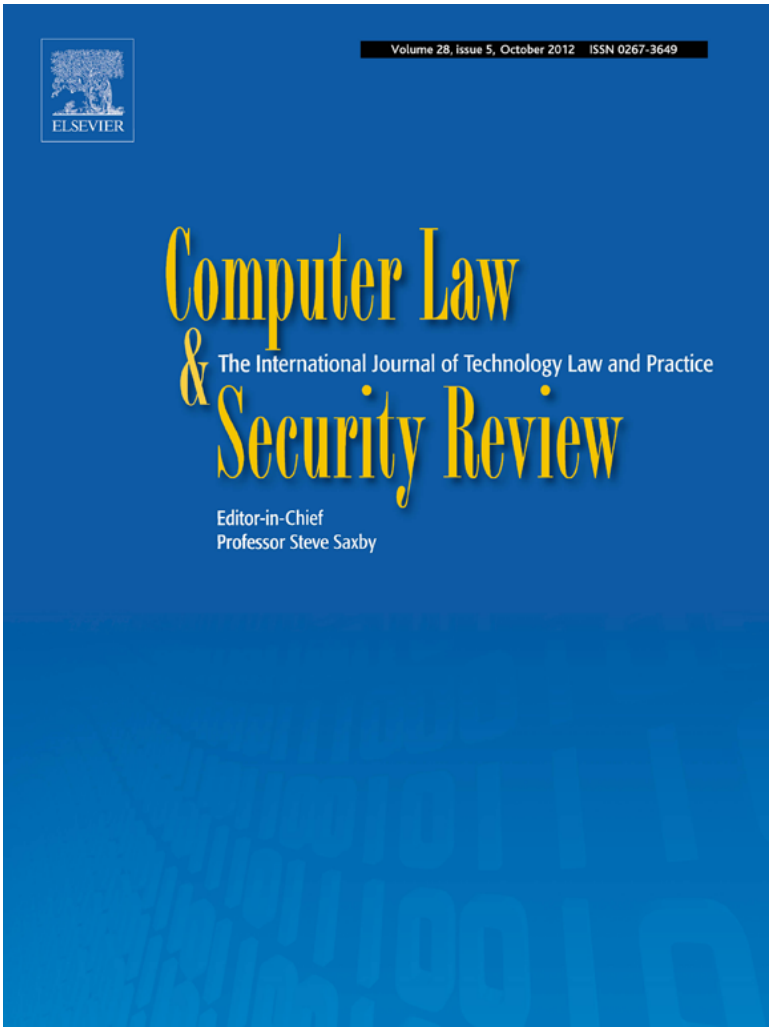

COMPUTER LAW & SECURITY REVIEW 28 (2012) 551–559

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Trust in the information society

Brian O'Neill

Dublin Institute of Technology, College of Arts and Tourism, Dublin, Ireland

Keywords:
Trust
Online safety
Safer Internet policy
Protection of minors
EU Kids online

ABSTRACT

Trust is an important feature for all users of the Internet who rely on the safety and security of network technologies and systems for their daily lives. Trust, or the lack of it, has also been identified by the European Commission's *Digital Agenda* as a major barrier to further development of the information society in Europe. One of the areas in which concerns have been raised is in relation to children's safety online. As a result, substantial efforts have been made by policymakers and by the industry to build greater trust and confidence in online digital safety. This paper examines what trust means in the context of children's use of the Internet. Should policy on trust enhancement, for instance, include children's own trust in the technologies or services they use or is it sufficient to seek to reinforce parental and adult confidence that children can be adequately protected? What is required to build that trust from either perspective? Does it need, or should it include a relationship of trust between parents and children? To tease out these questions further, the paper examines current European Union policy frameworks on digital safety, particularly industry responses to the call for a more trusted Internet environment for children, and argues that technical solutions to be effective need to carefully balance a number of competing objectives and to be sufficiently grounded in evidence of parental and child experience of the Internet.

1. Introduction

> *Europeans will not embrace technology they do not trust — the digital age is neither "big brother" nor "cyber wild west".* (A Digital Agenda for Europe, 2010)

As recently observed in a European Commission communication, the Internet is something that was originally designed for adults and not for children (European Commission, 2012a). However, given that children now use it in very large numbers and at an increasingly young age, issues of digital safety and welfare of young people online have taken on a major importance for policymakers. Most recently, as cited above in *A Digital Agenda for Europe*, the European Union's strategy for the information society, trust in the Internet has been linked with confidence in the safety of the online world for children. "Europeans will not engage in ever more sophisticated online activities", the strategy argues "unless they feel that they, or their children, can fully rely upon their networks" (European Commission, 2010). In the Digital Agenda Assembly of 2011, the European Vice-President Neelie Kroes gave an extraordinary emphasis to the importance of reinforcing trust in children's safety online. The "huge positive social, cultural and economic potential of the Internet" could only be unlocked, she argued, if barriers to trust were overcome, including such seemingly intractable problems such as bullying, harmful material and abuse suffered by children online. To this end, she called on a coalition of CEOs of all industry groups to come up with concrete proposals to see how this could be achieved within a short timeframe (Kroes, 2011).

