Protecting children's privacy online: a critical look to four European self-regulatory initiatives

Milda Macenaite

Cite as Macenaite M., "Protecting children's privacy online: a critical look to four European self-regulatory initiatives", in European Journal of Law and Technology, Vol 7, No 2, 2016.

ABSTRACT

This article examines the rise of self-regulatory initiatives as private governance mechanisms adopted by the Internet industry in the EU to protect children's privacy online. It analyses four specific initiatives and performs a formal self-regulatory process analysis focusing on procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects, in order to reflect on the strengths and shortcomings of the self-regulatory process. The analysis shows significant limitations of self-regulation in the area of online child safety, characterized by broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions. It is argued that sector-specific, institutionalized European codes of conduct, which disentangle protection of online safety and privacy as policy aims, could permit achieving better formulation, adoption and enforcement of voluntary rules, and thus better safeguard the privacy of children in the dynamic multi-jurisdictional, multi-stakeholder dominated online environment.

Keywords: children; European Union; online risks; privacy; self-regulation; soft law

INTRODUCTION AND BACKGROUND

The area of children's privacy protection on the Internet has recently witnessed a vast increase in attention and regulation within the EU. There are several driving factors behind such developments. First, the importance of children rights, including the right to privacy and personal data protection, has grown. The EU has not only enshrined children's rights to protection and care in the European Charter of Fundamental Rights, but also has identified effective protection of these rights among the main priorities in its strategic documents (European Commission 2006, 2012). Second, a sharp increase in Internet usage by ever younger children and the complexity of the technology mediated environment has raised serious concerns about online child safety (Van der Hof, 2014). Protection of privacy and personal data in such a complex environment has become a prerequisite for guaranteeing online child safety and, thus, has started to constitute a separate, though interrelated, pillar within many online child safety initiatives. Third, since 1999 the European Commission's Safer Internet Program has achieved remarkable progress in awareness raising and educational initiatives, multi-stakeholder involvement in safer Internet policy making and Internet content creation. Part of this Program fostered the gathering of more empirical data about online risks and their impact on children's online experiences across Europe (Livingston *et al.* 2012; O'Neill *et al.* 2013) which provided policy recommendations and implications (O'Neill *et al.* 2011). Empirical research has indicated that some of the most important concerns among children are related to personal data misuse and reputational damage, such as hacking of social media accounts, creation of fake profiles, and impersonation (Mascheroni & Ólafsson 2014). These concerns are well grounded, as 9% of children aged 11-16 have experienced personal data misuse online (Livingstone *at al*. 2011). Research has also clearly revealed the difficulties that children face when finding and using reporting tools and privacy settings to protect themselves online (Livingstone *at al*. 2012). All this in turn has penetrated discussions and has called for action among policy makers, academics and other stakeholders.

Since the very beginning, the protection of children online as a policy area in the EU has entailed an "unshakable commitment to self-regulation" (O'Neill *et al.* 2013, p. 15). [1] As paradoxical as it may seem, the implementation of protection of children's rights to privacy and personal data protection - both fundamental human rights - has to a large extent been playing into the hands of the industry in their online safety initiatives. As self-regulation and private rule-making has been put forward by the European Commission as a cornerstone of the regulatory process of online child protection, the effectiveness of the concrete self-regulatory rules becomes crucial in order to guarantee actual protection. Despite the obvious advantages proposed by soft law, such as the socio-technological expertise of the industry, innovation, reactive speed and reduced costs for the public bodies, in essence private rule-making, in particular where self-regulation is involved, is still often perceived as inherently feeble or ineffective regulation (Scott *et al.* 2011). Due to the lack of transparency, accountability coupled with ineffective enforcement, legal and media governance scholars question the results that self-regulation can provide, perceiving them as rather limited in practice (Latzer *et al.* 2013; Koops *et al.*2006; Bonnici 2008). Scholars within regulation studies (Scott *et al.* 2011) worry that self-regulation – as a community-based mode of private governing – raises legitimacy problems, due to its significant differences from the traditional democratic government model. If private regulation is more than technical implementation of authority, it is questionable to what extent it can advance a fair struggle between competing public and private interests (Scott 2012). In cases involving a public interest, such as the protection of vulnerable Internet users, there is a question whether self-

regulatory initiatives can afford such protection to the same extent as serve the interests of the private sector (Livingstone 2011). This is particularly true for the area of online self-regulation which in general is known to "suffer from the perception that the individual's privacy rights are in the hands of those who have the most to gain from the processing of personal data" (Bennett 2004, p. 233). As a consequence, self-regulation may easily result in "self-service by the industry, with public interests being neglected vis-à-vis private interests" (Latzer *et al.* 2013, p. 375). It is not surprising, therefore, that in order to balance public and private goals in the self-regulatory process, in reality public actors often need to play a more active (co-regulator's) role. However, due to the many different forms that co-regulation may take, it does not necessarily ensure effective regulatory outcome either.

Despite the diversity of rules and their adoption processes, the Internet industry has, until now, managed on a European level to agree on four alternative regulatory initiatives that, among their other provisions, substantially deal with the protection of the online privacy of children. [2] These initiatives include: an arrangement among social networking service providers – the Safer Social Networking Principles for the EU; two documents adopted by broad industry Coalitions – ICT and CEO Coalitions; and a sectorial code of conduct adopted by direct marketing companies to regulate the use of personal data in their activities. Although different, these four initiatives all have amongst their other objectives the aim to mitigate online privacy risks, such as personal data misuse, commercial data exploitation, conduct and contact risks.

The aim of this paper is to examine the emergence of self-regulatory initiatives in the EU, aiming to address online privacy risks for children as governance mechanisms and explore their strengths and shortcomings. By analyzing the key provisions in four self-regulatory initiatives, the paper aims to perform a formal self-regulatory process analysis, rather than self-regulatory outcome analysis, focusing on procedural regulatory aspects. The analysis is based on the evaluation criteria that, according to regulatory scholars, must be present in self-regulatory regimes to consider them as effective and legitimate, i.e. procedural criteria (rule formulation, monitoring, enforcement) and organizational criteria (organizational structures, role of public actors).

The paper is structured as follows. The first section provides a short overview of the rise of self-regulation in order to protect children from risks in the Digital Single Market, discussing the main drivers and catalysts of such a rise. The second section describes the current self-regulatory regime for the online privacy protection of children, drawing on two different areas: online child safety and online advertising. Four self-regulatory initiatives are analyzed: the Safer Social Networking Principles, the CEO Coalition's Statement of Purpose, the ICT Coalition's Principles, and the FEDMA code. [3] These are the only existing self-regulatory initiatives dealing with online child privacy as a substantial part of their content. A formal self-regulatory process analysis focusing on the above-mentioned procedural and organizational aspects of the initiatives is performed in the third section, in order to evaluate their adequacy as regulatory mechanisms. The fourth section provides an evaluation of the initiatives. Conclusions are drawn in the last section.

1. THE RISE OF SELF-REGULATION IN THE DIGITAL SINGLE MARKET

Self-regulation related to the Internet has a long tradition. A wide range of voluntary initiatives, such as codes of conduct, rating/filtering systems, hotlines, standards, have been contributing to the protection of public interests and supplementing the existing state regulatory frameworks for two decades. One of the most prominent regulatory goals pursued by the means of self-regulation is the protection of minors in the communications sector, including on the Internet. In fact, reliance on self-regulation, rather than on legislation, in order to protect children's safety and privacy online in Europe can be traced back to the mid-1990s (European Commission 1996). Since then, policies aiming to create a safer - in more recent policy documents framed as "better" (European Commission 2012) - Internet for children place significant emphasis on alternative regulatory initiatives, like self- and co-regulation (Lievens 2010). Preference for self-regulatory rule-making in relation to the online environment has been repeatedly confirmed in the main strategic EU policy documents, such as the Digital Agenda for Europe (COM/2010/0245 final), and the Agenda for Children's Rights (COM/2011/0060 final). References to sectorial industry codes of conduct were incorporated into the EU Data Protection Directive (95/46/EC), the EU Unfair Commercial Practices Directive (2005/29/EC) and, most recently, the General Data Protection Regulation (2016/679). All of these acts encourage self-regulation by the industry in general and, in the latter case, codes of conduct to protect the privacy and personal data of minors in particular.

