Chapter 8

Industry
Towards the Socially Responsible Internet
Industry CSR Practices Across Europe

Bence Ságvári & Miklós Péter Máder

The topic of children's online safety, a key driver in shaping internet regulation across Europe, has for many internet service providers (ISPs) and online content providers moved to the forefront of their corporate social responsibility (CSR) practices. Research shows that to be effective and to avoid being overly protectionist, children's online safety requires a complex mix of multi-stranded and multi-stakeholder approaches (Livingstone and O'Neill 2010). Digital safety policy is about finding the right balance between regulatory and legislative interventions on the one hand, and awareness-raising and educational initiatives on the other. While the former rests on state and international regulation, supported by self-regulatory measures on the part of industry, responsibility for the latter – given the slow progress in integrating internet safety into the school curriculum at least in several countries across Europe (see chapter 10, this volume) – resides primarily with industry and NGO initiatives.

The aim of this chapter is to look more closely at the involvement of industry, in particular ISPs, in supporting safer internet policy in Europe and the kinds of strategies companies follow to reduce the risk and harm associated with children's internet use. Firstly, we briefly review the industry perspective on questions of regulation of the internet and locate online safety within the main regulatory models and paradigms. We then look at corporate social responsibility practices, specifically questions of liability, trust and confidence towards ISPs. In the second part of the chapter, we discuss corporate social responsibility within the context of conceptual models of the regulatory space, illustrated by real industry examples of best practice from major European telecommunications and internet companies.

Brief Overview of the Regulatory Environment

Phases of Regulation

From an engineering perspective, the internet has always been more or less self-regulated (Tambini, *et al.* 2008). Direct governmental interference in the development of the internet was minimal, and the underlying technological rules and standards by which it evolved were developed largely by self-regulatory bodies such as W3C (World Wide Web Consortium) and IETF (Internet Engineering Task Force).

In terms of regulation, John Palfrey has identified four distinct phases in the development of the internet (Palfrey 2010). The first period was characterized by the idea of internet as a separate domain and up until the end of the 1990s in most countries online activities were outside the radar of the state or only very weak regulation applied. Penetration rates were very low and the social and economic impact of the internet was very far from what it is today. Comparing the genesis of the commercial internet to traditional media such as radio and television there is one major difference in terms of regulation: in most countries internet service providers do not need a government license for their operations, a fact that has had a major impact on the development of services. At the same time, its evolution was also underpinned by a dominant libertarian belief in the free and universal access to information as well as the democratizing and transparent nature of the network. It was also widely held (an argument that still exists in some forms) that the internet represented a separate world (that of cyberspace) with special qualities that made its regulation impossible, even counterproductive. During this period, the internet was relevant only to a small minority of people and clearly the risks and potential threats faced by users (including children) were minimal both in quantitative (i.e. number potential risks) and qualitative terms (seriousness of risk and harm). This has been described as the generative period of the internet (Zittrain 2008), characterised by an almost completely undisturbed period of development for companies and almost completely uncontrolled activities of users.

The second period, that of "access denied", was roughly between 2000 and 2005. During this phase, governments began to think more strategically about certain online activities that needed to be blocked or heavily managed. Most restrictions were based on governments' efforts to hide certain parts of the internet from their citizens. Many types of filtering practices were developed at this time, varying in scope and technology (i.e. DNS, IP or URL filtering techniques), and much of it developed by the industry itself. At a global level, a wide range of social, religious and political information was filtered, mostly in countries with authoritarian and semi-authoritarian regimes. In North America and Europe, the problem of child pornography became the central focus of filtering and blocking (first in the Scandinavian countries) as one of the most evident types of harmful content. In the United States, the government also introduced regulations about what kind of content children could access in libraries and schools (Weitzner and Price 1998; McClure and Jaeger 2009).

The period roughly between 2005 and 2010 could be considered as a phase of "access controlled", a period in which regulatory approaches became more sophisticated. During this period, the number of control points increased, e.g., registration, licensing and identity requirements to control what people/organizations do online. Questions of liability and responsibility also became increasingly important. Industry players were forced to take an active part in blocking and in some countries – for example, China – in surveillance of the internet.

Palfrey (2010) argues that we have more recently entered the latest phase of development, the period of so-called "access contested". Online activities have become an inseparable part of the lives of hundreds of millions of people around the globe. The internet has become an essential and inescapable economic, political and social priority for governments everywhere. In this phase, companies have implemented new strategies for coping with the spread of regulation and liability. In contrast to earlier periods where regulation took the form of state-to-individual control, the focus has moved elsewhere. In general, the emphasis of government regulation is on companies, constraining what they can do directly and requiring them to regulate individuals' behaviour. This approach, for instance, can be recognised in the European Commission's CEO Coalition initiative, which places the onus on industry as a whole to provide better tools for a safer internet. The proposed actions affect all members in the online eco-system, from media companies (content providers) to basic service providers (ISPs), by sharing responsibility for internet safety among them. Some actions and tasks are specific to content providers (e.g., content classification), while others belong more to the domain of service providers (e.g., effective takedown of child abuse material, parental controls). Since the dominant business models of the industry themselves constantly change, the evolution of the issue of obligations and responsibilities will remain an ongoing area of policy interest into the future.