The foregrounding of trust as an issue comes at an important time in policy debates about the future of the

0267-3649/$ – see front matter © 2012 Brian O'Neill. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2012.07.005

Internet and whether it should be subject stricter regulation and control. Concerns about trust to date have been concerned primarily with issues of cybersecurity, such as protection against terrorist attacks as well as the protection of citizens' interests against fraud and other forms of cybercrime. Trust in the context of children's online safety is a new emphasis – even if the distribution of child abuse material is one of the most discussed and notorious forms of cybercrime – and brings to the fore a number of important issues and debates about what constitutes a trustworthy online environment for children. Moreover, a consideration of trust in this context raises key questions about what kinds of trusted relationships are involved. Who is doing the trusting and how can such trust be justified and maintained? As discussed in the following, trust is a complex and multi-faceted phenomenon, combining individual as well as more general experiences and perceptions, technical attributes as well as a social dimension. In the case of policy related to child protection, there is also the delicate balancing act between, on the one hand, promoting opportunities and supporting rights to freedom of expression and exploration, with the need for appropriate measures to protect children's safety.

The field of digital safety is typically presented as a multi-stakeholder one with responsibility for protection shared across a variety of institutions, social and policy actors, as well as with parents and children themselves. So it is with trust, and in this paper the distinct relationships (trust between children and adults, trust between adults and Internet service providers, trust between government and industry etc.) all combine to create conditions in which trust is either won or lost. But to further elucidate what is required to create the optimal conditions for trust, it is necessary to define how trust as a concept is being deployed.

2. Trust and the Internet

The Internet, as most commentators agree, offers the most extraordinary extension of potential for social interaction of our times and represents an extreme context in which trust may be developed or indeed tested (Hardin, 2006). Trust is central to the everyday lived experience of the Internet due in no small measure to reliance by citizens and consumers on Internet technologies for communicative and commercial interactions. In a wide-ranging literature that draws on its technological, legal and social dimensions, there is a strong consensus that trust is a core concept of information systems and their implementation in society. Widely diverging perspectives on its implications, however, prevail (De Paoli and Kerr, 2008). Trust, in the context of this paper, draws primarily on the sociological approach and refers to the relationships that exist when an actor or *trustor*, places confidence or reliance on another *trustee* with respect to an object of *trust* (Hardin, 2006). Trust is thus at minimum a binary or dyadic relationship between trustor and trustee (O'Hara and Shadbolt, 2005) but in practice, encompasses an increasingly complex set of mediated and networked relationships involving both individuals and institutions as social agents.

The social relationship that constitutes trust is defined by Hardin as one in which we believe the trusted person or object has 'the right intentions towards us' and is competent to do what we trust them to do (Hardin, 2006). This, he argues, is primarily a cognitive matter in that it depends on an assessment, based on relevant knowledge, of the trustworthiness of the potentially trusted person or object. Trust is, therefore, not a simple matter. A number of factors come into play in the forming of judgements about trustworthiness such as availability of evidence, expectations based on prior experiences – both good and bad, personal motivation deriving from anticipated benefits of trusting, and disposition to risk-taking. Some definitions also point to a strong ethical or values-based underpinning for trust. Cohen-Almagor defines trust as "confidence, strong belief in the goodness, strength, reliability of something or somebody" (Cohen-Almagor, 2010), an indicator of the quality and transparency of relationships between people (and things) that enable 'trusted' interactions to take place. In this case, the decision to trust or not is based, less on knowledge than on conformity with a belief system and whether the object of trust, in our case perception of what the Internet offers, is in keeping with moral conceptions of what is trustworthy. In the rational model of 'encapsulated interest' espoused by Hardin (2006), trust is rooted in the mutual recognition of respective interests and benefits of trusting within a framework of ongoing relationships.

To date, most attention has been focused on the trustworthiness of the Internet as a platform for e-commerce or e-government services. In this context, the Internet has been described as an 'experience technology': higher levels of experience tend to engender greater levels of trust with Internet users gaining more confidence and skill in the use of online services over time (Dutton and Shepherd, 2003). Yet while the underlying technical features of security are important in contributing to the conditions for trust, a social understanding of trust focuses less on how people's attitudes and behaviour towards technology in favour of thinking about trust, online or offline, as a relationship between people (Friedman, 2000). While it may not always be possible to identify trust in the online world with direct dyadic relationships, ultimately the existence or absence of trust comes down to the question of the possibility or risk of betrayal by others (Cheshire et al., 2010). Experience and skill in negotiating the online world may reduce the risk of entering situations where there is higher likelihood of betrayal. It cannot mitigate it entirely however; neither can it account for the impact of prior negative experiences or third-party reputational information, both of which can have a profound impact on trust (Cook, 2003).

Just how far trust as experienced in the offline world translates into online life is an area of dispute. Online interactions, while closely mirroring and resembling real world social life, conceal many of the features that contribute to trust, and present new kinds of relationships across time and space, that would not be possible in the offline world (Nissenbaum, 2001). Furthermore, identities are frequently hidden or misrepresented, social roles are lacking and many of the traditional cues for building and maintaining trust are simply absent in cyberspace. Thus, as the Internet has developed from being a network of enthusiasts and techno-experts into a mass phenomenon, the potential for dissimulation, fraud, exploitation and abuse of trust has magnified

exponentially (Mansell and Collins, 2005). As such, trust – or the lack of it – has become a major obstacle to governments' efforts to further develop the information society, and in particular the digital economy. Wide variations of trust and excessive media attention about the negative aspects of cybercrime or illegality online have made citizens cautious and guarded in their adoption of e-commerce and e-government services (Dutton and Shepherd, 2003). At the same time, rapid uptake of new services and technologies, such as social networking, cloud computing and reliance on Internet-connected devices suggest different kinds of attitudes prevail and different levels of trust exist according to the context in which online services are used.