There are various reasons why the EU considers industry self-regulation as the preferred option in the area of online child safety and privacy protection. More generally, a tendency to relate voluntary rule making rather than hard law with cyberspace regulation has been clearly expressed since the infancy of the Internet and grounded in cyber-libertarian ideas about an independent and unregulated cyberspace (Barlow 1996, Weber 2002). In fact, the Internet being global creates worldwide problems, such as safety and privacy risks for the users, which go beyond the capacity of individual states to solve, and thus requires global solutions. Self-regulation allows for detaching these solutions from the complex hard law Internet-related dilemmas of jurisdiction, applicable law and effective cross-border enforcement of legislation. It therefore also allows for softly reducing regulatory fragmentation on both sides of the Atlantic, getting US-based companies providing services to the EU citizens on board and imposing voluntary rules on them.

Other reasons that have driven the rise of self-regulation include the rapidly changing technological landscape and the difficulty of adjusting the national laws of the Member States to the new Internet-related developments (De Haan *et al.* 2013). Self-regulation was thus seen as able to address the emerging issues in a more time-saving and cost-efficient way. Also, multi-stakeholder involvement into the regulatory process and an informal-law-making environment seemed to promise more expertise and innovation than the traditional law making process and as a collective effort permitted reconciliation of conflicting interests - to preserve fundamental human values in the face of economic and technological pressures. In this respect, self-regulation was seen as able "to operationalize vague and general policy objectives" and provide practical guidance to the relevant parties on how to carry out their activities, in such a way "moving discussions from high-level policy rhetoric and slogans to more mundane, nitty-gritty action" (Webb 2004, pp.14-15). This evidenced a way to depoliticize important public issues, replacing them with technical solutions, procedures, and formalities driven by industry (Webb 2004). For instance, reliance on

practical instruments such as parental control software, reporting mechanisms, content rating, and filtering systems introduced by self-regulation has allowed the EU to respect both freedom of expression and internal market and competition rules (Lievens 2010).

Finally, protection of online privacy in particular requires achieving a careful balance between ensuring the free flow of information and safeguarding the rights of users. Balancing these and similar competing interests can be complicated in legislative instruments not only due to their typical features such as rigidity or central implementation, but also the sensitivities involved. For example, as regards Internet content regulation, there is a propensity for state censorship, and therefore regulation in this area can be intentionally left to private parties (Lievens 2010).

2. SELF-REGULATORY INITIATIVES ADDRESSING ONLINE CHILD PRIVACY

This section introduces the four EU self-regulatory initiatives adopted to mitigate online privacy risks for children, with the focus on their main characteristics (the year of the adoption, actors involved, nature and scope of the initiatives and the privacy-related provisions). All child-related provisions of the four initiatives are summarized and compared in Table 1 below.

2.1. SAFER SOCIAL NETWORKING PRINCIPLES

The Safer Social Networking Principles for the EU (the SNS Principles) (European Commission 2009) is an early example of self-regulation in the area of online safety of minors. Initiated and supported by the European Commission, this self-regulatory initiative was adopted in 2009 and brings together approximately 20 social networking service (SNS) companies. The common goal of the participants, as claimed in the introductory part of the Principles, is "to maximise the benefits of the Internet while managing the potential risks to children and young people". To reach this goal, the providers have to assess the risk of potential harm that their service may cause to children, and consider the application of the specific seven overarching principles-guidelines. Two principles in particular encourage a safe approach towards personal information and privacy by having adequate safety tools and policies implemented in online social networking services. The third Principle requires empowering children through tools and technology and providing them with assistance with regard to inappropriate or unwanted content or conduct through special measures and technological tools. Concrete measures and tools that service providers should offer include, for example, non-searchable private profiles, profiles set to 'private' by default, ability to control who can access full profiles and post comments, 'easy-to-use' report tools. The sixth Principle asks service providers to enable and encourage their users to employ a safe approach to personal information and privacy through privacy settings and supporting information. Providers should offer user-friendly and accessible privacy options that enable users to make informed decisions about personal information that they publish and allow for privacy status and setting to be visible all the time. The remaining principles focus on awareness raising about online safety, age-appropriate services for the intended audience (e.g. indication of the minimum registration age, deletion of under-aged user accounts), and effective mechanisms to report inappropriate content and behaviour.

In essence, the SNS Principles provide only guidance for the providers of SNS and, thus, are merely aspirational in their nature. They are in no way prescriptive or legally binding.

Participating SNS providers are left with a wide discretionary power while judging whether to respect certain principles and to what extent, considering the particular nature of their services. This leads to inconsistent and hardly measurable enforcement of the Principles, one of the shortcomings which will be discussed later in this paper.

2.2. COALITION TO MAKE A BETTER AND SAFER INTERNET FOR CHILDREN

In contrast to the SNS Principles, an initiative which aims to shape the behavior of private actors in a technology-specific domain, the Coalition to Make a Better and Safer Internet for Children (CEO Coalition), has been designed to gather a broad range of private companies working in various sectors of the ICT industry, such as operating system providers, handset manufacturers, Internet Service Providers, broadcasters, social networks and mobile operators. Launched in December 2011 on a high political level - personally by the Vice-President of the European Commission responsible for the Digital Agenda for Europe N. Kroes - the CEO Coalition aims to propose and develop, first of all, technical solutions and measures to protect children online. It was hoped that later these solutions proposed by the Coalition members can also be embraced by other market players. This initiative spans traditional technological or sectorial boundaries, and is defined by the practice in which companies are engaged - providing ICT services or products directed at or used by minors rather than by specific technology, like the SNS Principles.

Since its formation, around 31 companies have joined the CEO Coalition. According to the CEO Coalition's Statement of Purpose (CEO Coalition 2011), the five areas in which the companies agreed to take action and develop solutions include: tools for users to report harmful content and contact, age-appropriate privacy settings, content classification, parental controls, effective take down of child abuse material. The second area - age-appropriate privacy settings - is the most important reference to online privacy that can be found in the Coalition's Statement of Purpose. However, the intention of Coalition members in this area has been limited to pooling current practices and data together on a possible single appropriate level of privacy settings across services and related user information protocols. The mere compilation of a database on these issues seems to be a very modest aim, acknowledging privacy as a human right and the influence of default-settings on the online behavior and practices of children. The lack of ambitious and clear goals has characterized this initiative since its inception and consequently attracted criticism from various actors within civil society (EDRi 2013).

Despite the initial enthusiasm, especially on the political level, currently the CEO Coalition is not very active in practice. After the first year of functioning the progress has been suspended, although publicly the Coalition members and the European Commission affirmed their commitments to collaborate. Apart from a few spin-offs from the Coalition in the area of content classification, future collaboration (if it happens at all) appears to be essentially limited to awareness raising and the sharing of best practices and educational materials among the Coalition members.

2.3. ICT COALITION FOR CHILDREN ONLINE

Another self-regulatory initiative that is similar to the CEO Coalition in terms of content, membership and timing is the ICT Coalition for Children Online (ICT Coalition). The main difference between the two initiatives lies in their formation process. The ICT Coalition was formed by the industry without any involvement of the European Commission. In its own capacity, it elaborated a set of principles - Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU (ICT Coalition 2012). Although adopted a month after the CEO Coalition's Statement of Purpose, in January 2012, the ICT Principles actually preceded the CEO Coalition in terms of negotiations and drafting by one year. Almost identically to the CEO Coalition, the ICT Coalition Principles pursues the aim "to help younger Internet users across Europe to make the most of the online world and deal with any potential challenges and risks" [4]. Given the overlap in focus and members, it is not entirely clear why the CEO Coalition was initiated in the first place, creating a parallel initiative to the already ongoing industry effort.

