Joseph Savirimuthu

Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?

extracted from:
Ingi Iusmen
Helen Stalford (eds.)
The EU as a Children's Rights Actor
Law, Policy and Structural Dimensions

Barbara Budrich Publishers
Opladen • Berlin • Toronto 2016

This chapter is available as a free download from https://shop.budrich-academic.de (http://dx.doi.org/10.3224/978384740193c). A paperback of the whole book is available at a charge.
The page numbers of the open access edition correspond with the paperback edition.

ISBN 978-3-8474-0193-3
DOI 10.3224/978384740193c

Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Ein Titeldatensatz für die Publikation ist bei der Deutschen Bibliothek erhältlich.

Verlag Barbara Budrich Barbara Budrich Publishers
Stauffenbergstr. 7. D-51379 Leverkusen Opladen, Germany
86 Delma Drive. Toronto, ON M8W 4P6 Canada
www.barbara-budrich.net

Jacket illustration by Bettina Lehfeldt, Kleinmachnow, Germany – www.lehfeldtgraphic.de
Picture credits: Central Audiovisual Library of the European Commission/ © European Union, 2015
Editing: Alison Romer, Lancaster, UK
Typesetting: Anja Borkam, Jena, Germany

Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?

Joseph Savirimuthu

Introduction

There is a powerful meme – empowering children. This meme is being given a new lease of life as children are regarded as central to the pursuit of EU economic, social and cultural goals. The idea of empowering children is likely to be welcomed by many, not least by those who have long battled to encourage policymakers to take into account children's needs and interests in the networked environment (Savirimuthu 2012: 31-38; Commission 2011b). Arguments in the 1990s and those which continued into the turn of this century about using regulations to create a safe environment for children remind us that many significant concessions made in accommodating children's needs and interests were not easily obtained. Policymakers and stakeholders turned to empirical studies and ground-breaking initiatives under the Safer Internet Programme, and together crafted a delicate balance between online child safety concerns and children's engagement and participation in the networked environment (Commission 2011a, 2011b). In just over two decades, significant progress has been made in creating a safe networked environment for children. That is not all. Children have emerged as major consumers of social media and new technologies (OfCom 2014: 39-42). Empowerment of children, during this period, has increasingly become entwined with the pursuit of economic objectives and the single market.

It is easy to be dazzled by the rhetorical and ideological appeal of empowering children and overlook the negative outcomes. Concerns have, for example, been expressed that a combination of an inability to constrain business interests and a failure to provide adequate safeguards for children in the realm of food advertising and marketing, are undermining children's health and well-being (Bailey 2011: 63-69). The uneasy intuition one feels about policymakers pushing through the *raison d'être* for empowerment, which at times shows scant appreciation of adverse social costs, is resurfacing in another sphere of public policy – empowering children to manage their personal data as a basis for promoting innovation and economic opportunities in the digital economy. Empowerment is now regarded as the flagship of the Com-

mission's European Strategy for a Better Internet for Children (Commission 2012a) (the EU Strategy). Many have remarked favourably on this EU Strategy, in view of previous Commissions' efforts in the realm of online child safety (O'Neill, Staksurd and McLaughlin 2013). Formulated in 2012, the EU Strategy now paves the way for a more ambitious agenda against the background of a new policy and constitutional landscape in post-Lisbon Europe (Commission 2010; Commission 2011). It is worth noting that the EU was already at the forefront of promoting children's rights before the coming into force of the Lisbon Treaty (Savirimuthu 2012). The major difference then was that discourse about children's rights was framed in terms of obligations to respect *human* rights more generally.

Protection of *children's* rights is now explicitly recognised as an objective of the EU (Article 3 TEU). The integration of the European Union Charter of Fundamental Rights (OJ C 83, 30.3.2010, p. 389-403, hereafter the Charter) into the EU regulatory framework ensures that fundamental rights have "the same legal value as the Treaties" (Art 6 TEU). It contains a number of provisions that are relevant to children's virtual lives. Article 8 of the Charter, for example, makes explicit the protection of personal data as a fundamental right of all individuals. Data protection rules and norms must now empower children. Children will now be able to exercise their rights to information self-determination as individuals and citizens in the digital economy. This has to be read in conjunction with Article 24 of the Charter which states that in all actions relating to children, the child's best interests must be a primary consideration. The dilemma facing policymakers in translating Article 24 of the Charter into meaningful policy adjustments must now be considered alongside other developments. At present, under current data protection rules, children are not regarded as a group of individuals meriting specific "protection and care as is necessary for their well-being" (Article 24 Charter). Rather, children fall within the age-generic provisions of EU secondary legislation which, protect the personal data of all "natural persons" (Directive 95/46/EC, Official Journal L 281, 23/11/1995, Arts 1 and 2(a), hereafter the 1995 Directive) and Directive 2002/58/EC Official Journal L 201, 31/07/2002 (hereafter, the e-Privacy Directive).