Each of these considerations bears particularly on the topic of children's use of the Internet. From a developmental perspective, trust has long been recognised as fundamental to child and adolescent psychosocial growth, essential to the child's development of feelings of safety and security in the world (Erikson, 1950; Rosenthal et al., 1981). Such trust depends greatly on the quality and reliability of the child's caregivers, without which children may fail to develop trust or learn to perceive the world as inconsistent and unpredictable. In online terms, children's safety and security has been a priority since the early development of the World Wide Web, through a variety of legislative and regulatory measures reflecting strong international consensus on the rights of the child to protection in the online world (United Nations, 1989; Flint, 2000; UNICEF, 2011). Accordingly, a range of both government and industry-sponsored schemes has evolved to provide additional layers of protection where children's use of the Internet is concerned. These include age-rating classification schemes for online content, filtering systems to block content that may be unsuitable or harmful, reporting systems to alert similarly harmful or unsuitable content, all of which are intended to create conditions of security and safety that facilitate the fostering of trust in the Internet for learning, information and communication.

Three particular issues stand out in policy debates about such forms of protection. Firstly, the mediation of children's access to the Internet varies considerably, ranging from highly restrictive and protective approaches to libertarian and permissive. Parental mediation of children's use of the Internet, in the first instance, as with all forms of media and entertainment, structures and defines the nature of the access that young people may enjoy. Similarly, schools, peer cultures and the wider society act as strong mediating factors in young people's developing relationships, many of which are now conducted online. The contextual knowledge, therefore, contributing to judgements about trustworthiness are filtered through different relationships, the most important of which are those that exist between parents and children, and between children and their peers, teachers and other influential socializing agencies. In each instance, knowledge, experience and trust are important factors in determining the outcomes involved.

Secondly, the Internet industry as the object of trust in this instance, assumes special responsibility when it comes to acting as a gateway or providing services to minors. In contrast to the *caveat emptor* principle that may be said to characterize the adult population's relationship to the Internet, services provided for children are subject to higher degrees of regulation and more stringent criteria of safety, security and reliability. While children access many services not specifically designed for their age group, the Internet industry overall has adopted, or has been encouraged to adopt, a responsible attitude to ensure where persons under the age of eighteen access their services, that appropriate mechanisms are in place to ensure their safety and welfare. In other words, there is a greater onus on industry in the context of young people's use of the Internet to reciprocate trustworthiness and to minimize the risk of any harm resulting.

Thirdly, the assumed costs and burden that arises from ensuring safety in the online world for children is one that leads to deep divisions between advocates of free expression on the Internet and those proposing stronger child protection measures. Creating a more trusted environment, it is argued, leads to greater restriction overall, constrains innovation and comes at the expense of benefitting the population as a whole (Powell et al., 2010). Trust in this sense involves the demonstrable reduction or elimination of risk but undermines some of the fundamental values upon which the Internet was founded and destroys its potential for future innovation (Zittrain, 2008).

Such tensions inevitably resonate within any consideration of trust in the context of children and the Internet. Yet, it is in the policy arena that the issue has been debated most, the principal features of which are reviewed in the following section.

3. *The Digital Agenda*, trust and safer Internet policies

The overarching policy framework within which trust, specifically trust in relation to children's use of the Internet, has been identified as a fundamental objective is that of the Digital Agenda, Europe's overarching strategy for the promotion of the information society (European Commission, 2010). Intended to deliver the economic and social benefits deriving from a single digital market, the Digital Agenda builds on the European Union's ambition to be among the most competitive and dynamic knowledge-based economies in the world. Citing some of the persistent obstacles to full realisation of the information society, the Digital Agenda is framed against a recognition that digital inclusion remains a significant challenge. 30% of Europeans have still never used the Internet; the quality of Internet access remains uneven; other regions in the world – the US, Japan and South Korea – far exceed participation rates and investment in digital technologies. Arguing that a lack of trust in the online environment is among the factors 'seriously hampering the development of Europe's online economy' (European Commission, 2010), the Digital Agenda cites Eurostat data that only '12% of European web users feel completely safe making online transactions. Threats such as malicious software and online fraud unsettle consumers and dog efforts to promote the online economy' (p. 16). In summary, it argues:

> *Europeans will not engage in ever more sophisticated online activities, unless they feel that they, or their children, can fully rely upon their networks. Europe must therefore address the rise*

> *of new forms of crime – "cybercrime" – ranging from child abuse to identity theft and cyber-attacks, and develop responsive mechanisms. In parallel, the multiplication of databases and new technologies allowing remote control of individuals raise new challenges to the protection of Europeans' fundamental rights to personal data and privacy*. (European Commission, 2010, p. 5)

In response, a number of measures are proposed, building on the activity of the European Commission under its Safer Internet Programme (European Commission, 1999), and which specifically promote greater safety online as a trust-reinforcing mechanism. This includes provision for:

- Multi-stakeholder engagement: "Addressing those threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies, both at home and globally" (p. 16).
- Educational activities and awareness raising campaigns for the wider public are also recommended the EU and Member States can step up their efforts, e.g. through the Safer Internet Programme, providing information and education to children and families on online safety, as well as analysing the impact on children of using digital technologies (p. 16).
- Industries are also be encouraged to further develop and implement self-regulatory schemes, in particular as regards protection of minors using their services (p. 17).