The ICT Coalition is made up of 23 different companies from across the ICT sector, and just as the CEO Coalition can be considered a functional initiative in its nature. In terms of scope, the ICT Coalition Principles focus on six key areas: harmful content, parental controls, abuse/misuse of technology, sexual abuse content/illegal contact, digital literacy and awareness, and privacy. The privacy area is defined by Principle 5, according to which companies promise to manage and provide options for privacy settings in a user friendly way (easy to understand, prominently placed, user friendly and accessible) and enable children and parents to make informed decisions, as well as to raise awareness among all relevant parties. This commitment, if still limited in its aim, provides much more clear and ambitious goal than the action of the CEO Coalition on the same matter.

In practice, the ICT Principles oblige each company (or group of companies) to present a document, which states objectives to be attained and benchmarks as far as applicable to its specific services and products, which would allow proper monitoring of further implementation in the six areas mentioned above. Companies that are signatories to this initiative are expected to report on their progress after the adoption of the Principles. More than half of the companies have published their progress reports on the Coalition's websites, based on which an independent review of the achievements took place.

2.4. EUROPEAN CODE OF PRACTICE FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING

A very different initiative in its nature compared to the three online child safety initiatives is the European Code of Practice for the Use of Personal Data in Direct Marketing (the Code) (FEDMA 2003), a self-regulatory initiative adopted in the advertising sector to regulate data collection for marketing purposes. The aim of the Code is, in part, to protect minors from commercial risks inherent to the online world. The Code is based on more detailed and thorough analysis of how industry collects and processes personal information rather than broad commitments and statements.

The Code was adopted in 2003 by the Federation for European Direct and Interactive Marketing (FEDMA), a sectorial organization widely representing the direct and online marketing industry on the European level through promotion and protection of its interests, lobbying for a favorable legislative environment and education and training. Currently

FEDMA reports to have around 400 direct members in more than 30 countries, and nearly 10,000 companies are represented indirectly through their membership in national Direct Marketing Associations. The Code has been implemented on the national level by all FEDMA members.

The Code is European in character, as the Article 29 Working Party, a European body representing the national data protection authorities, has approved it in accordance with Directive 95/46/EC as providing sufficient added value by addressing data protection problems in the direct marketing sector (A29WP 2003). By approving the Code, the Article 29 Working Party also underlined that the general provisions of the Code cannot solve all specific issues related to online direct marketing, and asked FEDMA to draft an annex to the Code applicable to the online environment and in particular addressing the protection of children. As a result, in 2010 following an extensive and long consultation process with the Article 29 Working Party, the Code has been supplemented with an Annex applicable to online marketing (FEDMA 2010), which was also approved by the Article 29 Data Protection Working Party (A29 WP 2010). Section 6 of the Annex deals with the protection of children and, among other things, establishes the responsibility of the data controller for setting up the procedures to guarantee verification of the age of the minor and the authenticity of the parental consent. However, it acknowledges that there is no easily accessible, universally accepted age verification system available on the Internet. The Code also obliges data controllers to provide child-appropriate information about data processing, prohibits family data collection from children, limits collection of sensitive data, and forbids incentives to provide personal data for marketing purposes or in exchange for a reward, including games of chance, tombola or lotteries.

Table 1. Child-related provisions of the four initiatives

Provisions	SNS Principles	CEO Statement	ICT Principles	FEDMA Code
Awareness raising, user empowerment	✓	-	✓	-
Age appropriate services	✓	-	-	-
Conduct & content reporting tools	✓	✓	✓	-
User-friendly privacy settings	✓	✓	✓	-
Content classification	-	✓	✓	-
Parental controls	✓	✓	✓	-
Take down of illegal content	✓	✓	✓	-
Age verification	✓	-	-	✓
Understandable information	✓	-	✓	✓
Prohibition to collect information about family members	-	-	-	✓
Requirement of prior consent for collection of sensitive data	-	-	-	✓
Prohibition to incentivize children to provide personal data in exchange for rewards	-	-	-	✓

3. COMPARATIVE ASSESSMENT OF THE SELF-REGULATORY INITIATIVES

The comparative assessment in this section is based on the main evaluation criteria that, according to scholars in the areas of electronic communication and technology regulation and governance, must be present in self-regulatory regimes to consider them as effective and legitimate.

Although in the electronic communications sector conceptual frameworks for evaluation of self- and co- regulatory initiatives are still in the initial stage of their development (Latzer *et al.* 2013), several efforts to propose a set of criteria to evaluate the effectiveness of voluntary rules have been made by academics (Schulz and Held, 2002; Latzer *et al.* 2007; 2013). On a policy level, the European Commission has also recently looked for criteria to define accountable and efficient self-regulation which could deliver on its societal goals (CoP 2013). These contributions highlight the need for clearly formulated rules and requirements, effective monitoring and oversight, enforcement mechanisms and sanctions, including independent complaint assessment procedure. Writings on self-regulation in industries other than ICT have similar requirements for effective industry self-regulatory arrangements (Bowman & Hodge 2009; Sethi and Emelianova 2006; Gunningham & Rees 1997; Doing & Wilson 1998; Jenkins 2001).

In addition, interdisciplinary literature on governance and self-regulation underlines the importance of a background presence of public actors (Ayres & Braithwaite 1992, Gunningham & Grabosky 1998, Rees 1997) and the existence of recognized industry organizations (Latzer *et al.* 2007) in enhancing the adoption and enforcement capacity of self-regulatory rules. The latter refers to acknowledged and structured industry bodies, such as the associations of specific industry segments, which have experience and administrative capacity in dealing with self-regulation.

Taking into account the contributions mentioned above, the paper uses two sets of criteria to evaluate the self-regulatory process related to the initiatives described earlier: procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors). These criteria and their precise indicators are applied to the four initiatives in Table 2.

3.1. CONTENT OF THE RULES

Clearly defined objectives and measurable standards set forth by self-regulation that are able to add additional value to the existing legislative provisions can enhance potential advantages and reduce failures of self-regulation. As noted by Latzer *et al.* (2007), the way the self- and co-regulatory initiatives are designed may constitute an important enabling institutional/organizational factor. Ideally, a self-regulatory initiative should specify a mission statement with a reference to a public policy objective, define clear, measurable goals and intended outcomes. Additionally, it should clarify the regulatory added value in relation to the existing state regulation (Latzer *et al.* 2007).

When comparing the four initiatives, one of the most striking differences lies in the formulation of the rules embodied in the self-regulatory texts under analysis. All the initiatives adopted in the online child safety domain set only general targets and aims, which can be denoted more as intentions or statements of commitments rather than as rules.

Consequently, they add little to the existing legislative framework. The CEO Coalition's Statement of Purpose and reports provide the clearest illustration of broad objectives from all three safety-related initiatives (e.g. "to take positive action to make the Internet a better place for kids"; to "continue to work with wider stakeholders to raise awareness on parental controls"). These statements also almost entirely repeat the legislative requirements ("to offer clear and understandable information" in privacy policies). In contrast, the sectorial code in the online advertising area provides much more precise rules and obligations for its members. [5] It is thus a much more measurable self-regulatory text which builds upon the general data protection standards that are not tailored to children, an additional level of specific protection adding value to the existing data protection law. For example, the FEDMA members are required to obtain prior consent before collecting sensitive data or are prohibited from processing certain types of data.

Lack of clear, prescriptive rules and measurable standards in the policy area of child online safety leads to several shortcomings. First, companies adhere to the same initiative in very different ways. Some of the companies commit to do very little, some take obligations seriously within the scope of the same principles and others even claim that certain obligations are not applicable to their services or products. Second, due to imprecise goals it is difficult to measure and compare compliance among the members and to evaluate the level of fulfillment of the agreed objectives. The latter problem will be discussed in more detail below.

Notwithstanding this, one should note that broad and vague objectives do not automatically lead to the failure of a self-regulatory initiative. Vague prescriptions and high-level statements of intent not only allow for adapting the requirements to specific services and products, but also leave companies room for innovative solutions. In addition, the inclusion of more prescriptive rules may be premature in the beginning of the self-regulatory process, especially in the areas where technological solutions are still scarce, like in relation to age verification technologies. This, however, does not preclude the possibility of developing quantifiable and enforceable standards over time.