The ever growing importance of safety for children. From self-regulation to co-regulation of ISPs

Although the technology-focused, libertarian approach to the internet remains important today, rapid consumer adoption over the last decade or so has inevitably led to calls for new forms of regulation, especially in the field of child protection. Certainly, the "hands off" policy adopted by most governments in the early years of the internet is no longer tenable. Beyond the engineering and technicist perspective, the 1990s was also a period in which self-regulation as a solution was advocated both by the EU (and its Member States) and the industry.[1] Subsequently, the focus has shifted to a more co-regulatory approach, requiring the more active involvement of the state (Tambini, *et al.* 2008).[2]

There are many reasons behind this shift in emphasis. For one, the social, economic and political significance of the internet reached a 'tipping point' (e.g., the rapid growth in the number of users, the more and more ubiquitous nature of online activities such as social networking, e-commerce, etc.), when 'pure' self-regulation was no longer sufficient. But it was also true that experience showed that many self-regulatory models lacked effective procedures for supervision, enforcement and compliance, in many cases showing merely a declaration of goodwill rather than rigorous implementation (Tambini, *et al.* 2008:4). A 2011 report of the European Commission acknowledged the importance of many industry self-regulatory measures. However, it also highlighted several deficiencies such as the lack of monitoring of several initiatives or the non-mandatory nature of compliance of ISPs with codes of conduct.[3]

It is not difficult to see that the adoption of different self-regulatory measures and compliance with various codes of conduct is a necessary but not sufficient condition for achieving real progress in terms of internet safety. Without sufficient internal monitoring within organizations and third-party verification, few of these initiatives have the chance to succeed. But it is also the case that implementation of verification schemes is highly complicated and significantly increases the costs of self-regulation. Given that this is self-regulation, these are expenses that must be borne by companies themselves, making the process even more challenging.

However, self-regulation does offer a number of obvious advantages. It provides industry with a lead role in framing the regulatory environment and grants them the initiative in the elaboration and implementation of policy. Self-regulation has also distinct advantages for society as well, given that government-initiated schemes can in many cases be too slow and overly bureaucratic, and prove inadequate in keeping pace with the fast changing technology and service environment. More recently, all the major regulatory initiatives in children's online safety were for the most part initiated by the European Commission, and therefore are more accurately described as examples of co-regulation.

The Safer Mobile Use by Younger Teenagers and Children, for instance, was adopted by all leading mobile operators in 2007.[4] These EU-supervised, though largely self-regulatory measures included access controls for adult content, awareness raising campaigns, classification of commercial content and fighting against illegal content on mobiles. The first self-regulatory agreement for social network companies (following the EU's initiative) was signed in 2009.[5] The Safer Social Networking Principles included commitments regarding awareness raising, age appropriate services, user empowerment, easy to use reporting tools, response to notifications of illegal content or conduct and safe use of privacy settings.

In December 2011, 25 CEOs of leading ICT companies at the invitation of Vice-President Neelie Kroes joined forces and published their proposals for a safer internet for children and young people in the EU.[6] The initiative is unique in the sense that the complete value chain of the internet industry is represented by a number of major players, including social media companies (Facebook, Google), network operators and ISPs (BT, France Telecom – Orange, Deutsche Telekom, Telefónica, Vodafone, Telenor, etc.) and hardware manufacturers (Nokia, RIM, LG). The Coalition is a cooperative voluntary intervention and it is the Commission's expectation that new members will join and adopt the solutions developed by the founding members. All participating companies are required to draft their own roadmaps and targets on how to implement the principles. According to the plans, there will be regular self-reporting on progress both at company and group level, and the principles will also be reviewed every two years. Sanctions envisaged include exclusion from the Coalition in cases of not applying the principles.

More self-regulatory in nature is the ICT Coalition (Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU), formulated by another consortium of industry players.[7] This initiative covers much similar ground to that of the CEO Coalition. It includes principles designed to raise awareness on practices that promote online safety in areas of content, parental controls, dealing with abuse/misuse, child sexual abuse content or illegal content, privacy and control, education and awareness. Positive elements of this initiative can be found in its proposals for reporting and implementation. Much of the monitoring process is based on self-reporting of the corporate members (which does not really guarantee unbiased and independent judgement), but an independent expert panel was also appointed and financed by the ICT Principles Stakeholder Group to carry out a review of the consolidated report prepared by the signatories.

The Liability Debate

Focusing more specifically on the role of ISPs in supporting a safer internet for children, ever since the development of a mass market for the internet, the question of liability for content was from the outset the main issue in assessing the role and responsibilities of ISPs. The proponents of zero-liability usually argued that providing internet connectivity to end-users is much like any common carrier communication service, such as that of the telephone. Using a simple analogy, no telephone company could be held responsible for harmful or even criminal communication over its networks (as for example, discussing the details of a murder). Although there is some truth in this argument, the internet is much more complex than simply a transmitter of human voice. The textual, audible, graphical and video formats of digital content, and the one-to-one and one-to-many nature of communication make it a unique network of interconnected computers much closer to mass media in nature.