Added emphasis was given to the theme of a more trusted Internet for children, when Neelie Kroes, Vice-President of the European Commission, called on Internet companies at the Digital Agenda Assembly of 2011 to deliver 'safety by design' features, such as privacy by default for younger users of social networking services and better systems for age rating of content and for parental controls (Kroes, 2011).

Against this background, four main policy initiatives have emerged which have served to focus attention on specific actions that could be achieved to make the Internet, using the terminology of the moment, not just a *safer* but a *better* place for children. Firstly, in December 2011, a *CEO Coalition* of the main Internet companies in Europe was announced as a cooperative voluntary effort, under the leadership of the European Commission. A number of strategic areas of intervention are identified to 'make the Internet a better place for kids', namely: simple and robust tools for users to report harmful content and contact; age-appropriate privacy settings; wider use of content classification; wider availability and use of parental controls; and the effective take down of child abuse material (CEO Coalition, 2012).

Secondly, in a parallel initiative led by industry, 25 companies early in 2012 announced the formation of an *ICT Coalition for a Safer Internet for Children and Young People* and publication of a set of principles to guide the development of products and services that actively enhance the safety of children and young people online. Here, industry self-regulation is promoted as an effective measure to 'give parents, carers and teachers' greater confidence that Signatories follow best practice in online child protection' (ICT Coalition, 2012). The Principles commit participating companies to minimum standards of responsibility in similar areas to those considered by the CEO Coalition, including content, parental controls, dealing with abuse/misuse, child sexual abuse and illegal content, privacy, education and awareness.

Thirdly, proposals were introduced in January 2012 by the European Commission to reform its 1995 *Data Protection Directive*. The reforms are intended to standardize data protection provisions across the 27 member states and to harmonise the framework for data protection within a single digital market (European Commission, 2012c). In addition to simplifying requirements for businesses and saving them money, a key objective of the reforms is to engender greater trust through giving individuals greater control over their data in the online world and affording them greater consumer protection. Thus, a requirement for parental consent for collection of data from minors under the age of 13 is formalized and brought into in line with the US position under the Children's Online Privacy Protection Act (COPPA). The proposals also strengthen citizens' ownership and control over their own personal data. The Regulation contains provisions for a minimization of data to be collected in the course of online interactions, for controls on Internet services to be automatically set to the most private level ('privacy by default') and that users would also have a 'right to be forgotten' or the right to request that personal data be deleted and taken down on application. Furthermore, 'privacy by design', whereby high standards of privacy protection are built into new products and which enable users to more easily move their data between services, are similarly intended to place the user in control.

Finally, drawing many of these elements together, the European Commission in May 2012 launched its new strategy for 'a better Internet for children' (European Commission, 2012a). Arguing for ongoing collaboration between industry, government and diverse stakeholders, the Commission offered by way of explanation:

> *Ongoing effective industry self-regulation for the protection and empowerment of young people, with the appropriate benchmarks and independent monitoring systems in place, is needed to build trust in a sustainable and accountable governance model that could bring more flexible, timely and market-appropriate solutions than any regulatory initiatives*. (European Commission, 2012a, p. 15)

The strategy sets out a plan to create more online resources and positive content for children, which combined with greater emphasis on digital skills for young people, and better tools to ensure safety, is viewed as the best way to create a more trustworthy Internet environment.

Actions under the strategy are organized under four main goals:

- To stimulate the production of creative and educational online content for children and develop platforms which give access to age-appropriate content
- To scale up awareness raising and teaching of online safety in all EU schools in order to develop children's digital and media literacy and self-responsibility online
- Creating a safe environment for children where parents and children are given the tools necessary for ensuring their protection online – such as easy-to-use mechanisms to report harmful content and conduct online, transparent

default age-appropriate privacy settings and user-friendly parental controls;
- Combating child sexual abuse material online by promoting research into, and use of, innovative technical solutions by police investigations.

Together, the above initiatives – the CEO Coalition and the ICT Coalition, the reform of the 1995 Data Protection and the EC strategy for a better Internet for children – combine to consolidate a decade of European Union policy that has favoured cooperation between lawmakers, industry, civil society as well as parents and children. Yet, such policy pronouncements come at a crucial period in international debates about Internet regulation and fall somewhere in the middle of contrasting positions between those advocating the necessity of defending Internet freedom from any governmental control and those proposing or introducing much more direct regulatory intervention.[1] Whether such measures can ultimately be successful needs to be assessed in the context of the kinds of risks and challenges to trust addressed. This is examined in further detail in the next section dealing with the proposals of the CEO Coalition to make the Internet a better place for kids.

4. Making the Internet a better place for kids

4.1. *Risks and online safety*

In each of the instances above, policy has attempted to tackle areas in which there is persistent trust concern, such as harmful and illegal content, unwanted contact, concerns over personal data and privacy, or the ability of parents to moderate what their children do online. The CEO Coalition, whose proposals are the main topic of analysis here, promises to deliver proportionate and pragmatic solutions to such seemingly intractable problems, and in so doing enhance the trustworthiness of the Internet as a safe place for children. But what is known about such risks and how severely is trust undermined by concerns over children's safety and security? Drawing on data from EU Kids Online, one of the principal sources of information about online risks for European children, the following highlights the principle features of such concern.[2]

It might appear at the outset that whatever about parental concerns, children have few reservations about using the Internet. 75% of children across Europe are online (European Commission, 2012b) and spend close to one and a half hours per day online, (Livingstone et al., 2011a). Children are also going online at ever-younger ages and age 7 is the reported age of first use for many Northern European countries. Just under half of children across Europe enjoy private access to the Internet by going online in their own bedroom. A third goes online via a mobile phone with smart phones and other mobile devices becoming increasingly popular. It would appear that despite parental worries and evidence of risks, children are enthusiastically embracing online opportunities, and that trust has not prevented them going online in very large numbers.