In addition, from a policy making perspective it may be questioned whether companies would be at all willing to commit themselves to something more than broad statements and intentions. Even if the state of the art of technological developments and expertise of the industry may theoretically allow for prescriptive provisions, the motivation to have detailed self-regulatory rules can still depend on various other factors. These factors, for instance, can be pressure on corporate image (Gunningham 1995) or peer pressure and mutual benefits, the perception of the importance of avoiding hard regulation, the willingness to forestall or shape future laws, and the existence of distrustful public attitudes towards their services or technology (Webb & Morrison 2004, Bowman & Hodge 2009). Moreover, the motivation of companies also can be largely profit-oriented in nature, such as increasing or maintaining customers, decreasing risk, or decreasing the likelihood of a legal violation and liability (Webb 2004). As direct economic benefit for the industry in the policy area of online child protection is clearly not a driving force to create or join self-regulatory initiatives, broad and vague commitments should be of no surprise.

3.2. MONITORING AND OVERSIGHT

There is wide support for the view that effective self-regulation requires independent or third-party monitoring and oversight (Schulz and Held 2002; CoP 2013, Latzer *et al.* 2007; 2013). Drawing upon the experiences of self-regulation in industries other than ICT, independent monitoring and compliance verification appears to be an important precondition for any effective industry self-regulatory arrangement (Bowman & Hodge 2009; Sethi and Emelianova 2006). No less important is the "willingness to make the findings of the independent external audit available to the public without prior censorship" (Sethi and Emelianova 2006, p. 230-231). Other scholars have similarly claimed that monitoring and disclosure clearly matters (Gunningham & Rees 1997; Doing & Wilson 1998; Jenkins 2001). Jenkins (2001, p. iv), in an analysis of corporate codes of conduct, recognized that it is essential to include provisions on effective monitoring into them in order to see an impact and, in addition, claimed that "the reluctance of many firms to include independent monitoring as an integral part of their code gives rise to some suspicion that they may be used as a public relations exercise rather than a genuine attempt at improving conditions and performance" (Jenkins 2001, p. 27).

Different oversight and monitoring mechanisms are used by each of the initiatives, ranging from external oversight to a pure information disclosure practice and self-reporting. Two of the initiatives, the SNS Principles and the ICT Principles, enjoy the strongest evaluation procedures carried out by independent third parties. Compliance with the SNS Principles is periodically measured through the evaluations carried out by external experts. However, their final reports are approved and published by the European Commission, causing doubts about the total independence of the conclusions. Since the adoption of the initiatives, two such evaluations have taken place (Staksrud & Lobe 2010; Donoso 2011). The evaluations were carried out in two steps: assessment of individual self-declarations of the participating SNS and practical testing of their websites. Overall, according to the latest assessment in 2011, only 3 from 14 self-declarations were assessed as "very satisfactory", while the remaining 9 were only "rather satisfactory" and 2 "unsatisfactory" (Donoso 2011). Self-declarations were better evaluated than their real implementation on the concrete websites, underlining the problem of objectiveness among participating SNS. Although the evaluation of other principles showed some signs of success, privacy was shown to be the area where the majority of the SNS failed to meet their commitments. Only 3 SNS from 14 providers were evaluated as very satisfactory. The main weakness noted by the assessor related to the lack of explicit information regarding the characteristics (e.g. age-appropriateness, availability, user- friendliness, etc.) of the privacy settings on the services and the lack of information regarding whether these services provide users with supporting information to help them make informed decisions about their privacy settings.

Yet, even positive evaluation does not necessarily reflect the practical impact that self-regulation has on Internet users. Although the majority of the tested SNS demonstrated some positive progress, tangible results, especially in the area of privacy protection, remain limited. As indicated by empirical evidence-based research, which compared SNS Principles with 9-16-year-old children's experiences and skills on the social networks, many industry players do not meet their commitments (e.g. in guaranteeing effective age-restriction or setting children's profiles to 'private') (Livingstone *et al.* 2013).

Similarly to the SNS Principles, the ICT Coalition has lately introduced an independent monitoring mechanism to evaluate how the Coalition members implement the ICT Principles. It established a position of an independent assessor who carried out his first

assessment in 2014 (O'Neill 2014). The evaluation was based on the statements of the ICT Coalition members, without actual testing of their services and products. Although individual commitments and best practices in the six broad areas related to online safety are to be applauded, the concrete implementation and measurement of compliance may be questioned. Given the above-mentioned trend among the SNS providers to self-declare more than is actually implemented, only formal evaluation of declarations without comparing them with the actual achievements may have an impact on objective assessment results. Moreover, due to the broad, and sometimes ambiguous, targets, it is not clear from the assessment to what extent (and if at all) all the members of the ICT Coalition achieved the agreed goals. The report, therefore, looks more like a summary of best practices rather than an assessment indicating the actual level of compliance.

Contrary to the external evaluation schemes mentioned above, which admittedly have their shortcomings, it is much more difficult to establish compliance in the case of the CEO Coalition. It does not undergo any formal monitoring process, despite its own evaluation of the work in progress. Such self-assessment took place after the first year of functioning of the CEO Coalition and was rather broad, recognizing that progress had been made in all the working areas but more effort was needed to achieve the agreed goals (CEO Coalition 2012). In February 2013, the CEO Coalition published its final report containing recommendations and best practice description (CEO Coalition 2013). In addition, in January 2014 individual companies produced separate reports on how they have implemented or will implement the recommendations of the Coalition (CEO Coalition 2014). Such a self-evaluation mechanism appears to be very subjective and limited.

In contrast, the FEDMA Code sets forth a well-defined and institutionalized monitoring mechanism. According to the Code, the burden of monitoring has been primarily shifted to the national direct marketing associations (DMAs). It is not surprising, as advertising, even if it is a cross-border phenomenon, is also "very often nationally distinctive, using the local language, characters, and humor familiar to the target audience" (Verbruggen 2013, p. 515). Therefore, a national rather than European system of adoption, review and enforcement seem to better serve the goal of voluntary governance. In practice, several of the DMAs have a compliance tool in place and carry out compliance monitoring, either when a company becomes a new member of the national association with subsequently action only on complaints, or involving monitoring the compliance with the Code on a more regular basis (Fiquet M 2015, personal communication). For example, some of the DMAs have a certification program every year or every two years (Fiquet M 2015, personal communication). In addition, the Code encourages the companies themselves to regularly monitor how they conform to the provisions of the Code (for example, via self-audits), but this is more a piece of advice rather than a strict obligation. In addition to the main enforcement efforts on the national level, a "Data Protection Committee" has been established on the European level at FEDMA to monitor the application of the Code, to consider annually if a revision of the Code is necessary and to provide the Article 29 Working Party with an annual report on the functioning of the code at national level and in cross-border activities. However, despite the established internal structures and the formal obligation to report to the national data protection authorities, the European Commission and the European Data Protection Supervisor (via the Article 29 Working Party meetings), FEDMA does not officially assess the extent to which its members comply with the code. Only some informal discussions on the functioning of the Code took place with the European Commission after the Code and the Annex were adopted (Fiquet M 2015, personal communication).

Lack of an independent monitoring scheme in the activities of the CEO Coalition can be seen as a very serious shortcoming. However, even if the remaining online safety initiatives are monitored and evaluated by independent experts, there are significant pitfalls: the final reports published by the European Commission may not be entirely independent, evaluation results may greatly depend on the methodology and sources used (actual testing of the services or evolution of self-declarations), and due to vague targets lack of a clear indication of the level of compliance. Also, the positive evaluation does not necessarily reflect the practical impact of self-regulation as, from the perspective of Internet users, empirical evidence may suggest that in reality companies fail to meet their commitments.

3.3. ENFORCEMENT

Enforcement of self-regulatory rules depends on the existence of and access to the procedures to handle possible complaints in relation to the infringement of the self-regulatory rules and the sanctioning of the members for established violations. Latzer *et al.* (2007, p. 21) identified the following elements of an adequate enforcement mechanism in relation to disputes and complaints: existence of a relevant enforcement organizational structure such as a unit to handle complaints, a defined enforcement and complaint handling procedure, a visible and well-known contact point to which to report potential infringements, an appropriate appeals mechanism. They claim that the level of enforcement can be measured based on the amount of complaints filed and disputes registered or any other modes of industry notice to members. Once a violation is found, a test of self-regulation effectiveness is "whether it has 'shown its teeth' to a member through some type of sanction" (Cave *et al.* 2008, p. 23), such as withdrawal of membership, or censure for non-compliance. The two elements of enforcement (i.e. complaint handling procedures and sanctioning mechanisms) will be analysed below.