The proposals to reform current data protection rules explicitly identify children as legitimate rights bearers with specific needs and interests (Commission 2012b). While such proposals are to be welcomed, when viewed as whole they raise some intriguing practical and conceptual challenges for data protection regulations (Fuster and Gutwirth 2013: 531-539). Of particular interest in this chapter are the premise and consequences of aligning children's right to information self-management with innovation under the EU's model of empowerment. For practical reasons, the chapter does not rehearse the tensions between the concept of children's rights and paternalism on the one hand and autonomy and protection on the other (Savirimuthu 2012: 10-

12 and 193-197, Fortin, 2009: 19-29). The discussion will concentrate instead on the outcomes of empowering children within the context of data protection law. It undertakes a critical assessment of pillar 2 of the EU strategy and will show that the current use of the 1995 Directive and e-Privacy Directive to reinforce these fundamental rights in a manner that is consistent with children's best interests should not underestimate the impact of particular features of networked environments on children's autonomy, agency and expression.

The analysis presented below proceeds on the following presumption: if children's needs and expectations are to be better addressed in a principled and credible manner, policymakers must take into account the specific features of networked environments that expose regulatory and structural imbalances that contribute to individuals' ability to assert control over their personal information. This chapter suggests that the assumptions we make about empowerment and its value in enhancing children's rights to information self-determination cannot be easily reconciled with the fact that networked environments modulate visibility, exposure and information sharing practices (Cohen 2013: 1916; Boyd and Marwick 2014: 1062). Nowhere is this mismatch between the EU Strategy's vision of empowering children and the reality of networked environments more clearly evidenced than by the construction of business models, which view personal information as a commodity to be exploited for no purpose other than to gain competitive advantage in the networked economy. A case in point is the practice of aggregating personal information for generating profiles of children and serving them with advertisements based on their browsing habits and online interactions. The protective potential of both the 1995 Directive and the e-Privacy Directive is being outpaced by the speed and scale of the transformative nature of social media and new technologies on society and the emergence of the personal data ecosystem. The extension of the empowerment meme as a policy objective in data protection law is problematic since it is far from clear how innovation potential and economic dynamics are to be reconciled with children's fundamental rights to privacy and protection of their personal data, without effective protection mechanisms being installed at the outset. This prompts questions as to whether the adjustments made in the proposed reforms would be sufficient to advance children's best interests as envisaged in the Charter.[1]

The specific aim of this chapter is to articulate why there is a need to begin a serious dialogue on how children's best interests can be better integrated into EU data protection legislation in a manner that is compatible with children's reasonable expectations and their rights under the Charter, while being alive to the political, economic, and social drivers of the broader policy agen-

1 Compare Commission 2012b in particular recitals 29, 38, 46 and European Parliament and of the Council amendments / COM/2012/011 final - 2012/0011 (COD), recitals 29, 38, Article 8 and Article 32(a).

da in the EU. Section 1 begins with some preliminary observations on the vision proposed by the EU Strategy, noting the political faith in self-regulation coupled with the restricted objective of encouraging children to exercise greater responsibility over their personal data to minimise risks of peer victimisation and online sexual solicitation. Section 2 considers the implications of new technologies and the design of communication spaces for children's autonomy over their personal data and privacy. Section 3 examines whether policymakers' confidence in the ability of EU data protection legislation to adequately protect children's personal data is both principled and credible. It will be suggested that the structural and substantive logic of existing and proposed law continue to be instructed by businesses' desire to extract maximum value from personal information. Section 4 confronts the data protection challenges from a fresh, rights-based perspective; it asks, 'what if' businesses meet the standards of the Convention on the Rights of the Child (CRC). The discussion will leave the conclusions open-ended but will suggest that requiring businesses to act in accordance with CRC values may prove to be a subtle strategy towards creating a mindset that could ultimately achieve two immediate outcomes. First, it may help resolve the protection/empowerment balance inherent in children's rights and explicit in the Charter, in particular Articles 24, 7 and 8. Second, knowing that businesses voluntarily integrate CRC standards may be a far more effective and sustainable strategy than threats of legislative intervention, monetary penalties and investigations. The chapter concludes that steering data protection rules towards embracing fundamental CRC values through design solutions and codes of practice may help demonstrate and realise a principled and sustainable approach towards furthering children's best interests.

1. The EU Strategy and Information Self-Determination

It is of course right that there should be an EU Strategy for the Internet that seeks to ensure that children in the networked environment do not find their trust and confidence impaired by threats to their safety. Why should children be exposed to risks to their health and well-being by the mere fact of using the Internet or other communication devices such as smartphones and computers? The EU Strategy has 4 main pillars; these aim to:

i. stimulate the provision of high quality creative and educational online content for children and young people;
ii. raise levels of awareness of the opportunities and risks associated with use of the internet and equip young people with the skills needed to use the internet safely and responsibly;

iii. create a safe online environment for children; and
iv. combat the distribution of child sexual abuse material via the internet and use of the internet for the purposes of child sexual exploitation (Commission 2012a: 7-16).

A host of familiar approaches and measures previously adopted are regarded as being relevant to reaching the objectives set out in the 4 pillars (Commission 2012a: as above). These involve calls for greater coordination between industry, Member States and the Commission in implementing child safety policies and initiatives to support parents and children.