At the same time, when asked if they felt there were lots of good things on the Internet for children their age, less than half of 9–16 year olds in Europe (44%) said it was 'very true'. Over half of Internet-using children also said there were things online that would bother children their age. This is a perception that does not diminish with age and nearly 60% of 15–16 year olds say that the Internet is not a totally safe environment (Livingstone et al., 2011a).

From an adult perspective, Eurobarometer found in 2008 found that 65% of parents in the 27 EU member states were worried that their child might see sexually or violently explicit images on the Internet; 60% of parents expressed concern that their child could become a victim of online grooming and over half were worried that their child could be bullied online (Eurobarometer, 2008). EU Kids Online found that among all the concerns parents may have about their children, online risks feature in the top five concerns. One third of parents say they worry a lot about children being contacted by strangers or their children seeing inappropriate content (Livingstone et al., 2012).

If the Internet is perceived by parents and children to be unsafe or problematic, do young people have the skills to be able to negotiate this and to manage their safety? EU Kids Online found that of 8 basic skills asked about, on average just 4 were claimed by each child. Boys claim slightly more than girls. Younger children have markedly fewer skills: just a third, for example, knows how to change privacy settings on a social networking profile, block unwanted messages, and fewer again say they know how to change filter preferences. In another question, children were asked if they felt they knew more about the Internet than their parents. Here, somewhat surprisingly, many appear to lack confidence in their own abilities and just 36% overall say they know more about the Internet than their parents. Teenagers are somewhat more confident (56%) and younger children the least (12%).

The fact that the incidence of risk may not always match parental concerns does not take away from the fact that such worries are genuine expressions of unease about risks online and an indication of the level of distrust that exists that many parents and children feel. This, therefore, is the background against which the CEO Coalition has proposed action to provide reporting tools, more effective privacy settings, transparent content classification and parental controls as means to reduce risk and harmful consequences for children. An important consideration is the ability of such measures to achieve positive outcomes without limiting or constraining children's opportunities online.

[1] See, for example, OSCE, 2011. Why Internet Freedom Matters. http://www.osce.org/fom/86003.

[2] EU Kids Online is a thematic network funded under the EC Safer Internet Programme in three successive phases of work from 2006 to 14 to enhance knowledge of children's and parents' experiences and practices regarding risky and safer use of the Internet and new online technologies. In 2010, EU Kids Online conducted a face-to-face, in home survey of 25,000 9–16 year old Internet users and their parents in 25 countries using a stratified random sample and self-completion methods for sensitive questions. Full findings of the survey are published in LIVINGSTONE, S., HADDON, L., GÖRZIG, A. & ÓLAFSSON, K. 2011a. Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.

4.2. *Reporting mechanisms*

The development of simple and robust reporting tools is the first area of action proposed by the CEO Coalition. Reporting mechanisms, such as single-click buttons or icons for reporting or flagging potentially harmful content or contacts, have been an important element of online safety though the availability, effectiveness and take up of such mechanisms has been inconsistent. To be effective, reporting mechanisms need to be accessible and easy to use, as well as transparent and accountable in their operation. The Coalition proposes context-sensitive mechanisms to be available across all services and devices, covering clear and commonly understood reporting categories (CEO Coalition, 2012).

Policymakers have long advised children to tell someone if they've been upset online. Overwhelmingly, children tell a friend, followed by a parent, when something online has bothered them. Less frequently, they tell a teacher or any other adult in a position of responsibility, appearing to show less trust in those who may have more expert solutions (industry sources, helplines etc.). Most children do attempt some form of proactive strategy when they encounter problems online, rather than remain passive or fatalistic. This suggests a desire to cope as best they can and a readiness to adopt new technical tools if these are available. Specifically, in relation to use of reporting mechanisms, EU Kids Online found that:

- *14% had seen sexual images on websites* of whom one third were bothered. Just 15% of those upset reported the problem (e.g. clicked on a 'report abuse' button, contact an Internet advisor or 'Internet service provider (ISP)' and of these 13% said this had helped.
- *15% have seen or received sexual messages online* (children 11–16). Over a quarter were bothered by this and of these, 19% reported the problem but just 11% said this had helped. Four in ten blocked the person who sent (40%) and/or deleted the unwanted sexual messages (38%) and in most cases said that this action helped the situation.
- *6% of young people (9–16) have been sent nasty or hurtful messages on the Internet* of whom 81% have been fairly upset by the experience. Just 9% of these used a report abuse mechanism and 5% said this had helped.

Therefore, the proportion of young people using report mechanisms is small, ranging from 9% who report cyber bullying to 19% who report 'receiving sexual messages'. This suggests that such technical features require greater promotion on the part of service providers as well as better training in digital skills. As a solution that helps children when they encounter a problem online that bothers them, reporting would appear to work best for seeing sexual images (13% said it helped) and somewhat less so for other risks encountered, suggesting that better solutions are needed for peer-to-peer risks. There may be many reasons why the solutions children try, when upset, do not help the situation, but one possibility is that the technical tools are flawed or difficult to use, and another is that adults – professional or personal – are unprepared or unable to help children. Mostly, children said the approach they chose helped in up to two thirds of cases. In more than 50% of the cases where a provider was contacted this was perceived as effective/helpful. The challenge, therefore, is to ensure reporting tools are better known, more visible, better trusted and more widely used when children come up against situations that they cannot fix themselves.