Complaint handling procedures are not present in the majority of initiatives (the SNS Principles, the CEO and ICT Coalitions), with the exception of the FEDMA Code. The latter, being a European initiative, dedicates the establishment of procedures to solve any complaints that may arise from the application of the Code to the national DMAs. According to the information provided by FEDMA, the Code enforcement mechanisms have been put into practice and national DMAs have received and solved several complaints in cases of malpractice (Fiquet M 2015, personal communication). As set out in the officially established mechanisms, the complaints are normally handled by special compliance boards, ethic committees or similar commissions formed at the DMA level. Only if the DMAs appear to be unable to solve complaints due to their cross-border aspects, FEDMA could take up and investigate the dispute itself. The Code establishes a mechanism for that by stating that the investigation on the FEDMA level should be carried out by the Data Protection Committee, an internal body composed of representatives from national direct marketing associations, FEDMA and companies that are direct FEDMA members according to its internal rules of procedure. In practice, however, up to now FEDMA has not yet received or handled any cross-border complaints (Fiquet M 2015, personal communication). The small number of actual complaints may well be related not so much to procedural enforcement issues, but to practical difficulties for individuals in complaining about online behavioral advertising. Online advertising substantially differs from traditional print, broadcast or outdoor advertising (Verbruggen 2014). As "advertisements may appear only to individual consumers and perhaps only once, it can be difficult to prove that the ad was served and that it violated the applicable code(s) of conduct" (Verbruggen 2014, p. 97).

Neither the SNS Principles nor the CEO Coalition self-regulatory initiatives include any reference to sanctions. As a result, only symbolic sanctioning mechanisms relating to companies' reputation can be used in order to improve compliance. In cases of poor performance, the European Commission in practice tends to put pressure on companies through "naming and shaming" in public press releases. [6] In contrast, an explicit reference to sanctions is present in the FEDMA code and shortly mentioned in the ICT Principles. Pursuant to the Code, as national DMAs are responsible for the application of the Code, they have to apply the same sanctions stipulated in their countries for the breaching of their national codes. Most of the time the sanctions applied by the DMAs on the national level include "naming and shaming", DMA membership removal or passing the complaint to the national regulators, such as the national data protection supervisory authorities (Fiquet M 2015, personal communication). Moreover, depending on the type of violation, if the FEDMA Data Protection Committee gets to handle the complaint - which, as mentioned earlier, has not been the case until now - it can equally recommend the FEDMA Board to expel a member or apply other sanctions (e.g. "to initiate legal action against a member or a non-member in order to safeguard the ethics of the profession") (FEDMA 2003, p. 18). However, FEDMA is not able to enforce fines or apply other monetary sanctions due to the fact that it is a voluntary, fee-based membership organization and fines would diminish incentives for membership. To a lesser extent, a similar sanctioning possibility is present in the ICT Principles. The text of the Principles establishes a possibility to exclude a member, if it does not seek to apply the Principles. However, given the embryonic nature of the initiative, it is still not possible to know the extent to which the ICT Coalition will take this possibility seriously. In addition, contrary to the whole package of benefits that industry associations provide to its members (e.g. lobbying, good practice developments), exclusion from a Coalition does not seem to promise the same loss for companies and therefore calls into question the extent of the threatening power it may carry.

The absence of enforcement mechanisms and dissuasive sanctions in case of malpractice, and the lack of specific bodies to enforce them in the majority of the online child safety initiatives, present significant limitations. Reliance on symbolic sanctioning through public 'naming and shaming' does not help much to deal with violators or free riders. Sectorial industry associations, in contrast, tend to operate within a well-defined set of regulatory institutions and rules, which in turn provide for cohesive and appropriate organizational and sanctioning mechanisms for the implementation of self-regulatory rules. In addition, due to additional benefits besides being part of the voluntary rule-making process, industry associations have a much wider impact on their members if they impose exclusions as a sanctioning mechanism.

3.4. ORGANIZATIONAL STRUCTURE OF THE INDUSTRY

The availability of recognized organizations and their internal structures, such as secretariats and special committees, for regulatory tasks in the existing market environment may help to achieve a greater level of adoption and more effective implementation of self-regulatory rules. If a well-established organization in a particular segment can perform regulatory tasks and provide necessary organizational assistance, i.e. backup the initiatives, the practicability of adoption and compliance with voluntary schemes is much higher (Latzer *et al*. 2007). A significant difference exists between the FEDMA as a representative of a direct marketing industry and the other remaining multi-stakeholder dominated institutions in terms of their organization. FEDMA and the DMAs already have refined institutions, have experience with codes of conduct, and have necessary personnel and organizational structures that can

monitor implementation, handle complaints, and impose fines. The need for a particular organizational structure seems to be increasingly recognized, but still under development, in the ICT Coalition, which has appointed an independent evaluator, hired an external consultant, and sought transparent and open functioning processes (creating a website, providing information to relevant stakeholders, etc.). The remaining online child safety initiatives are characterized by loose bonds among their members, and operate more as cooperative and consensual technical networks rather than structured organizations. Such open governing structures, what regulatory scholars (Kohler-Koch 2002; Kooiman 2003; March 1998, and Rhodes 1997) would call governance networks, are issue-specific constituencies build by a public authority as an activator, which interact though multilateral negotiations in order to upgrade common interests while pursuing the individual benefit (Kohler-Koch 2002). This model brings its own disadvantages of loss of oversight and steering and fragmented coordination.

The absence of the proper organizational structures in the online child safety initiatives, and reliance on the European Commission in terms of organizational matters, may be seen as negatively influencing their performance. Yet, as Weber (2012, p. 3) reminds us, "cyberspace is not regulated or supervised by any of the existing bodies" and "there is a certain lack of sufficiently involved international organisations". Apart from industrial associations for specific sectors, there are no stable organizational structures for ICT policy domains where multi-sectoral and multi-stakeholder action to protect vulnerable users is required. When the focus of regulation is child safety and privacy risks in conjunction, only a combination of different stakeholders representing a wide range of online technologies, services, platforms and business models can propose solutions.

3.5. ROLE OF PUBLIC ACTORS

Potential intervention via hard-law by national or European authorities is considered to be an additional incentive for companies to adopt and enforce self-regulatory rules. The ability to pose a real regulatory threat of intervention by public bodies can enable better adoption and enforcement of self-regulation (Latzer *et al.* 2007). In addition to providing the shadow of hierarchy, i.e. threatening to adopt legislation unless private actors accommodate the legislators' demands in self-regulatory rules, public bodies can actually be involved in the adoption and implementation of self-regulation. Although self-regulatory rules related to public interest could hardly be adopted without any kind of involvement from public institutions, possible forms of such involvement greatly differ. The possible levels of institutional involvement range from encouragement (provision of carrots, inspiration) and appreciation on a political level to financial and personnel support, collaboration on an institutional level, or even co-regulation (direct control in a legal sense), periodic reviews performed by public officials, establishment of alternative scenarios in case of failure (sticks), and a clear definition of responsibility among industry and public authorities (Latzer *et al.* 2007).