Cohen-Almagor (2010) has compared this special role of ISPs to a large bookstore, where the owner of the bookstore could not be held responsible for the content of each and every book on sale on its shelves. However, if it turns out that some books contain illegal content (such as child pornography) or violate copyright, the owner of the store has a legal and moral responsibility and must take action to remove the questionable material from the shelves. Similar rules have been applied to the liability of ISPs. In Europe, the E-Commerce Directive of 2000 specifies the basic principles on the liability of intermediaries and introduced the 'notice and take down' mechanism. According to its provisions, ISPs providing hosting services are protected from liability if:

- "the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or
- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information." [8]

On the other hand, most ISPs and web-hosting companies have developed their own guidelines specifying prohibited content and usage. These include not just those elements that are formulated by current laws but usually they set their own terms of use as well.

Who Pays the Ferryman? The Issue of Monitoring Content

Both the history of internet regulation to date and our own informal interaction with industry personnel suggest that ISPs are generally resistant to the idea of fully monitoring the content going through their servers. Their opposition can be explained by the expected costs of employing professional staff to develop the methods capable of monitoring the data flow. In addition, with current technology it is not possible to perform a complete and effective monitoring of content going through the networks of ISPs.

Another risk is that if they non-voluntarily or voluntarily accept to extend their activity to include monitoring and filtering, it will be a 'crossing the Rubicon' moment for the industry. As mere intermediaries in content distribution they are legally protected from liability, but if they engage in any filtering of content they become liable right away. It is also worth noting that fighting against illegal content in a constantly changing technological environment is much like a game of cat and mouse. Looked at in simple terms, assuming responsibility for content hardly, therefore, makes for a predictable business model or gives certainty for the future.

In November 2011, a ruling from the Court of Justice of the EU precluded network providers from implementing systems for large scale filtering and blocking of users' electronic communication.[9] The Court's clarification made it clear that fundamental rights and the freedom of a network provider to conduct its business should be protected and disproportionate technical enforcement that infringes the rights of others is also contrary to EU law. The otherwise complicated and costly systematic analysis of all content passing through an ISP's network undermines both consumers' right to protection of their personal data and their right to receive and impart information.[10]

Currently, the economically rational choice for ISPs is simply to remove any content they are notified about, and otherwise do nothing to monitor content and let end-users, the police and of course, ultimately the content providers, decide what is stored and sent over their network infrastructure (Tambini, *et al.* 2008: 8). Further recent developments on illegal content and copyright issues in the USA and in Europe (SOPA, PIPA, ACTA, etc.) could have consequences for the liability of ISPs which ultimately could have implications for online safety as well. However, at the time of writing the end of this process is still not resolved.

Corporate Social Responsibility in Safer Internet Use

What 'Lubricates' Business: Trust

> All human action occurs in time, drawing upon a past which cannot be undone and facing a future which cannot be known (Barbalet 1996: 82)

Across the world, hundreds of millions of people use both free and paid online services everyday based on an attitude of trust. Trust in this sense is a crucial strategy for dealing with an uncertain and uncontrollable future (Sztompka 2003). We trust ISPs to provide smooth connectivity between our client computers and distant servers and not to misuse the information they gather from our browsing behaviour. We store our most trusted personal or business secrets on Google's or in other company's servers in forms of emails, documents, or family photos and videos. We also trust social networking sites to ensure that there will be no faults in their privacy settings: the posts I intend to share with my friends will not appear on the screen of my boss. An even more sensitive issue is that of online financial transactions. There are numerous examples of how we implicitly trust all kinds of services as well as the companies behind them for many of our daily activities. On the internet, the logic of trust is even more fundamental than that of some traditional "offline" industries, since more and more pieces of our personal data are moving to the cloud. Of course, many people do not think about trusting a service before they start to use it. They just decide whether it is useful and/or interesting to them. However, when something goes wrong (for example, data is lost or stolen, privacy is undermined, the expected level of filtering is not working, etc.) the issue of trust becomes paramount. The reputation of a company is largely based on trust, and when trust is damaged, it easily leads to a loss of business and/or increasing costs in restoring credibility. The issue of digital confidence (especially in terms of online financial transactions) was addressed by the European Union in its *Digital Agenda for Europe* in 2010.[11] In any event, this is something that most internet companies are already keenly aware of. Building and maintaining trust around their services and the company itself is a primary goal that has an unquestionable business rationale behind it. Creating a safer online environment for children by the industry could also be interpreted as a dimension of trust (O'Neill 2012). Although in this case the logic is somewhat reversed, given that the industry as a whole is more or less at the beginning of the process, so generally speaking they are in the phase of building and accumulating trust rather than unintentionally losing it. Those companies that take a leading position in providing effective tools for online safety, or are able to achieve efficient awareness raising through their communication and other initiatives could build up consumer trust first (i.e. in the groups of parents, policy makers, and of course among children themselves etc.). This could also have a definite business advantage.

Growing Importance of CSR in Safer Internet Use

In parallel with the development of self- and co-regulation, and in line with the above question of trust, industry players are increasingly considering the issue of online safety as an activity of corporate social responsibility (CSR). Clearly, companies are themselves influenced by being part of the wider social-cultural context. Employees working for internet companies are also mothers and fathers, affected directly by the problems of online security. But it is also true – as Porter and Kramer have stated – that many companies awoke to the importance of CSR only after being surprised by public responses to issues they had not previously thought were part of their business responsibilities (Porter and Kramer 2006).