4.3. *Privacy settings*

The area of online privacy is one that attracts considerable public and policy attention, particularly with regard to the risks that young people face by either disclosing too much personal information or inadequate control over their data once posted online. The question addressed by industry in its statement of purpose is whether adequate, age-appropriate privacy settings are available to keep children safe online. Areas of risk mostly centre on young people's use of social networking sites (SNS). EU Kids Online found that overall 59% of 9–16 year old Internet users have a social networking profile, including three in four of 13–16 year olds. More controversially, one in three of 9–12 year olds use social networking sites, frequently in contravention of their terms of service (Livingstone et al., 2011b).[3]

A key issue from the point of view of engendering trust is whether children are able to protect their privacy, understand the embedded safety tools provided and have the digital skills to manage settings and their personal information. EU Kids Online found that overall 43% of SNS users keep their profile private so only their friends can see it; 28% have partially private profiles so friends of friends can see them; and 26% say that their profile is public so that anyone can see it. Age, digital skill and the ease with which settings can be managed make a difference in the use of privacy settings. In most countries (15 of 25), younger children are *more* likely than older children to have their profiles public. Just over half of the 11–12 year olds but over three quarters of the 15–16 year olds say they know how to change the privacy settings on their profile. Almost half of the younger Facebook users, compared to a quarter of the older Facebook users say they are not able to change their privacy settings. And with regard to personal information, children are rather *more*, not less, likely to post personal information when their profiles are public rather than private or partially private. One fifth of children whose profile is public displays their address and/or phone number, twice as many as for those with private profiles.

Many users rely on the default privacy settings provided by social networking services yet these, as successive independent evaluations have revealed, are not in fact 'private' by default and require considerable adjustment to restrict access to information (Donoso, 2011). At the same time, children and young people use SNS services to share information and make new friends, thereby sometimes engaging in riskier practices in order to build popularity and larger numbers of contacts

[3] According to EU Kids Online 38% of 9–12 year olds have a social networking profile. The minimum age of 13 for most social networking services is based on US legislation. Online collection of personal information for persons under the age of 13 must comply with COPPA – Children's Online Privacy Protection Act with strict rules regarding age verification and consent. For this reason, many Internet services set their age limit at 13 and over. The age limit in some countries is higher, e.g. 14 in Spain and South Korea.

online. However, the fact that one third of SNS users do not know how to change their privacy settings suggests there is considerable scope for developing easier to use privacy controls. Therefore, taking into account age appropriateness and different levels of digital competence, default privacy settings should be more accessible for all, more restrictive according to the age of the user and more context sensitive to situations where children may be more vulnerable. The increasing problem of under-age users – made all the more difficult to identify as these are users that have registered with a false age – places an added need to protect younger SNS users as well as the need to examine the effectiveness of existing age limits and the use of better age verification techniques.

4.4. *Content classification*

Schemes of content classification have been advocated since the early days of the Safer Internet programme and inherit many of the features developed for audiovisual services in traditional media content regulation (Machill et al., 2002; D'Udekem-Gevers and Poullet, 2001). In this area, the CEO Coalition indicates that it would seek to build on existing initiatives such as the PEGI[4] and other age-rating systems developed in the gaming and other audiovisual sectors, while examining the applicability of age rating and content classification to such areas as user-generated content and app-stores (CEO Coalition, 2012).

Content classification covers a wide range of rating systems, including producer and user-based systems, designed to provide widely accepted classification categories to aid decision-making in relation to age appropriateness. Content risks – to be distinguished from *contact* and *conduct* risks – also take a variety of forms and can be considered under the following general headings (Livingstone and Haddon, 2009):

- *aggression:* including dangers of aggressive, violent, racist content and hate speech;
- *sexuality*: with the potential of encountering problematic online sexual content;
- *values or ideology*: with accompanying dangers of biased information, racism, blasphemy, health "advice"; and
- *commercial interests:* and engaging with potentially harmful commercial content.

Each of these has been discussed, to a greater or lesser degree, in policy circles, and some have been the focus of considerable multi-stakeholder initiatives. However, the nature of the harm at stake is not always clear. For instance, although society tends to be anxious about children's exposure to pornography or racism or the circulation of sexual messages, the nature of the harm that may result and which, presumably, motivates the anxiety, nonetheless often goes ill defined. The challenge remains, therefore, for any classification scheme to be broadly acceptable, it needs to provide clarity about the applicability of risks to different age groups and the likelihood and nature of the harm that might result. Classification of content (including website content, functionality, applications, pictures, videos, etc.) could be based on existing models of content classification such as PEGI or the current online ratings for youth currently in place in Germany.[5]

The classification of content may be either based on labelling or descriptions depending on what may be most appropriate/effective based on the actual content to rate and the nature of platforms being age-classified. However, user-generated content (UGC) presents further challenges. Among the content risks found by EU Kids Online to be most prevalent is exposure to various types of potentially harmful user-generated content (including hate speech, pro-anorexia, self- harm, drug-taking or suicide) – experienced by 21% of 11–16 year old Internet users in Europe (Livingstone et al., 2011a). Companies claim they are unable to monitor all the content that is uploaded to their websites/platforms, whether by users or other third-party app developers, and therefore cannot rate or guarantee that content is "safe" for the intended audience. Dealing effectively with new user trends and new technologies promoting shared, peer-generated content, therefore, needs to explore technical solutions such as automated, machine-readable content classification systems as well as community-based, user rating systems that currently operate in popular video sharing sites such as YouTube. Such an appeal to users' responsibility for classification and self-rating of content likewise requires levels of digital literacy – and digital citizenship – that may be effective in the more mature markets but will prove difficult to operate in newer use environments where often the needs are greatest.