The EU institutions have never publicly threatened the industry with real and immediate legal provisions on child safety if self-regulation fails to deliver expected results. Several areas, however, like personal data protection and behavioral advertising, have been touched upon or are under consideration by the European Commission. The recent revision of the European Data Protection Directive (96/46/EC) has given a possibility to address protection of children's privacy online. The newly adopted General Data Protection Regulation (2016/679) has, for the first time, explicitly recognized that children deserve specific protection of their personal data, as "they may be less aware of risks, consequences,

safeguards and their rights in relation to the processing of personal data" (Recital 38). The Regulation has introduced far-reaching changes in relation to the processing of children's personal data: it requires verifiable parental consent before processing personal data of children under the age of 16 (unless the Member States choose another age limit between 13 and 16), obliges companies to give information to children in a clear, audience-appropriate language, and foresees other additional rights and safeguards, such as the right to be forgotten. These legislative developments happened despite the fact that public consultation revealed the willingness of companies to develop codes of conduct together with the Article 29 Working Party and to ensure their proper enforcement rather than to have legislative provisions on child-related data protection matters (European Commission 2010). The actual influence of these new legislative provisions will, however, depend on how much practical guidance and specification the European Commission and data protection authorities will provide to companies implementing the General Data Protection Regulation.

Regarding the advertising sector, the "regulatory gorilla in the closet" (Verbruggen 2013) has been present for longer and felt more clearly. Children have been protected from Internet-based audiovisual services, programmes and advertisements as vulnerable consumers in the Directive 2010/13/EU on Audiovisual Media Services. Also, the European Commission is currently gathering evidence to explore whether the existing regulation is effective and adequate to protect children from online marketing in social media, online games and mobile applications, or whether changes are necessary in regulatory approach, including the initiatives taken by the industry (European Commission 2015). Based on the outcome of the exploration, potential amendments can be expected in relation to children as vulnerable consumers protected in the Guidance document to the Directive 2005/29/EC on Unfair Commercial Practices (SEC(2009) 1666) and to the upcoming review of the Directive on Audiovisual Media Services. It is difficult to establish any connection between the legislative initiatives mentioned above and the better performance of the self-regulation under analysis.

As mentioned above, an adequate level of support from the public institutions is considered to significantly enhance the performance of self-regulatory initiatives. In fact, it is often claimed that co-regulation is the most successful form of self-regulation. In the area under analysis, the EU is the most intensively involved in the SNS Principles and the CEO Coalition, but mainly in the form of inspiration and financial and personnel support. The SNS Principles are financed under the EU Safer Internet Programme and the European Commission provides supporting activities, hosts industry and stakeholder meetings, hires independent experts for periodic assessments, publishes assessment results on its website and evaluates the compliance via press releases. Similarly, the CEO Coalition has been initiated by the Commissioner N. Kroes in person, inviting specific companies to participate in the initiative. In addition, the EU supports the work of the CEO Coalition on financial, know-how (Commission representatives participate in Coalition meetings) and organizational levels (hosts stakeholder meetings, publishes information on its website). Yet, as emphasized earlier, the rules of both initiatives are broad and rely more on good-will commitments rather than enforceable obligations resulting in limited added value to actual protection.

It therefore seems that content approval is more important for initiatives than procedural and political support, which may guarantee that industry takes on board all the most relevant public policy issues and challenges - in other words avoiding pick and choose tactics - as well as formulating clear and enforceable rules. In this respect, contrary to the SNS Principles and the CEO Coalition, the FEDMA code seems to experience a more balanced support from the public authorities. Although initiated entirely by the direct and

online marketing industry, the European Commission together with the Article 29 Working Party has been closely involved in the drafting procedure of the Code. The rules on the protection of children are the direct result of such involvement as the Annex had been approved as compliant with and adding value to the EU data protection rules only after the provisions of child protection had been introduced.

As a result, the approval of self-regulatory rules as a procedural step in order to adopt a European code of conduct is not only a desired "political backing" of the self-regulatory rules for the industry but also a guarantee for those to be protected that their interests and societal values will be taken into account.

Table 2. Assessment of the four initiatives

Criteria		SNS Principles	CEO Statement	ICT Principles	FEDMA Code
Content of the rules	Prescriptive, measurable rules	-	-	-	✓
	Broad statements of intent	✓	✓	✓	-
Monitoring & oversight	Internal self-assessment	✓	✓	✓	✓
	External assessment by an independent party	✓	-	✓	-
Enforcement (complaints & sanctions)	Existence of a body to handle complaints	-	-	-	✓
	Defined complaint handling procedure	-	-	-	✓
	Reputational sanctions	✓	✓	✓	✓
	Organizational sanctions (expulsion, membership suspension)	-	-	✓	✓
Organisational structure	Industry association	-	-	-	✓
	Ad-hoc network/coalition	✓	✓	✓	-
Role of public actors	Initiator of the initiative	✓	✓	-	-
	Approver of the rules	-	-	-	✓

4. THE WAY FORWARD

This analysis showed significant limitations of self-regulation in the online child safety area, characterized by broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions compared to a sector specific, institutionalized European code of conduct in the area of advertising.

Drawing on the differences in the online child safety and advertising domains, it seems that the policy goal of protecting children's privacy online can be approached from two different angles. Privacy can be viewed from a social or informational lens. The online child safety initiatives are mainly concerned with social privacy, a concept often used by the American

scholars to note "the ability to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics" (Boyd 2014, p. 60) in the networked publics. It refers more to the negotiation of social boundaries, in particular to the management of diverse audiences through privacy settings and controls, and is entangled with online safety. The concept of social privacy and the risks to it relate to various values to be protected that are at stake, such as seclusion, intimacy, identity, reserve, self-determination and autonomy. Social privacy, being about control of social situation and context (e.g. hiding from public environments), is a broad concept and significantly differs from informational privacy, which refers just to the control of the flow of personal data (Westin 1967). Informational privacy, a more European concept, and even more precisely protection of personal data from illegal and illegitimate collection and use, instead, is the focus of the sectoral – and not surprisingly European in its nature – FEDMA Code. While dealing with informational privacy in terms of personal data protection, a single risk and one well-defined facet of privacy, the rules and requirements for legitimate data processing are very clearly set in a legislative framework and, therefore, can be easily implemented also on a voluntary level. As a result, while addressing social privacy, with its inherently different safety and privacy risks on the Internet, in one initiative, the multi-scope online child safety initiatives unavoidably use deliberately vague language, leaving the companies to decide for themselves how they will respect each of the agreed requirements. It would be very difficult, if not impossible, to address all the aspects of social privacy in a uniform and measurable way. Consequently, clear and detailed rule-making is only possible when the rules aim to mitigate a single informational privacy risk, such as personal data misuse, in the sectorial code of the advertising industry. As a result, without denying the need for general rules to protect other aspects of privacy, it would be more beneficial to self-regulate online child privacy issues separately from safety initiatives and use sectorial industry associations for such self-regulatory tasks.

Such a human rights-based approach, instead of a safety-based approach, would consequently require the EU to take a stronger and better defined self-regulatory strategy. The conditions for that seem to be envisioned in the General Data Protection Regulation. It encourages associations and other bodies to prepare codes of conduct for the purpose of specifying the application of data protection provisions when the personal information is collected from children. The Regulation also requires an independent body which has an appropriate level of expertise and is accredited by the competent supervisory authority, to monitor compliance with codes of conduct. More reliance on sectorial codes would not only bring online privacy protection mechanisms more in line with the human rights perspective, but also possibly lead to clear rules given the possibility for public authorities to approve their content and the similarity of the industry players. As noted by Bennet (2004, p. 232), the main defining feature of the industry associations and their codes is "a broad consonance of economic interest and function, and by extension a similarity in the kinds of personal information collected and processed", and "sectoral codes permit, therefore, a more refined set of rules tailored to the issues within each industry".

The aim of the online child safety initiatives to empower the users through technological solutions to manage their social privacy could, instead, be partially realized by putting more pressure on the industry providing online services for children to implement the privacy by design and privacy by default principles. Special privacy protection tools should be implemented at the early design stage of online services and products offered to children and enabled by default. For example, services and applications could be designed in a way that only the minimum amount of personal data necessary to deliver the services are collected from children, and children are not subject to online behavioural targeting,

including profiling. Privacy settings and reporting tools could be prominently placed, easily accessible across all connected devices and age appropriate by default.

CONCLUSIONS

Achieving effective industry self-regulation is never easy, especially in a rapidly changing, multi-jurisdictional, multi-stakeholder dominated online environment.

