional elements of respect and fairness. We need to convey these old principles to the new promise land.

(citation: **Spiros Tassis, "Regulation and Self-Regulation of online activity",** Fourth International Conference on Information Law and Ethics, Thessaloniki, Greece, May 20-21, 2011)

[26] Neelie Kroes European Commission Vice-President for the Digital Agenda "The internet belongs to all of us Press conference on Net Neutrality Communication" Brussels, 19th April 2011.