4.5. *Parental controls*

Parental controls have long been advocated as a technical solution to the challenge of parental mediation and monitoring of young people's Internet use. These are typically software tools that allow parents or carers to block or filter some types of websites, to keep track of websites accessed by young people or to set limits on the amount of time spent on the Internet. Research has found, however, that the take up of parental controls or filtering technologies is low and despite the considerable policy attention such technologies have received, they are only used in less than one third of cases

[4] PEGI is the Pan European Game Information age-rating system developed in 2003 with the support of the European Commission and replaced a variety of national rating systems under one common European system. The system is supported by the major console manufacturers, including Sony, Microsoft and Nintendo, as well as by publishers and developers of interactive games throughout Europe. The age-rating system was developed by the Interactive Software Federation of Europe (ISFE). See: http://www.pegi.info/.

[5] In Germany, a more complex system of games content regulation exists under a youth protection system youth protection system incorporating the Youth Protection Act (YPA) and the State Treaty on Youth Protection in the Media (STYPM). Through a system of classification and labelling, content providers can opt for rating their own content or submit online content for classification by an established organization. Mandatory age rating only applies to physical media such as games distributed on disk; online age rating is a recommended voluntary system.

(Duerager and Livingstone, 2012). There is considerable variation across Europe in the use of filtering technology, ranging from 46% in the UK to just 5% in Romania. In general, filtering is less used in Eastern European countries and most used in English-speaking countries. The use of parental controls is more common with younger children and 39% of parents of 9–12 year old children use filtering software.

Interestingly, the use of parental controls is one that impinges upon the issue of trust in a number of ways. Parental controls have been advocated for parents who lack the confidence or knowledge about the Internet, working on the basis of filtering out websites parents do not wish their children to see. This, while building confidence for less experienced users, can create a "false" sense of security for parents, teachers, or carers who may think that by applying certain types of software, their children will be safe online. It may also be seen as a lack of trust in children as Internet users, conflicting with democratic or more permissive styles of parenting, and in contravention of their rights to access information. For this reason, their use and configuration remains controversial and a somewhat disputed area of digital safety (Eastin et al., 2006; Kirwil, 2009). For its part, the CEO Coalition has committed to developing more usable controls, allowing parents greater choice in how they should be configured and implemented (CEO Coalition, 2012). Among the challenges facing developers of parental controls include keeping pace technological change so they are available across all services and devices. In addition, while filtering proves reasonably effective in restricting access to certain types of website content, it struggles to deal with user-generated content, thereby undermining its perceived value in creating a safer Internet browsing environment.

5. Conclusion

The rise of concern with trust in modern societies has been associated to a great extent with the perceived increase in the amount of risk that impinges on everyday life (Beck and Ritter, 1992). The trust-reinforcement measures proposed under initiatives such as the CEO Coalition of Internet companies and the EC strategy for a better Internet for children tackle some of the most persistent areas of risk identified in the online world. Since its inception, governments and industry stakeholders have attempted to mitigate the most pernicious aspects of harmful content, abuse, misuse and fraud on the World Wide Web. Given its borderless and constantly evolving nature as well as the widely held commitment to ensuring the Internet is not constrained by excessive regulation, responsibility for managing risks encountered online has been devolved to the citizen and user level (Lievens, 2007). Accordingly, the undermining of trust – and how to counteract it – has justifiably received much attention in policy debates.

Concerns about children's welfare on the Internet are among the top worries expressed by parents and do contribute to a wider perception that it is not a totally safe or positive environment for young people. That has not prevented children enthusiastically embracing the online world and rapidly incorporating it into their everyday social interactions and leisure opportunities. In the case of the measures proposed to reinforce trust, most attention is focused on strengthening user-controlled security features: labelling systems to guide the filtering out of unwanted content; parental controls to monitor minors' use; alert mechanisms to report when something goes wrong; strengthened instruments to remove illegal content. These initiatives build on longstanding pillars of safer Internet policy that focus on empowering parents and to a lesser extent children to manage risks they encounter in the course of their online activities. In this sense, trust equates to the minimizing of risk and the belief that those risks are best dealt with by technical solutions.

While enabling parents to identify and manage Internet risks is always a good thing, an aspect that remains relatively untouched by this approach is that of children's and young people's own trust in the online environment. Safer Internet policy has increasingly emphasized the need for greater digital literacy and citizenship skills that empower young people to self-regulate and to more effectively manage their own digital lives (European Commission, 2009). Crucially, this is an approach that recognizes children and young people as rights holders and places the question of trust on a different footing, that of the mutual recognition of rights, not just between children themselves but between adults, parents and children and which would seek the realization of rights as a legitimate policy goal. This is an area where clearly more work needs to be done but for which there exists a strong tradition of rights-based policy and regulation (Council of Europe, 2006) that supports user empowerment by Internet technologies and services as positive tools to be embraced rather than feared.

Acknowledgements

Research for this paper was supported by the Digital Childhoods project funded under the Irish Research Council for Humanities and Social Sciences Senior Fellowship Scheme.