1.1 Framing the Problem: The Model of Empowerment

The EU Strategy requires data protection and privacy risks encountered by children to be specifically addressed (Commission 2012a: 5, 11-13). The Commission does not disguise the imperatives driving this multi-faceted conception of children and stresses that empowering children is not simply a rhetorical turn:

> Paying attention to the demands of children opens up a wide range of business opportunities. The global digital content market is predicted to cross 113 billion Euros in 2028. The market worth of mobile apps was 5 billion euros, and is expected to grow up to 27 billion euros by 2015, mainly driven by games and with more than 5 billion mobile subscriptions worldwide. The global video game market is predicted to reach sales of over 62 billion euros. With the wide proliferation of tablets, smart phones and laptops that children use heavily, the potential market for interactive creative and educational online content for both young children and teenagers is substantial. Online and mobile apps and games provide unprecedented opportunities for business development, in particular for SMEs and creators, as they allow for direct contact with potential users/clients. Children themselves could become online creators and start-up businesses. (Commission 2012a: 3)

There are some subtle social and economic engineering undercurrents that should not go unobserved. First, it should be noted that the Commission is clearly aware of the need to calibrate current political, economic and social frameworks with the transformative nature of networked environments and technologies. Unlocking the value of personal data is regarded as a policy that is intended to stimulate innovation and provide new economic opportunities. Second, there is an assumption that these policy objectives cannot be attained unless orthodox approaches to privacy and data protection are made more adaptable and flexible without undermining individuals' fundamental rights (Commission 2012a: 3-8 and 15). It would not have gone unnoticed that against this background, the EU Strategy's conception of children in networked environments have been undergoing a reassessment of late, in terms of their legal status, their expectations as citizens and equally im-

portant, policymakers' expectations of them as consumer citizens in the digital economy. This expansive view of children has been based on the wisdom that aligning children's interests as consumers with those of the market will give rise to considerable economic and cultural opportunities. The EU Agenda for the Rights of the Child (2011), it will be recalled, sets in place a blueprint for advancing children's needs and interests not simply as individuals with constitutional rights but also as legitimate actors in the social and economic sphere (Commission 2011b). Investment in children is increasingly regarded as a policy priority (Piper 2010: 1 and Commission 2011b: 3-4).

Let us for the moment accept uncritically the premise that a new model of empowerment is needed to unlock the value of children's personal data. What safeguards does the Commission envisage as being necessary to protect the rights of children under the EU Strategy? Pillar 2 provides some possible answers to this question. The Commission begins by suggesting that all children should be empowered and those who are vulnerable protected:

> Children have specific needs and vulnerabilities and their difference has to be recognised. The internet and ICT provide children with a wide range of opportunities to play, learn, innovate and be creative, to communicate and express themselves, to collaborate and engage in society, to be more aware of the world around them, and to develop essential skills, and exercise their rights. But children also need to be protected. (Commission 2012a: 3)

Section 2.3.4 of the EU Strategy contains some measures regarded as providing adequate safeguards to possible problems resulting from empowering children. There is, first of all, an acknowledgment that industry, Member States and the Commission will need to work together to ensure that as personal data is collected and used, and that businesses will engage fully with children and equip them with information and tools to help them make meaningful choices and decisions (O'Neill, Staksrud and McLaughlin 2013: 11-18). The EU Strategy also identifies two particular data mining practices that need ongoing oversight. The heading to Section 2.3.4 provides a clue to the mischief intended to be addressed – "Online Profiling and Overspending".[2] We get a sense of the Commission's thinking of the risks posed by profiling and advertising and the steps to be taken in the following extract in the EU Strategy:

2 See the efforts made in the UK: OFT investigates free children's web and app-based games. Press Announcement, United Kingdom Office of Fair Trading, April 12, 2013: http://www.oft.gov.uk/news-and-updates/press/2013/33-13. The OFT's Principles for online and app-based games, United Kingdom Office of Fair Trading, OFT1519: http://www.oft.gov.uk/shared_oft/consumer-enforcement/oft1519.pdf. Annex to the OFT's Principles for online and app-based games, United Kingdom Office of Fair Trading, OFT1519a: http://www.oft.gov.uk/shared_oft/consumer-enforcement/oft1519a.pdf. Online games industry given two months to get house in order following OFT investigation, Press Announcement, United Kingdom Office of Fair Trading, January 30, 2014: http://www.oft.gov.uk/news-and-updates/press/2014/05-14.

Children, especially younger ones, do not have a developed ability to engage critically with advertising messages. In virtual worlds, children can often pay for virtual goods via their mobile phones, by calling or texting, and therefore with no prior parental permission necessary. Children may also seek to access online gambling or gaming sites. They can download ringtones for their mobile phones or accidentally access the internet on their mobiles. All this may incur high charges. The aims are to make sure that standards for advertising on websites for children allow a level of protection comparable to that of advertising in the audiovisual services and that, with regard to behavioural advertising, no such segments are created to target children, and to ensure that spending online or on mobile phones by children does not generate unforeseen high costs. (Commission 2012a: 12-13)