Since the motivations behind CSR activities vary both between industries and countries, it is impossible to provide a universal framework for CSR in safer internet use. According to Swanson (1995), at least three main types of motivations stand out. For those companies following the *utilitarian perspective*, CSR is an instrument to support performance objectives (profitability, return on investment, sales numbers, etc.). In the case of ISPs and content providers, more knowledgeable and self-conscious users also mean more profits for the companies, and for that reason many of them actively engage in activities promoting digital skills. This could also have positive implications on children's online safety since many programmes target parents and grandparents.

When the approach of *negative duty* dominates, companies want to demonstrate in their behaviour and communication that they conform to the stakeholder's or to larger society's prevailing norms and values. For example, the increased media attention on the negative aspects of internet use (especially in the case of children) and its potential threat to companies' business interests has encouraged them to deal with this problem more systematically. In many cases, multinational telecommunication companies have integrated CSR practices on internet safety at the highest strategic level. This is then pushed down to local managers at the national level encouraging them to work on, among other things, different awareness raising campaigns, even if they had no intention of engaging in this kind of activity previously.

And finally, the *positive duty* approach can be defined as companies' self-motivation to have a positive impact regardless of their purely economic or communicative objectives. This type of motivation suggests that there should be mutual dependence between companies and society, and both business decisions and social policies must follow the principle of shared values. Benefiting one at the expense of the other undermines the long-term prosperity of both. For ISPs and content providers, this shared value with society is evident in children's safer internet use. CSR activities in this field could certainly be beneficial for society, but it is also valuable for businesses in supporting the emergence of knowledgeable and responsible future users and developing and maintaining trust towards their services and brands.

The problem of effective CSR, however, lies in the scope of these programmes. For example, a successful industry-supported initiative can contribute to the education and training of a few hundred or thousand children, but these numbers – although large in themselves – pale by comparison with the total population in need of support.

Some Evidence on the Role of ISPs

Data from EU Kids Online underlines some important issues regarding the role of ISPs in providing information and advice on safety tools and safe use of the internet across Europe (Livingstone, *et al.* 2011). In general, around one fifth (21.6%) of parents received some kind of information from ISPs. The picture across Europe varies widely: in Bulgaria and Spain these figures are below 10 per cent, while in Finland and Norway it is between 38 and 41 per cent. Likewise, data from other countries shows a mixed picture and in no case do ISPs act as the main source of safety information. Rather, these varying results can be traced back to the mix of effective CSR practices of the industry and soft or hard regulatory pressure from governments.

However, there would appear to be quite a strong demand for a more intensive role on the part of ISPs in providing support for internet safety. According to EU Kids Online data, around one in four parents would like to have information and advice from such companies in the future. After the child's school and traditional media (television, radio, newspapers, magazines), ISPs were the next preferred source of safety information.

From the perspective of children, the current role of ISPs is much less significant. Only 6 per cent of children reported receiving information from their ISPs, while 12 per cent got information from websites. But cross country differences are significant: in Austria the proportion of children receiving information from ISPs reached 14 per cent; in Spain and Italy it stayed below 2 per cent which in fact means that – according to the data – ISPs took literally no role in educating children in these countries. This does not mean that there are no industry initiatives in this field. However, their effectiveness does not reach the threshold of social visibility and measurability.

The results of the EU Kids Online survey also provide evidence on the lack of effectiveness of industry-provided reporting tools. Only a small minority of children who were upset by something they encountered/experienced online used these opportunities, since in many cases they lack child-friendly user interfaces or easy operation (Livingstone, *et al.* 2012).

Conceptualizing Industry Strategies

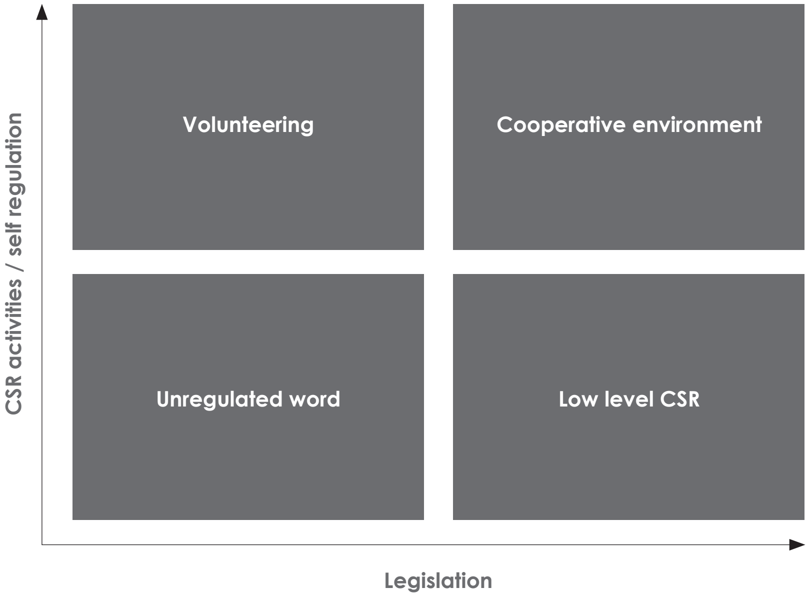
State vs. Self-regulation

In order to better understand the activities of ISPs and content providers in this area, an overview of the legal, ethical and regulatory framework is required. The industry's field of operation is determined primarily by the regulatory environment. However, it is also shaped by other factors such as cultural-political traditions, dominant values of the society, the general conditions of civil society and, last but not least, by the advocacy skills of both government and companies. The regulatory landscape can itself be characterised by on the one hand, legislation (state-regulation), and the prevailing practice of self-regulation, on the other.