Brian O'Neill (*brian.oneill@dit.ie*), *Dublin Institute of Technology, College of Arts and Tourism, Dublin, Ireland.*

REFERENCES

Beck U, Ritter M. Risk society: towards a new modernity. London: Sage; 1992.

CEO Coalition. Coalition to make the internet a better place for kids. Statement of purpose. Brussels: European Commission; 2012.

Cheshire C, Antin J, Cook KS, Churchill E. General and familiar trust in websites. Knowledge, Technology and Policy 2010;23: 311–31.

Cohen-Almagor R. Responsibility of and trust in ISPs. Knowledge, Technology and Policy 2010;23:381–96.

Cook KS. Trust in society. London: Russell Sage Foundation Publications; 2003.

Council of Europe. In: Council of Europe, editor. Recommendation Rec(2006)12 of the Committee of Ministers to member states

on empowering children in the new information and communications environment; 2006. Strasbourg.
D'udekem-Gevers M, Poullet Y. Internet content regulation: concerns from a European user empowerment perspective about internet content regulation: an analysis of some recent statements. Computer Law and Security Review 2001;17: 371–8.
De Paoli S, Kerr A. Conceptualising trust: a literature review (NIRSA) working paper series no. 40. NIRSA – National Institute for Regional and Spatial Analysis; 2008.
Donoso V. Assessment of the implementation of the safer social networking principles for the EU on 14 websites: summary report. Luxembourg: European Commission, Safer Internet Programme; 2011.
Duerager A, Livingstone S. How can parents support children's internet safety? London, LSE: EU Kids Online; 2012.
Dutton WH, Shepherd A. Trust in the internet: the social dynamics of an experience technology. Oxford: Oxford Internet Institute; 2003.
Eastin MS, Greenberg BS, Hofschire L. Parenting the internet. Journal of Communication 2006;56:486–504.
Erikson E. Childhood and society. New York: Norton; 1950.
Eurobarometer. Towards a safer use of the internet for children in the EU: a parents' perspective. Luxembourg: European Commission Safer Internet Programme; 2008.
European Commission. A multiannual community action plan on promoting safer use of the internet by combating illegal and harmful content on global networks. 4-Year work programme 1999–2002. Luxembourg: European Commission Safer Internet Programme; 1999.
European Commission. Commission recommendation on media literacy in the digital environment for a more competitive audiovisual and content industry and an inclusive knowledge society. Brussels: European Commission; 2009.
European Commission. A digital agenda for Europe. Brussels: European Commission; 2010.
European Commission. Communication on the European strategy for a better internet for children. Brussels: European Commission; 2012a.
European Commission. Digital agenda: new strategy for safer internet and better internet content for children and teenagers. Press release. Brussels: European Commission; 2012b.
European Commission. Safeguarding privacy in a connected world. A European data protection framework for the 21st century. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN: EN:PDF; 2012c.
Flint D. The internet and children's rights: suffer the little children. Computer Law and Security Review 2000;16:88–94.
Friedman B, Peter H, Khan J, Howe DC. Trust online. Communications of the ACM 2000;43:34–40.
Hardin R. Trust. Cambridge Polity Press; 2006.
ICT Coalition. Principles for the safer use of connected devices and online services by children and young people in the EU. Available, http://www.gsma-documents.com/safer_mobile/ICT_Principles.pdf; 2012.
Kirwil L. Parental mediation of children's Internet use in different European countries. Journal of Children and Media 2009;3: 394–409.
Kroes N. State of the digital union. The digital assembly. Brussels: European Commission; June 16, 2011.
Lievens E. Protecting children in the new media environment: rising to the regulatory challenge? Telematics and Informatics 2007;24:315–30.
Livingstone S, Haddon L, editors. Kids online: opportunities and risks for children. Bristol: Policy Press; 2009.
Livingstone S, Haddon L, Görzig A, Ólafsson K. Risks and safety on the internet: the perspective of European children. Full findings. London: LSE, EU Kids Online; 2011a.
Livingstone S, ÓLafsson K, O'neill B, Donoso V. Towards a better internet for children. London: LSE, EU Kids Online; 2012.
Livingstone S, ÓLafsson K, Staksrud E. Social networking, age and privacy. London: LSE, EU Kids Online; 2011b.
Machill M, Hart T, Kaltenhuser B. Structural development of internet self-regulation: case study of the Internet Content Rating Association (ICRA). Info 2002;4:39–55.
Mansell R, Collins BS. Trust and crime in information societies. London: Edward Elgar; 2005.
Nissenbaum H. Securing trust online: wisdom or oxymoron. Boston University Law Review 2001;81:107–31.
O'Hara K, Shadbolt N. Knowledge technologies and the semantic web. In: Mansell R, Collins BS, editors. Trust and crime in information societies. London: Edward Elgar; 2005.
OSCE. Why internet freedom matters. Available, http://www.osce.org/fom/86003; 2011.
Powell A, Hills M, Nash V. Child protection and freedom of expression online; 2010. Oxford Internet Institute forum discussion paper no. 17.
Rosenthal DA, Gurney RM, Moore SM. From trust on intimacy: a new inventory for examining Erikson's stages of psychosocial development. Journal of Youth and Adolescence 1981;10:525–37.
UNICEF. Child safety online – global challenges and strategies. Florence: UNICEF [Innocenti Research Centre]; 2011.
United Nations. Convention on the rights of the child [Online]. Available: http://www2.ohchr.org/english/law/crc.htm; 1989.
Zittrain J. The future of the internet and how to stop it. London: Penguin; 2008.