Finally, the Commission proposes a model of empowerment which defines the way children, their parents and industry negotiate the way personal data is to be managed (Commission 2012a: 8 -13). The expectation here is that children, under this model, will eventually have: (i) greater control over their personal data; and that (ii) businesses will be required to obtain their consent before personal data belonging to them is processed in certain instances.[3] These two measures can be described as the 'control' and 'notice and consent' models respectively. 'Control', implies that children will not only be provided with information to help them understand the way their personal data will now be collected but that they will be provided with tools, such as privacy settings, to help them regulate the flows of their personal data. The role of 'consent' is, like 'control', regarded as central to empowering children and is viewed as enabling them to make informed decisions and choices in respect of the way they use their personal data (Commission 2012a: 4 and 15). The ascription of responsibility to children in the way personal information is to be managed has two aspects. The first involves unlocking the innovation potential of personal data and the second, as the Commission observes, to promote development and civic engagement:

Young children need 'online playgrounds' where they can both play and learn; teenagers could benefit from creative and educational games to stimulate their imagination and support their positive use of the internet. (Commission 2012a: 7)

1.2 The Problem with Empowerment

Children's rights, the EU Strategy and the Agenda for the Rights of the Child become linked symbiotically with the Commission's Growth Strategy, Europe 2020. Stalford observes that the elevation of the children's rights agenda in the EU corresponds with the recognition that a failure to invest in children

3 The Commission does not make explicit, instances when children's ability to consent will not require parental oversight and appears to leave open the circumstances where children will be deemed to have full autonomy.

now will have long-term institutional, social and economic ramifications (2013: 9). The economic and social opportunities derived from conceptualising children as autonomous individuals capable of making lifestyle choices are considerable. The issue of commercial marketing to children is an ever-present problem and one which remains a highly contested terrain in public policy. While it is beyond the scope of the study to re-visit this debate fully,[4] it may at first blush seem that the Commission has anticipated concerns regarding likely adverse policy outcomes when it places children's rights to information self-determination at the heart of its strategy towards maximising the opportunities for economic growth and innovation (Commission 2012a: 7-8). Well-informed children, acting as responsible citizens should be allowed to determine how, when and by whom their personal data can be accessed and used. By fostering trust and empowering children, innovation opportunities can be realised and children and society generally will benefit from increased choices and access to a wide range of goods and services.

One does not doubt that personal data management and responsible use of the Internet and social media are relevant to children's developmental and educational opportunities too (Commission 2012c: 6). The recent qualitative study in the EU Kids Online project illustrates how engagement in the networked environment continues to enhance children's developmental processes through access to wide range of media, participation, formation of relations and experimentation (Vincent 2015; EU Kids Online 2014).

To safeguard children, society has long relied on the agency of privacy, data protection laws and responsible adults to help resolve some difficult dilemmas surrounding children's autonomy (Savirimuthu 2012: 10-12; Richards 2015: 64). Those dilemmas, although real, have long been mitigated through a combination of social and legal norms. Schools and homes continue to be regarded as spaces for nurturing, human development and fulfilment of children's potential. Parents and educators recognise the value of children enjoying private spaces for development, and would readily respect children's 'right to be left alone'. The EU Strategy's model of empowerment obscures the interplay between these social dimensions and underestimates some intractable dilemmas networked environments pose for children. Networked environments collapse contexts, redefine social norms and create the illusion of autonomy (Cohen 2012: 101-106). Understanding the social dynamics of networked environments, the scale and effects of monitoring, the range of personal data collected and observations made or inferences drawn, and uses of personal data, are crucial to grasping the problems and solutions

4 The Communication spends time focusing on the measures that need to take to safeguard children from inappropriate advertising and the financial implications for children and their parents. Advertising and commercial practices targeting children are now regulated by the Unfair Commercial Practices Directive 2005/29/EC. A sceptical view of the Directive 2005/29/EC can be found in Garde 2011 pp. 149-171.

that will be needed if the model of empowerment preferred by the Commission is to provide adequate safeguards for children's fundamental rights (Commission 2012c: 2-4).

Three specific concerns emerge from the Commission's framing of problems and the prescriptions offered. First, the premise that information self-management facilitates innovation does not give sufficient importance to the way communication platforms are designed to remove barriers to accessing personal information through a combination of promoting norms of visibility, information sharing and contractual instruments. Networked environments are far from neutral. Communication platforms have *ex ante* features, which favour the interests of business and constrain the choices of individuals and their ability to assert control over their personal information (Cohen 2014). Neither does the Commission give enough emphasis to the real imbalance that exists between individuals and those who collect their personal information. Increased awareness of the value of privacy and skills to manage personal data, will no doubt empower children in the sense that they may be able to make informed decisions about which information they should disclose, to whom and in what contexts. There is considerable body of opinion and studies however that point to features in networked environments, which undermine individuals' ability to retain control over their personal information (Steijn 2014; Hildebrandt 2009). Some degree of effective and principled regulatory oversight is still needed to ensure that these communication spaces do not continue to violate children's reasonable expectations for quiet enjoyment.

Second, the EU Strategy's entire focus on misleading advertising practices, peer victimisation and online sexual victimisation is in itself surprising. No one will disagree that many incidents involving children being victimised by their peers or approached by adults intent on engaging in sexual activity could have been avoided if children did not disclose particular information or engage in conversations that were risky. We need, however, to expand our understanding of 'harms' to also include other scenarios: loss of control over the collection and use of personal data; innocuous items of information that can be aggregated to create profiles which may lead to differential treatment; indiscretions committed by children in their naivety and immaturity that are unlikely to be forgotten and may come back to haunt them in years to come; and real risks of personal data being manipulated or used out of context.