In order to provide a theoretical framework for this regulatory-legislative environment, we present a simple model to depict the interdependencies between them. Figure 1 demonstrates this two-dimensional space with the two independent factors of self-regulation (the vertical axis) and legislation/state-regulation (the horizontal axis). The level of self-regulation and legislation can be interpreted as a continuum. A low level of self-regulation refers to the situation when industry players (content providers and ISPs) do not pay any special attention to online safety issues. By contrast, a high level of self-regulation means that industry recognises the importance of online safety and, therefore, voluntarily (or by 'soft' pressure from governments) act against the negative, harmful issues.

As far as legislation if concerned, a low level signifies an undervalued and under-regulated legislative environment. In this case, the safety issues do not appear as necessities for either the regulator or political decision makers. This is illustrated by Palfrey's first phase of the development of the internet when until the end of the 1990s online activities were below the radar of the state (Palfrey 2010). In 1998, the Children's Online Privacy Protection Act in the United States marked the end of this period. Palfrey's second "access denied" period began when states and governments started to think about online activities as something that needed to be blocked or heavily managed. It was a paradigm shift in legislation on children's online safety. Therefore, a high level of legislation signifies that both regulators and political decision makers are sensitive to online safety.

Figure 1. Regulatory Environment for Industry's CSR Activities



The levels of CSR activities / self-regulation and legislation therefore define four different scenarios.

1. '*Unregulated world*' refers to the situation where children's online safety is simply not on the agenda of either regulatory policies or of industry (its self-regulatory and CSR practices). This can be thought of as a phase before online child safety becomes an important topic of social responsibility, i.e., the period from the early to mid-1990s. CSR activities of ISPs and network operators were non-existent or very limited in scope and magnitude. The separate domain of online content providers was almost unknown.

2. The scenario of '*Low level of CSR*' appears when ISPs and content providers do not feel the necessity of proactive CSR or self-regulation, though governmental efforts have become alert to this issue. This more or less equates to Palfrey's third period, the 'access controlled' phase. From the late 1990s, regulation in this area mushroomed in many European countries. Early examples dating from 2001 include the Czech Ministry of the Interior's approval of the "Strategy of the Fight Against Information Technology Crime";[12] the Finnish Ministry of Transport and Communications began a campaign on safer chat;[13] while the Belgian online reporting service (www.ecops.be) also began operations. In this early period, CSR activities were sporadic; initiatives were mostly individual experiments in awareness raising and education. International experience and knowledge transfer in CSR practices were also limited. Multinational corporate CSR strategies were also rare.

3. '*Volunteering*' occurs when legislation is still weak, but some industry players act voluntarily to protect minors. In this scenario, CSR activities move ahead of the regulatory environment. In 2009, Hungarian Telekom's internet content site [origo] launched its video playing and sharing site designed exclusively for children (Videa Kid) containing only child-appropriate content. In 2010, the company launched the free Content Lock service for its customers. By using this service, subscribers have the ability to control access to adult content. In this scenario there is a growing social need and corporate motivation for effective and visible CSR practices. "Doing something" in the field of online safety is formulated as an expectation of ISPs, network operators and content providers.

4. While examples exist for both of the previous two scenarios on a global scale (i.e. China, Middle-East, etc.), the situation in Europe and in the United States was a rather more smooth transition from low to high levels of both CSR activities/self-regulation and legislation. So finally, the fourth case scenario '*Cooperative environment'* appears when both legislation and CSR activities/self-regulation appear to be high. By 2012, we see that the CSR strategies of a great number of network operators and ISPs

involve children's online safety. Companies are developing programmes, campaigns and other tools to support this objective. The CSR practices of the industry and governments' regulatory activities are head to head and mutually support each other. Professional organizations of the industry become more and more active in this field. For example, the European Telecommunications Network Operator's Association (ETNO) has set up a specific Online Child Protection Task Team to monitor international developments and initiatives to collect information on and share best practices amongst members, and to communicate externally ETNO's voluntary commitment to the cause.[14]

Awareness and Protective Developments

Taking a closer look at the available tools in both self-regulation and legislation, we see that they are quite similar. They include several forms of content filtering techniques (i.e. white and black lists, filtering and blocking) on the one hand, and awareness-raising and education type initiatives on the other. As an example, the "Principles for Safer Use of Connected Devices and Online Services by Children and Young People" produced by the industry-led alliance, the ICT Coalition, serves as a guideline here, because they cover many of the most recent issues in online safety. The principles and the basic tools are as follows:

1. Manage content – tools to manage access to certain content.
2. Parental controls – tools for parents to limit their children's exposure to potentially inappropriate content and contact.
3. Dealing with abuse/misuse – tools for users to report content or behaviour which breaches someone's interest.
4. Removal of child sexual abuse content – tools to remove the child sexual abuse content or illegal contact.
5. Privacy and control – tools to manage privacy settings appropriate for children and young people.
6. Education and awareness – tools to provide access to information that will help educate parents, teachers and children about media literacy and ethical digital citizenship.

These six principles/tools may be divided into two major groups. The first group includes all those kinds of education and awareness raising activities both in online and 'traditional' offline forms, while the second group includes providing tools for protection and improving the services available to support safer internet use.