This article analyzed four specific self-regulatory initiatives aiming to protect online child privacy. A formal self-regulatory process analysis focused on the procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects of the initiatives, and demonstrated significant limitations of self-regulation in the area of online child safety compared to the area of online advertising. The former suffers from limitations due to broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions. The comparison provides an opportunity to distinguish several features that can possibly contribute to greater effectiveness of the self-regulatory schemes to protect the online privacy of children.

First, clearly defined voluntary rules and measurable standards, rather than a broad statement of objectives, can enable better adoption and action of the voluntary initiatives in practice. In addition, formal approval of the industry formulated rules by public authorities can help to take into account public interests. However, it has been recognized that refined and detailed rule-making is possible when the rules aim to mitigate a single privacy risk, such as personal data misuse. Online child safety initiatives, where different risks and various aspects of social privacy are at stake, require multi-stakeholder dominated platforms which manage to agree only on broad statements and principles. They can hardly be prescriptive and provide technical implementations, as they inherently focus on desired outcomes, leaving a large margin of manoeuvre for implementation to individual companies. As a result, their adoption and implementation is inevitably more complicated and less measurable.

Second, lack of independent monitoring schemes and the absence of enforcement mechanisms and dissuasive sanctions in cases of malpractice in the majority of the online child safety initiatives could be mitigated by the availability of organizational structures for self-regulatory tasks. An industry association of a particular sector, through "institutionalization" of self-regulation, would not only provide the necessary personnel and organizational structures to enforce self-regulatory rules and impose fines for non-compliance, but also due to the additional benefit provided to its members, such as lobbying, education and training, could exercise a threatening power in case of exclusion. However, such stable structures do not exist yet in cases where multi-sectoral action to mitigate online privacy and safety risks is necessary.

Therefore, it has been argued that it would be more beneficial to tackle online child privacy issues separately from safety initiatives and use sectorial industry associations for the self-regulatory task. This would not only bring online privacy protection mechanisms more in line with the human rights perspective, but also lead to clear and more enforceable rules given the possibility for public authorities to approve their content and the similarity of the industry players.

Such a human rights-based approach, instead of a safety-based approach, would consequently require the EU to take a stronger and better defined co-regulatory strategy. The new General Data Protection Regulation envisions a similar future and encourages associations to adopt approved and monitored codes of conduct for the purpose of specifying the application of data protection provisions when processing children's personal data.

The aim of the online child safety initiatives to empower the users through technological solutions to manage their social privacy, instead, could be partially realized by putting more pressure on the industry to implement the privacy by design and privacy by default principles, also present in the Regulation.

Although the existing self-regulatory initiatives in the area of online child safety may be criticized, the broader potential of private governance networks in this domain should not be denied. Self-regulation "has advantages over no regulation at all" as even if doubtful in effectiveness it can overcome market failures and prevent violations of economic and privacy interests of the users (De Haan *et al.*, 2013, p. 112). Apart from effective or ineffective regulatory outcomes, the process of self-regulation alone may create innovation, permit mutual learning, awareness raising, sharing of resources among industry and other stakeholders. Due to the fact that the industry takes up the regulatory responsibility, some industry players may propose new technical solutions to protect children from online privacy risks (e.g. age-verification mechanisms, privacy by default measures, parental controls). From a user perspective, any improvement of privacy features and policies in online services and mutual change can be considered a sign of success of a regulatory process. The question is whether the initiatives that aim to bring industry together into networks for sharing knowledge and experience without adequate rules, monitoring and enforcement procedures should be called 'self-regulation' or this term should only be allowed "when it was surrounded by heavy qualifications or caveats" (Carr, 2015).

REFERENCES

A29WP (Article 29 Data Protection Working Party) (2003) Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 77, 13 June 2003.

A29 WP (Article 29 Data Protection Working Party) (2010) Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 174, 13 July 2010.

Ayres I, Braithwaite J (1992) *Responsive Regulation: Transcending the Deregulation Debate.* Oxford University Press, Oxford.

Barlow J.P. (1996) A Declaration of the Independence of Cyberspace. [Last accessed 20 June 2015]. Available from URL: https://projects.eff.org/~barlow/Declaration-Final.html

Bennett C. J. (2004) Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else? In: Webb K (ed), *Voluntary Codes: Private Governance, the Public Interest and Innovation,* pp. 227-249. Carleton University, Ottawa.

Bonnici M.J.P. (2008) *Self-regulation in Cyberspace*, T.M.C. Asser Press, The Hague.

Bowman D.M., Hodge G.A. (2009) *Counting on codes: An examination of transnational codes as a regulatory governance mechanism for nanotechnologies* ,Regulation & Governance 3(2), pp. 145-164.

boyd d. (2014) *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, New Haven, CT.

Carr J (2015) Big Brains in Berlin [Blog post]. [Last accessed 20 June 2015] Available from URL: https://johnc1912.wordpress.com/2015/04/22/big-brains-in-berlin/

Cave J, Marsden C, Simmons S (2008) Options for and Effectiveness of Internet Self- and Co-Regulation. RAND Europe. [Last accessed 20 June 2015] Available from URL:http://ec.europa.eu/dg/information_society/evaluation/data/pdf/studies/2006_05/phase2.pdf

CEO Coalition (2011) Statement of Purpose. [Last accessed 29 July 2014]. Available from URL: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ceo_coalition_statement.pdf

CEO Coalition (2012) Report of Mid-term review meeting of the CEO Coalition to make the Internet a better place for kids (2012). [Last accessed 29 July 2014]. Available from URL: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/report_11_july.pdf

CEO Coalition (2013) Summary report. [Last accessed 20 June 2015] Available from URL: https://ec.europa.eu/digital-agenda/node/61973

CEO Coalition (2014) Progress reports on actions to make the Internet a Better Place for Kids. [Last accessed 20 June 2015] Available from URL:http://ec.europa.eu/newsroom/dae/itemdetail.cfm?item_id=14391

CoP (Community of Practise) (2013) Principles for Better Self- and Co-Regulation. [Last accessed 20 June 2015] Available from URL: http://ec.europa.eu/digitalagenda/sites/digitalagenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf

De Haan J, Van der Hof S, Bekkers W, Pijpers R (2013) Self-regulation. In: O'Neill B, Staksrud E, McLaughlin S (eds.) *Towards a better Internet for Children. Policy pillars, player and paradoxes*, pp. 111-129. Nordicom, Gothenburg.

Doig A, Wilson J (1998) The Effectiveness of Codes of Conduct. *Business Ethics: A European Review* 7, 140-149.

Donoso V (2011) Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 14 Social Networking Sites. European Commission, Safer Internet Programme, Luxembourg.

EDRi (European Digital Rights) (2013) *CEO Coalition - the blind leading the bland*. [Last accessed 20 June 2015] Available from URL:http://edri.org/ceo_coalition.

European Commission (1996) Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (1996) 483 final.

European Commission (2006) Communication from the Commission - Towards an EU strategy on the rights of the child, COM(2006) 0367 Final.

European Commission (2009) Safer Social Networking Principles for the EU. [Last accessed 29 January 2015]. Available from URL:https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf .

European Commission (2010) Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data, 4 November 2010. [Last accessed 29 July 2014]. Available from URL:http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf .

European Commission (2012) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children, COM(2012) 196 Final.

European Commission (2015) Inception Impact Assessment, REFIT Evaluation and Impact Assessment of the EU Audiovisual Media Services Directive 2010/13/EU (AVMSD). [Last accessed 15 May 2016] Available from URL: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_006_cwp_review_avmsd_iia_en.pdf

FEDMA (2003) FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing. [Last accessed 20 June 2015] Available from URL: http://www.fedma.org/fileadmin/documents/SelfReg_Codex/FEDMACodeEN.pdf

FEDMA (2010) European Code of Practice for the use of personal data in direct marketing electronic communications Annex. [Last accessed 20 December 2014]. Available from URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_annex_en.pdf

Gunningham N (1995) Environment, Self-regulation, and the Chemical Industry: Assessing Responsible Care. *Law & Policy* 17, 57-109.

Gunningham N, Grabosky P (1998) *Smart Regulation: Designing Environmental Policy*. Oxford University Press, Oxford.