Third, the solutions proposed by the Commission, suggests that answers to some fundamental questions have not been fully thought through. For example, we could ask why it is that children either do not realise the privacy risks associated with their online activities or struggle to manage their personal data in networked environments (Solove 2013: 1883-1889)? Given children's reasonable expectations regarding the use of technology and opportunities for identity experimentation, play and learning, is it right that we divest all re-

sponsibility for the design of communication platforms to industry? How do we promote transparency, accountability and fairness in a way that is meaningful to children (Cohen 2012: 234-239)? How should we conceptualise spatial privacy in networked environments? What is privacy for? While it is not doubted that data collection and processing practices facilitate innovation and make possible new services, content and goods to children, it is equally important that the challenges in retaining control over personal information and the adverse impacts of aggregation are not only acknowledged but also addressed.

The policy prescriptions envisaged in the model of empowerment provides us with a glimpse of how assumptions and reasoning that prioritise economic benefits and consumer interests underestimate the extent to which data protection rules can or are able to respond to the needs and expectations of children. This is a point worth remembering when attempts are made to articulate the interplay between Articles 24, 8 and 7 of the Charter on the one hand and the operation of EU data protection law in networked environments on the other. Information self-determination in the context of online profiling or targeted advertising is not simply a matter of protecting vulnerable or impulsive children from visiting websites to engage in age-inappropriate activities or entering into a spending spree due to deceptive or misleading businesses practices. To those who are accustomed to the operation of data protection rules, it will not have gone unnoticed that the model of empowerment conceals a number of problems that EU data protection legislation has long struggled to resolve: individuals continue to underestimate harms to their reputation resulting from disclosure; privacy and information sharing policies are difficult to read and understand; tracking every digital footprint is time consuming, complex and expensive; and making informed yet highly speculative decisions about future harms is extremely difficult. Of course, the management of privacy, control over personal data and determination of contexts in which information can be disclosed is not a new problem. But what has changed dramatically are the nature and sheer scope of networked environments. The persistence and sophistication of new data mining technologies create conditions that require critical conversations about how children's expectations of privacy can be promoted. The next section draws out particular features of networked environments and information collecting practices that raise serious concerns about the empowerment model, as a prelude to understanding what strategies are available to address children's needs and expectations.

2. Networked Publics: Communication, Visibility and the Autonomy Trap

The Commission in the EU Strategy portrays a far from problematic view of the significance of communication platforms and its design features for children's ability to manage their personal data within the context of profiling and advertising practices. The recent Net Children Go Mobile reports for example, while highlighting the benefits derived from interaction between children's developmental processes and digital activities, expect that greater information awareness will promote control and information self-determination (O'Neill and Dinh 2015; Livingstone et al., 2012; Livingstone and O'Neill 2010). Both conceptions fall into the 'autonomy trap' as the emphasis on notice, consent and control assume that communication spaces are neutral environments, and underestimates the way in which the collapsing of contexts (e.g. Home/School, Work/Play, Public/Private) and processing of personal information redefines autonomy (Schwartz 2000: 821; Kang 1998: 1198). It may be helpful to begin by considering the particular dimensions of networked environments and information collecting practices that justify concerns being expressed about the role and value of empowering children to take full responsibility for their personal data.

2.1 Information Collection in Networked Environments

Four types of business activities in the networked environment have a direct impact on children's ability to manage their personal information: (1) information collection; (2) information processing; (3) information dissemination; and (4) invasion (Solove 2002: 1153-1154). For example, personal information is easily collected when individuals go online, browse websites and access content and interact with friends. Tablets, software applications (apps) and mobile phones now enable information to be collected from multiple venues and devices. Wi-fi is ubiquitous in most places and blurs private and public spaces of activity. Powerful analytic software is used to analyse personal data with a view to determining individuals' preferences, tastes and choices. Knowledge created from personal data can now be used for a wide range of purposes. An online business may use information collected from website visitors to provide services and goods relevant to their needs and preferences. Information relating to personal browsing habits and content accessed can be used to predict and, importantly, shape choices and values. Information generated from an individual's use of the internet or services can also be sold to or shared with advertisers. The economic opportunities created

from unlocking the value of personal data are all legal, subject to some safeguards provided by the law. That said the acts of profiling and targeting of children in particular with customised advertisements has long been an area of concern for privacy advocates.[5] In most cases, user consent to the use of the services or accessing content on websites is deemed to constitute assent to information collection, use and sharing practices.

Knowledge of the scale of data mining activities such as these still leave unexplained why the model of empowerment on which EU data law and policy is based can be seen as giving rise to the 'autonomy trap'. Marwick and Boyd articulate the notion that communication spaces constrain and shape individuals' management of their personal data (2014: 1065). I want to use their interpretation of 'networked publics' to show that children do desire to preserve their privacy and manage their personal information but encounter considerable difficulties asserting their 'right to be left alone' or rights to self-determination of their personal data. The dilemmas children face in managing their privacy and asserting meaningful control of their personal information flows from the design of communication spaces, which produces three consequences: (i) information self-management practices become defined by technological functionality; (ii) networked norms of visibility create audience dynamics that are difficult to resist; and (iii) access to personal data is used to redefine individual autonomy (Marwick and Boyd 2014: 1063).