In the first group of actions, the problems and potential threats and dangers of children's online activities need to be promoted among children, parents, caregivers, teachers and other related social workers. Topics include: What are the concerns? What to do in case of being abused? How to report these events? How to defend minors? What are the techniques and methods that can be used to increase the level of security for children? In this complex web of actors, there is a constant need for education as technology continues to develop. And year on year, hundreds of thousands of young children start to use the internet, and incorporate more and more online activities into their daily lives as they get older (Livingstone, *et al.* 2010). As such, awareness raising and education is something that needs constant development and reflection.

Safer Internet Day, an initiative of the Safer Internet Programme and Insafe,[15] has also provided ISPs and network operators with an opportunity to implement awareness raising campaigns across Europe. Some of these activities are realized in cooperation with national and local NGOs working in online safety. This also means that the effectiveness of these awareness raising and education initiatives also depends on the overall state of the civil society sector in a given country. Furthermore, in the case of some smaller countries (like for example Hungary) successful co-operation between industry and NGOs is often reliant on just a few enthusiastic and dedicated professionals.

The following activities of various European telecom and internet companies provide some examples of current educational and awareness raising CSR in children's online safety:

- A tour around schools and Italian town squares to train children to make informed and responsible use of the internet and new media (Safe Browsing) which plans to involve at least one hundred thousand young students, teachers and adults (Telecom Italia).[16]

- School campaigns – training of professors of computer science and Orange employee volunteers on internet safety for children to enable them to deliver awareness campaigns in schools, and supporting psychologists to give lectures in primary schools about safe internet usage (Orange).

- The opportunity for parents to have one-to-one live video discussion with experts on online safety (Orange).

- Congress for teenagers – sponsoring a congress dedicated to 'Teenagers on the net', where more than 1,000 young people participated (Orange).[17]

- Volunteer education kit ('Control Your Online Identity') for teenagers designed to help them learn to protect their personal data online and reputation online. Internet safety coaching kit for teachers and adults working with children to raise awareness of internet safety and support meaningful and open dialogue with children on this topic, helping them to recognize symptoms of cyberbullying, how to prevent online bullying from happening and how to intervene if it does (IBM).[18]

- BrukHue.com, a school campaign based on participation and dialogue with teachers, students and their parents to raise awareness of the issue of digital bullying and to spread knowledge about which situations may lead to bullying and how to avoid these (Telenor Norway with Norwegian Red Cross, Childminder and the Norwegian Media Authority).[19]
- Employee volunteers providing training for school children, teachers and parents associations on online safety. Employees are entitled to 3 days per year to volunteer time working on a good/charitable cause (Microsoft).[20]

The second group of principles/tools include activities based on IT security and system improvements. Managing content, parental control tools, reporting abuse, content removal and managing privacy settings are mainly technology-driven projects supplemented by a necessary non-technological, back-office infrastructure. Practical outputs of these projects include hotlines, passwords, pop-up windows, deleting and blocking content, adjustable privacy and security level settings. Here, the role of ISPs and industry in general is not exclusive, since many tools are operated in conjunction with NGOs and government agencies.

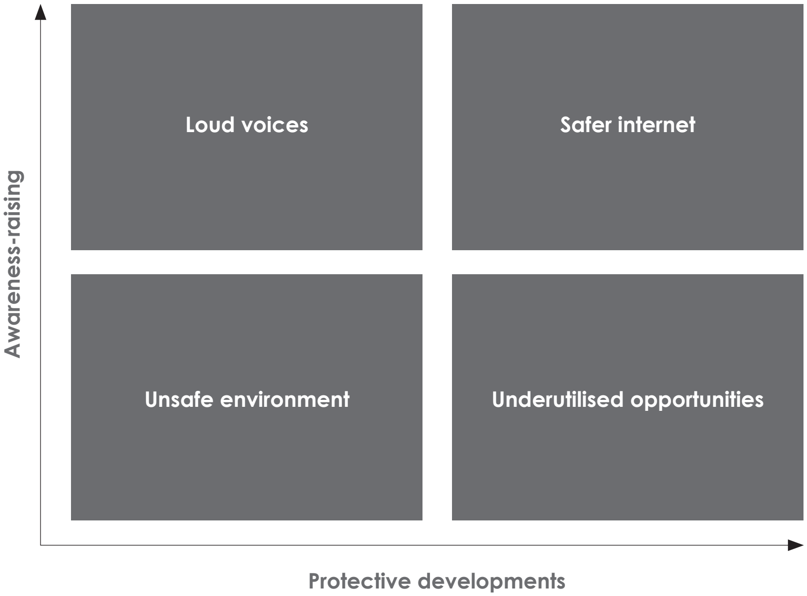
Some examples include:

- Search engines developed to provide safe content for children: such as fragFINN.de, a “smaller version” of the internet, an extensive list of websites that are both interesting and safe for children. Before a website is added to this “whitelist”, a team of media educators checks it against a set of strict criteria, ensuring that children have access only to websites suitable for them.[21]
- Child-friendly web pages, special content developed for children: for example, egyszervolt.hu, a Hungarian website with a child-appropriate user-interface and carefully selected content, such as tales, rhymes, songs, games.
- Internet hotlines for reporting criminal content: for example the Internet Watch Foundation (http://www.iwf.org.uk/) (co-funded by the European Union) the aim of which is to minimize the availability of potentially illegal internet content.
- Quality Control System: for example, the Hungarian site www.bigyoo.hu which has a Quality Control System to evaluate the content based on required features, recommended features and exclusive factors.
- Web Protection Software for children: a wide variety of parental control software has been developed by ISPs, network operators and NGOs.