Gunningham N, Rees J (1997) Industry Self-regulation: An Institutional Perspective. *Law & Policy* 19, 363-414.

ICT Coalition (ICT Coalition for Children Online) (2012) ICT Principles. [Last accessed 29 January 2015]. Available from URL:http://www.ictcoalition.eu/.

International, The Netherlands.

Jenkins R (2001) *Corporate Codes of Conduct: Self Regulation in a Global Economy.* United Nationals Research Institute for Social Development, Geneva.

Kohler-Koch B (2002) European Networks and Ideas: Changing National Policies? *European Integration Online Papers*, 6(6).

Kooiman J (2003) *Governing as Governance*. Sage, London.

Koops B.J, Prins C, Schellekens M, Lips M (eds) (2006) *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners*. Information Technology & Law Series (9). T.M.C. Asser Press, The Hague.

Latzer M, Just N, Saurwein F (2013) Self- and co-regulation: evidence, legitimacy and governance choice. In: Price M E, Verhulst S G, Morgan L (eds), *Routledge Handbook of Media Law*, pp. 373-397. Routledge, Abingdon / New York.

Latzer M, Price M.E., Saurwein F, Verhulst S.G. (2007) *Comparative Analysis of International Co- and Self-regulation in Communication Markets*, Research report. OFCOM, Vienna.

Lievens E (2010) *Protecting Children in the Digital Era: the Use of Alternative Regulatory Initiatives*. Martinus Nijhof Online, Leiden.

Livingstone S (2011) Regulating the Internet in the Interests of Children: Emerging European and International Approaches. In: Mansell R. Raboy M (eds) *The Handbook of Global Media and Communication Policy*, pp. 505-524. Wiley-Blackwell, Oxford.

Livingstone S, Haddon L, Görzig A, Ólafsson K (2011) *Risks and safety on the Internet: The perspective of European children.* Full Findings. LSE, EU Kids Online, London.

Livingstone S, Ólafsson K, O'Neill B, Donoso V, (2012) *Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition.* LSE, EU Kids Online, London.

Livingstone S, Ólafson K, Staksrud E (2013) Risky Social Networking Practises among "underage" Users: Lessons from Evidence-Based Policy.*Journal of computer-Mediated Communications*, 303-320.

March D (1998) *Comparing policy networks*, Open University Press, Buckingham.

Mascheroni G, Ólafsson K. (2014) Net children go mobile: risks and opportunities (2nd ed.). Educatt, Milan.

O'Neill B (2014) First report on the Implementation of the ICT Principles. The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU, Brussels. [Last accessed 20 June 2015] Available from URL: http://www.ictcoalition.eu/

O'Neill B, Livingstone S, McLaughlin S (2011) Final recommendations for policy, methodology and research. LSE, EU Kids Online, London.

O'Neill B, Staksrud E, Mclaughlin S (2013) *Towards a better internet for children: policy pillars, players and paradoxes*. Nordicom, Gothenburg.

Rees J (1997) *The Development of Communitarian Regulation in the Chemical Industry. Law and Policy 19, 477-528.*

Rhodes R.A.W. (1997) *Understanding Governance. Policy Networks, Governance, Reflexivity and Accountability*. Open University Press, Buckingham.

Schulz W, Held T (2002) Regulierte Selbstregulierung als Form modernen Regierens. Im Auftrag des Bundesbeauftragten für Angelegenheiten der Kultur und der Medien, Arbeitspapiere des Hans-Bredow-Instituts nr. 10. Verlag Hans-Bredow-Institut, Hamburg.

Scott C, Cafaggi F, Senden L (2011) The Conceptual and Constitutional Challenge of Transnational Private Regulation. *Journal of Law and Society*38(1), 1-19.

Scott C (2012) Beyond Taxonomies of Private Authority in Transnational Regulation. *German Law Journal* 13, 1329-1338.

Sethi S.P., Emelianova O (2006) A Failed Strategy of Using Voluntary Codes of Conduct by the Global Mining Industry. *Corporate Governance: The International Journal of Effective Board Performance* 6, 226-238.

Staksrud E, Lobe B (2010) Evaluation of the implementation of the Safer Social Networking Principles for the EU Part I: General Report. European Commission Safer Internet Programme, Luxembourg.

Van der Hof S (2014) No Child's Play: Online Data Protection for Children. In: Van der Hof S, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web - Regulating Online Child Safety*, pp. 127-141. TMC Asser Press / Springer Press, The Hague.

Verbruggen P (2013) *Gorillas in the closet? Public and private actors in the enforcement of transnational private regulation,* Regulation & Governance 7(4), pp. 512-532

Verbruggen P (2014) *Enforcing Transnational Private Regulation: A Comparative Analysis of Advertising and Food Safety*. Edward Elgar, Cheltenham.

Webb K (2004) Understanding the Voluntary Codes Phenomenon. In: Webb K (ed), *Voluntary Codes: Private Governance, the Public Interest and Innovation,* pp. 3-35. Carleton University, Ottawa.

Webb K, Morrison A (2004) The Law and Voluntary Codes: Examining the "Tangled Web." In: Webb K (ed) *Voluntary Codes: Private Governance, the Public Interest, and Innovation*, pp. 97-174. Carleton University, Ottawa.

Weber R.H. (2002) *Regulatory models for the Online World*. Schulthess, Zurich.

Weber R.H. (2012) Future Design of Cyberspace Law-"Laws are Sand" (Mark Twain, The Gorky Incident), *Journal of Politics and Law* 5(4).

Westin A. F (1967) *Privacy and freedom*. 1st ed. Atheneum, New York.

---

[1] Due to the significant degree of involvement and input on the part of the European Commission into the online child safety self-regulatory initiatives, it is difficult to apply a clear categorization to the adopted initiatives and label them self-regulation or co-regulation. Given the existing rich typology of Internet co-regulation and the difficulty of clearly separating self-and co-regulation both as concepts and as practices, this paper refers to the initiatives under analysis as self-regulatory initiatives. It uses the term 'self-regulation' in a broad sense, encompassing a process of rule setting wherein the industry alone or together with other stakeholders formulates the rules, enforces and adjudicates them. In this sense, it follows the definition of self-regulation provided by the EU itself in point 22 of the Interinstitutional Agreement on Better Law Making (OJ EU 321/1, 31.12.2003), denoting "the possibility for economic operators, the social partners, non-governmental organizations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)".

[2] For the sake of comprehensiveness, one additional self-regulatory initiative should be mentioned - The European Framework for Safer Mobile Use by Young Teenagers and Children (2007) Available from URL: http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/04/saferchildren.pdf [Last accessed 20 December 2014]. This initiative is excluded from the analysis in this paper because it focuses merely on online child safety, excluding online privacy from its content.

[3] The existence of similar international initiatives, such as the IAB Europe EU framework for Online Behavioural Advertising ([Last accessed 20 July 2015] Available from URL: http://www.iabeurope.eu/files/5013/8487/2916/2013-11-11_IAB_Europe_OBA_Framework.pdf) and the EASA Best Practice Recommendation on Online Behavioural Advertising 2011 ([Last accessed 20 July 2015], Available from URL: http://www.easa-alliance.org/page.aspx/386) should be acknowledged. However, due to the lack of substantial provisions on children's privacy (they entail only a prohibition to create segments for online behavioural advertising purposes that are specifically designed to target children under the age of 12) and the overall focus of this paper on the European level, these self-regulatory initiatives were left outside the scope of the paper.

[4] ICT Coalition, 'A brief description who we are'. [Last accessed 1 May 016]. Available from URL: http://www.ictcoalition.eu

[5] The exact implementation of the FEDMA Code rules is left to the national direct marketing associations (DMAs) and may vary from country to country. Some DMAs can go

further than the Code requirements and reformulate as well as implement the rules more rigidly, some can just take the principles and adapted them in their national codes while some other simply translate the FEDMA Code into their language.

[6] See for example, European Commission - Press release, 2011, Digital Agenda: only two social networking sites protect privacy of minors' profiles by default. [Last accessed 29 July 2014]. Available from URL: http://europa.eu/rapid/press-release_IP-11-762_en.htm