2.2 Networked Publics

A significant proportion of children have Facebook, Twitter and Instagram accounts. Smartphones and tables have apps that increase the convenience and 'real-time' experience of interaction. Apps enable children to update their social network profiles, receive regular updates of postings by friends and contacts and develop their identities (Livingstone 2008: 393-411). Scholars seeking to resolve the privacy conundrum have drawn insights from the dynamics of digital natives in 'networked publics' (O'Neill and Dinh 2015; Livingstone et al. 2012; Livingstone and O'Neill 2010). 'Networked publics' can be described as communication spaces constructed through networked technologies such as smart phones, tablets, laptops and computers. These communication spaces are distinctive in the sense that they mediate interac-

5 See for example, Schwartz 1999: 1644; Sweeney1997: 100; Zarsky 2003; De Hert and Papakonstantinou 2012. More recently, Article 29 Working Party has issued an opinion and an Advice Paper: Opinion 2/2010 on online behavioural advertising and Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

tions between people and imagined communities. Networked publics, whether these emerge on Twitter, Instagram or Facebook, represent a type of communication space. Each communication space has its own technological affordances or features that allow individuals to share information, build relations and participate in conversations in communities (Schmidt 2014: 3-14). Some illustrations can be provided to emphasise how flows of information are modulated by the design of communication spaces and tools. For example, Twitter provides @ for users to tweet information. Individuals can use text or hashtag (#) to start conversations or participate in discussions. People who follow each other on Twitter can also use the direct message facility ('DM') to have private conversations with each other. Messages are limited to 140 characters and can contain hashtags, photos and links. Facebook, another site favoured by children, also provides technological affordances for individuals to participate in networked publics but does not restrict the size of posts or length of conversations. Like Twitter, the communication space designed by Facebook is accompanied by the expectation that individuals connect with 'Friends'. This expectation of reciprocal social relationships distinguishes Facebook from Twitter. Only 'Friends' can connect and share information with each other on Facebook. When individuals connect with each other on Facebook, technological affordances structure the flow of personal information, which enable the individual to see each other's post on their 'News Feed'. Individuals can also use technological settings on Facebook to define their audiences, determine which posts are accessible and by whom, and use search tools on the site to find new 'Friends'. Technological affordances such as 'tagging', 'Like', and comment boxes allow individuals to interact with each other. Facebook provide users with timeline and notification facilities to enable users to obtain real-time experience with their connections and obtain regular updates. Increasingly, social media can be accessed through devices other than desktops.

Hyper-connectivity is an integral part of shaping audience dynamics and promoting norms of visibility and information sharing practices. Any credible attempt to empower children must account for the way networked environments modulate norms of visibility and information sharing. The design of communication spaces also structure behavioural norms, leaving users with the responsibility of defining the way their information is accessed or viewed (Johnson and Jajodia 1998: 26-34). Affordances such as 'tweet', 'tag', 'Like; or # create tools through which individuals engage in participatory activities, explore spaces for identity and experimentation while maintaining control over their personal data. These affordances also pose children with the dilemma of managing the boundaries of 'publicness' (Marwick and Boyd 2014: 1062). It is true that privacy settings enable users to control who participates in their networks. However, consent to terms on social networking sites enables service providers to access vast amounts of personal information. In

networked publics, since notice and consent are effectively meaningless, children are left with the predicament of making complex and undesirable trade-offs, resorting to social stenography techniques or accepting that the cost of obscurity is exclusion from participation in communities.

In summary, an awareness of the role played by these structural dimensions is critical to understanding why the Commission's model of empowerment may be the wrong solution to a real problem. The structural dimensions of online environments shape and influence the way children define their spaces for intimacy, identity and engagement. By failing to give sufficient weight to the nuances of children's information sharing practices and their desire to participate in networked environments, the Commission appears to have formulated a strategy for the future based on contestable premises and conceptions of information self-determination that do not quite match the complexities of networked environments. The result of this approach is that reliance is ultimately placed on data protection rules to alleviate any regulatory tensions and leaves open the question of how businesses will address children's expectations and needs.[6]

Having raised some questions about the shortcomings of the model of empowerment we can now turn to consider whether even a sympathetic reading of the 1995 Directive and the e-Privacy Directive can help redress the asymmetrical relations that define children and social media companies and if not, whether the proposed data protection reforms may provide the solution to the problems identified in this section. It should not have gone unnoticed that notwithstanding the ambitions mapped by the EU Strategy, if the regulatory strains are to be taken up by data protection rules, it will have to be guided by insights and values other than those provided by the market.

3. The EU Data Protection Directives, the Protection of Children's Personal Data and Networked Environments

We are very much at the initial phase of thinking through the appropriate regulatory responses to the challenges posed by the personal data ecosystem.