- URL blocking is the most "radical" and sometimes controversial method of protection, whereby a blacklist of forbidden URLs operates, based on police procedures or on the data of specialised organizations such as the Internet Watch Foundation (IWF).

These two groups of activities (awareness raising and education, and protective measures) can also be organized into a two-dimensional strategic space. Figure 2 demonstrates the possible scenarios.

Figure 2. Possible Strategic Actions of ISPs and Network Operators



Here the vertical axis refers to awareness raising. A low level means that problems go unrecognised by society as well as by industry, whereas a high level represents a situation where children's online safety is at the top of both industry's and society's priority list.

At an early stage, consumers' internet use was primarily exploratory in nature. User attention was consumed by the rapid growth of content and services. It took some years both at the level of the individual user and the industry before more and more encounters and experiences with harmful content led to the realization that there is a dark side to the internet as well. As a result, user awareness supported by both objective and in many cases overreactive media attention began to rise. For industry, NGOs and governmental agencies (certainly with different levels of commitment and focus in their strategies), developing initiatives in awareness raising (i.e. media and educational campaigns) became an important part of their activities.

The horizontal axis on Figure 2 refers to levels of development of protection and cyber security. Here a low level marks weak or missing protection, and a high level represents a well-developed, smoothly functioning system of online safety tools. It was not so long ago that there were no child locks, logging, filtering, black and white lists, etc., and even the awareness of the consequences of too low a level of protection were unclear.

Using a simple matrix, the following scenarios can be identified comparing the levels of awareness raising and online protection.

1. '*Unsafe environment'* describes the situation (or period) when the importance of children's online safety was low both at the level of society and industry, and the need for awareness raising and education was not on the agenda. Also, there were insufficient tools or applications for managing content or safety services for children. This phase of development can be viewed as the beginning period. In the mid-1990s, the internet was mostly the preserve of the early adopters and a few groups of professionals. It was far from reaching a critical mass both in terms of the number of users and available content and services. Harmful content certainly could be found online, but it posed little real danger to society (and especially to children) or to industry.

2. '*Loud voices*' is a condition where strong awareness raising meets ineffective protective tools: the regulatory environment is weak and the level of corporate responsibility is also low. This situation can be interpreted as the regulatory environment not matching the needs and expectations of society. This is a situation of under- or mis-regulation, where there are no real working tools for effective protection. From an historical perspective, 'Loud voices' could be considered as the seed phase of the late 1990s, when growing negative experiences and raising awareness of internet safety had come to the attention of different stakeholders (industry, governments, social scientists, etc.) The understanding of the nature of online risks and dangers was evolving, and scientific research started to focus on the societal effects of information technology use. However, effective regulation and functioning protective mechanisms were still missing. But the problem became evident at a larger societal level and public discourse started to grow stronger.

3. When the scenario of '*Underutilised opportunities*' dominates, state regulation, political objectives become important, industry is providing usable tools for security, but awareness raising, the activities of civil society, and participation from users do not follow. This was the situation, for example, in the late 1990s, when (as a consequence of governmental legislation and pressure) companies were pushed to incorporate content-blocking into their browsers (i.e. Internet Explorer) in the United States, but users

were not really interested, prepared or motivated to use this function. Certainly, there is an overlap between the second and the third scenarios, since they do not follow each other in predetermined sequence. Different historical and political traditions in the roles of governments in regulation and in the social embeddedness of industry could lead to the dominance of one of the two middle scenarios.

4. The '*Safer internet'* represents the co-existence and co-operation of state regulation, protective developments by industry and active awareness raising. These efforts mutually support one another. The initiative of the ICT Coalition (Principles for Safer Use of Connected Devices and Online Services by Children and Young People) demonstrates that major industry players have arrived at a stage where protective activities and CSR activities are both supporting the development of a safer online environment.

Conclusions

As we look at the development of legislation and CSR activities in respect of children's online safety from a lifecycle management point of view, we can analyse this process using phases of evolution in time. The four stages of a typical life cycle are: (1) introductory stage, (2) the growth stage, (3) the stage of maturity and (4) saturation stage (Levitt 1965). These stages are consecutive as time goes by.

The self-regulation/legislation and the awareness raising/protective development spaces can be analysed by this evolution in time. The 'unregulated world' and the 'unsafe environment' scenarios of the two theoretical models can be interpreted as the initial, introductory stages of the 1990s and early 2000s. In the past few years, the situation in Europe is moving in an ever more linear fashion towards 'safer internet' and 'cooperative environment' scenarios. This constitutes a stage of maturity where both policy (at national and EU level) and industry (global and local level), supported by such domains as research on children's internet use, media in general, and NGOs have more or less adequate knowledge and awareness when it comes to taking effective steps for a safer online environment, and finding the optimal balance between restriction and support.