6 Commission 2012a at p.13 states "build on self-regulatory standards such as those defined by the European Advertising Standards Alliance for behavioural advertising". This recommendation ignores the safeguards proposed by Article 29 Working Party Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf. Also see EDPS Opinion on the Communication from the Commission – "European Strategy for a Better Internet for Children" (17.07.2012) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/

The business models of social media organizations such as Facebook, Twitter, Tumblr and Instagram are constructed to build databases of personal information with the purpose of creating new value or selling the information available to advertisers. It is not a coincidence that companies such as Google, Facebook, Microsoft, Apple, Twitter, Yahoo and AOL have been actively making acquisitions and aggressively seeking "new ideas, products, and services to market, and managers are seeking ways to appropriate, control, and valorize the creativity of the common" (Zwick, Bonsuand and Darmody, 2008: 174). Innovation and competitive advantage are inextricably linked to leveraging the value of personal data. During the World Economic Forum in 2010, leading IT businesses from the developed economies, privacy advocates and other stakeholders participated in an initiative entitled, 'Rethinking Personal Data' (WEF 2010). The discussions revolved around the challenge of creating a framework that optimised the economic potential of personal data while ensuring that adequate safeguards were put in place. An overriding theme at the event was that data protection laws had to be both adaptable and flexible.[7]

The EU Strategy appears to be like-minded, which is to unlock the value of personal data. Even though personal information is not regarded as property, this has not prevented it from becoming a valuable asset for innovation, marketing and revenue generation (Purtova 2011). This is an important development in the digital economy. Revenue generated from the sale of communication devices and smart phones is being overtaken by those generated from advertising and marketing. The mobile advertising revenue expected from increased use of mobile apps for search, content and social activities is estimated to reach £73.82bn by 2020.[8] Online profiling and advertising practices are regarded as central to unlocking the value of personal data belonging to consumers. We do not need to be privacy or child safety scholars to realise that calls for industry to exercise self-restraint "with regard to behavioural advertising, [so that] no such segments are created to target children" is far from being a policy that will guarantee the pursuit of children's best interests (Commission 2012a: 13). If the Commission's purported child-centred focus can be queried, might similar doubts about the ability of EU data protection law to constrain the undesirable consequences that may follow from the problems of aggregation and behavioural advertising? Data protection rules are not based on requiring industry to positively advance the interests of individuals (Purtova 2014: 204-221). Its legacy and continued relevance lies in the uneasy relations between the pursuit of economic objectives and ensuring

7 See also Department for Business (2015): Innovation & Skills UK vision for the EU's digital economy; and Kunster and Thomas et al. (2013)..

8 ABI forecast available at https://www.abiresearch.com/market-research/product/1019237-mobile-security/.

that fundamental rights are not eroded, as the following observation makes clear:

> two of the oldest and equally important ambitions of the European integration process: the protection of fundamental rights and freedoms of individuals and in particular the fundamental right to data protection, on the one hand, and the achievement of the internal market – the free flow of personal data in this case – on the other. (Commission2010b)

Balancing these two goals has never been straightforward.[9] As new technologies and networked environments increase business access to individuals' personal data, concerns have been expressed about the impact of such activities on individuals' fundamental rights (De Hert and Papakonstantinou 2012: 42). A study conducted in 2012 of apps available on Apple's iTunes app store, Google's Play App store, and Amazon's Kindle Fire App store revealed the lack of transparency and varying degrees of compliance with privacy obligations.[10] Turow, for example, observes that the design of communication spaces embeds a power structure through which audience expectations are shaped and defined to serve the pursuit of economic objectives (2011: 174-189). This is a valid observation, not least because it underlines the constant resource demands placed on data protection officials to enforce its rules:[11]

> The fragmented nature of the app ecosystem, the wide range of technical access possibilities to data stored in or generated by mobile devices and the lack of legal awareness amongst developers create a number of serious data protection risks for app users. These risks range from a lack of transparency and lack of awareness amongst app users to poor security measures, invalid consent mechanisms, a trend towards data maximisation and elasticity of data processing purposes. (Article 29, 2013: 27)

Data protection laws have by necessity rather than by design developed solutions through a complex process of rule-making, investigation and negotiation. We see some of the limits to this rule making, particularly within the context of online profiling and targeted advertising. The structure of data protection law and its role in mediating ongoing tensions between innovation and individual rights, as well as the ongoing problems of transparency, ac-

9 It is also worth noting that data protection is regarded as being concerned with internal markets (first pillar) and law enforcement and judicial co-operation (third pillar) rather than across all three pillars. See background provided by Simitis 1987; Gutwirth 2012; Gellert and Gutwirth, 2012).

10 Future of Privacy Forum, FPF Mobile Apps Study (June 2012) 1-5, available at http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf. See also FTC staff report Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Feb. 2012) available from http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

11 The Article 29 Working Party is an independent body of the European data protection authority. One of its roles is to advise the European Commission on issues related to personal data protection.

countability and proportionality can be highlighted by turning to its unique rules.

The principal argument canvassed here is that EU data protection Directives provide a set of default rules that leans towards promoting information access. Checks on non-compliance are however left to negotiations, threats of sanctions and monetary penalties.[12] The economic logic of monetizing personal information is to a large extent also reflected in the limits placed on data protection rules to control information flows, with the result that significant externalities end up being placed on individuals, requiring them to make complex trade-offs (Brownsword 2009; Federal Trade Commission 2012).

The discussion below will show that the model of empowerment, with its emphasis on control and consent as a ground for processing personal data may be sound in theory but its application and implementation leaves much to be desired.