Looking back at the development of provisions and activities around internet safety we can see also that in Europe there were no serious deviations from the imaginary diagonals (from the low left to the top right corner) of the two theoretical models introduced in this chapter. Legislation and self-regulation, and also awareness raising and protective developments both evolved 'hand in hand'. Of course some national differences can be observed based mainly on a country's available financial resources, the structure of the internet industry, general political traditions of state-economy relations, cultural and value differences on children and education, etc. But common policies at the level of the European Union and the global nature of the industry (a few dozen multinational corporations are dominating the whole value chain) make convergence a universal phenomenon across Europe. But the data also shows that there is a demand from users for more active safety tools and for the provision of information from ISPs and industry in general.

It remains the case that more sophisticated evaluation and better tools to measure and evaluate children's online safety are still needed. There is a need for better indicators to measure the risks and harms children encounter online as well as to evaluate the effectiveness of the tools designed to protect them. Appropriate reporting and research needs to include hard and soft data at the same time, and requires input from all key stakeholders: industry players, state regulators and social science researchers.

Notes

1. See for example the recommendation of the European Council on the protection of minors from 1998. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:270:0048:0055:EN:PDF) Prior to this recommendation the EU published several official documents on the basically self-regulatory based development of Information Society and Internet.
2. In its 2006 recommendation the European Parliament and Council stated that the whole, self-regulation of the audio-visual sector was proving an effective additional measure, but it was not sufficient to protect minors from messages with harmful content and called for intensive cooperation between legislators, regulatory authorities, industry, associations citizens and civil society. (2006/952/EC) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:378:0072:0077:EN:PDF)
3. COM (2011) 556 – Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0556:FIN:EN:PDF)
4. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/139&format=PDF&aged=1&language=EN&guiLanguage=en
5. http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf
6. CEO Coalition (2011) *Coalition to make the internet a better place for kids. Statement of Purpose.* At: http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm
7. http://www.gsma-documents.com/safer_mobile/ICT_Principles.pdf
8. From Article 14 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF)
9. The background of the story dates back to 2007 when one of the Belgian ISPs was ordered to install a filtering system to monitor all peer to peer traffic on its network and to block the exchange of files which were included in the repertoire of Belgian Society of Authors, Composers and Publishers (SABAM).
10. http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0070&lang1=en&type=NOT&ancre=
11. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
12. http://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Czech%20Republic.pdf

13. http://www.lvm.fi/fileserver/creating%20a%20safer%20information%20society.pdf
14. http://www.etno.be/Default.aspx?tabid=2327
15. http://www.saferinternet.org/
16. http://hhxen0103.halvarsson.se/files/telecomitalia2010sren.pdf
17. http://www.orange.com/en_EN/press/press_releases/cp120203en2.jsp.
18. http://www-03.ibm.com/press/us/en/pressrelease/36700.wss
19. http://telenor.com/corporate-responsibility/initiatives-worldwide/united-front-against-digital-bullying/
20. http://www.csreurope.org/solutions.php?action=show_solution&solution_id=756
21. http://www.fragfinn.de/download/fragFINN_Flyer_engl.pdf

References

Barbalet, J. M. (1996) Social emotions: confidence, trust and loyalty. in: *International Journal of Sociology and Social Policy*, Vol. 16., No. 9/10, 75-96.

Cohen-Almagor, R. (2010) 'Responsibility of and Trust in ISPs', *Knowledge, Technology and Policy* 23(3): 381-396.

Levitt, T. (1965) 'Exploit the product life style', *Harvard Business Review* Nov/Dec, 43 (6): 81-94.

Livingstone, S. and B. O'Neill (2010) 'Promoting children's interests on the internet: regulation and the emerging evidence base of risk and harm'. Retrieved at: http://microsites.oii.ox.ac.uk/ipp2010/system/files/IPP2010_Livingstone_ONeill_Paper.pdf

Livingstone, S., L. Haddon, A. Görzig, and K. Ólafsson (2010) *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online.

Livingstone, S., K. Ólafsson, B. O'Neill, and V. Donoso, (2012) *Towards a better internet for children*. LSE, London: EU Kids Online.

McClure C.R. and P.T. Jaeger (2009) *Public Libraries and Internet Service Roles. Measuring and Maximizing Internet Services*. Chicago: American Library Association.

Nolin, J. (2010) 'Speedism, boxism, and markism. Three ideologies of the Internet', *First Monday* 15(10): 4 October 2010

Palfrey, J. (2010) 'Four Phases of the Internet Regulation', *Social Research* 77(3): Fall 2010

Porter, E.M. and M.R. Kramer (2006) 'Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility', *Harvard Business Review*, December 2006.

Swanson, D.L. (1995) 'Addressing a Theoretical Problem by Reorienting the Corporate Social Performance Model', *Academy of Management Review* 20 (1): 43-64.

Sztompka, P. (2003) *Trust: A Sociological Theory*. Cambridge: Cambridge University Press.

Tambini D., D. Leonardi and C. Marsden (2008) *Codifying Cyberspace: Communications Self-Regulation in the Age of Internet Convergence*. London: Routledge

Weitzner, D.J. and M.E. Price, (1998) 'Yelling 'filter' on the crowded Net: the implications of user control technologies', in E.P. Monroe (ed.) *The V-chip Debate: Content Filtering From Television To the Internet* (pp. 207-220). London: Routledge.

Zittrain, J. (2008) *The future of the Internet and how to stop it*. London: Yale University Press.