3.1 Personal Data

The EU data protection legislation governs the processing of 'personal data', which has been defined as:

> Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity. (Article 2(a) 1995 Directive)

This broad definition of personal data has kept pace with the way new generation of technologies capture information created by and about individuals.[13] Customisation, the development of sophisticated marketing and advertising techniques and the ease with which personal data is made accessible has led to an exponential growth in markets for collection, storage and processing of personal data. The "database privacy problem" that Solove highlights foreshadows the transformative nature of new technologies (Solove 2001: 1399).[14] The breadth of the definition of personal data under Article 2(a) of

12 See Article 29 Working Party letter to Google requiring it to review its privacy policies: http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf and Google's undertaking following the investigation by a number of national data protection authorities: https://ico.org.uk/media/action-weve-taken/undertakings/1043170/google-inc-privacy-policy-undertaking.pdf.

13 See for example, World Economic Forum, Personal Data: The Emergence of a New Asset Class, 2011, available at http://www.weforum.org/projects/rethinking-personal-data; and Zarsky 2004.

14 Solove, D (2001) *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, pp. 1404-1407 (p. 1399: "The Big Brother metaphor is definitely effective at cap-

the 1995 Directive corresponds with the emergence of personal data as a new class of assets (Zarsky 2004: 45). Recital 26 of the 1995 Directive provides that when determining whether a person is identifiable, account must be taken of "all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Digital technologies not only enable information, which is volunteered by individuals, to be collected but also those which are based on inferences and predictions derived from aggregated personal data.

For example, 'personal data' for the purposes of Article 2(a) of the Directive will include not only biographical or other personal information but also web searches, browsing history, devices used, activities on social media sites, emails, phone calls and user-generated content.[15] As society becomes increasingly connected with a range of technologies "behaviour is increasingly monitored, captured, stored, used and analysed to become knowledge about people, their habits and their social identity" (Van der Hof and Prins 2011: 111).

3.2 Conditions Imposed on Processing Personal Data

Articles 6 and 7 of the 1995 Directive provide a core set of obligations and safeguards in relation to the processing of personal data. Article 7, sets out a number of grounds where processing activities are regarded as legitimate. For example, processing of personal data by a party (known as the 'data controller') is lawful when an individual (known as the 'data subject') has given unambiguous consent (Article 7(1)(a) 1995 Directive). However, consent is not the only ground under which personal data can be processed. Processing undertaken to conclude a contract to which the data subject is a party or where processing of personal information is one which is imposed by law on a data controller is regarded as legitimate. While these grounds are regarded as legitimate *a priori*, Article 7(1) (f) of the 1995 Directive states that processing in the absence of consent is legitimate as long as it is regarded as:

…necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

turing certain privacy problems, but not all privacy problems are the same. I argue that the metaphor fails to capture the most important dimension of the database problem: the nature of our relationships with public and private bureaucracy and the effects of these relationships on human dignity and freedom.")

15 Article 29 Working Party Opinion 4/2007 on the concept of personal data (WP 136) pp. 16-17.

Processing of sensitive personal data relating, for example, to a person's race or ethnic origin, political opinions, health and sexual life have stricter requirements (De Schutter and Ringelheim 2008: 362) The fact that the grounds of processing are legitimate under Article 7 does not necessarily bring the matter to an end. Article 6 introduces a set of normative criteria, which the data controller is expected to respect. The values and standards which processing of personal data activities must adhere to are: fairness and lawful processing, minimality, purpose specification, information quality, data subject participation and control, disclosure limitation and information security. While there is some agreement regarding the circumstances when processing is lawful, determinations regarding the fairness of processing are not entirely straightforward. Recital 36 lends some colour to the scope of the inquiry, and provides that:

> if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.

Fairness has been interpreted as requiring data processing practices to be transparent and not disproportionate in view of the purposes for which the personal data was originally collected.[16] Both transparency and proportionality are regarded as an integral part of the balancing of the data subject's and data controller's interests. The principles of minimality and purpose of limitation are an obvious expansion of the principle of fairness. Article 6(1) (c) of the 1995 Directive provides that processing must be "relevant and not excessive in relation to the purposes for which they are collected and/or further processed". The purpose limitation principle engages both fairness and lawfulness, and states that "personal data shall be collected for specified, lawful and/or legitimate purposes and not subsequently processed in ways that are incompatible with those purposes."

There are three elements to the purpose limitation principle. First, data controllers are required to notify the data subject of the purposes for which processing is undertaken. Second, data controllers are required to adhere to the reasonable expectation of data subjects that the processing is compatible with the original purposes for which personal data was collected. Third, the purposes of processing must be lawful. The principle of information quality, which again overlays the grounds under which Article 7 processing is permitted, imposes a series of requirements, namely, that the personal data that is collected and processed is valid, relevant and complete. There is an expectation that data controllers take reasonable steps to ensure the quality of data (Article 6(1) (d)). Finally, even though Article 6 does not explicitly state the primacy of data subjects' reasonable expectation of control over the pro-

16 ECtHR, *Leander v. Sweden*, No. 9248/81, 26 March 1987, para. 58. Decision of 9.11.2010 in Joined Cases C-92/09 *Volker und Markus Schecke GbR* and C-93/09 *Hartmut Eifert*.

cessing of personal data, we can extrapolate from Articles 7, 8, 12 and 14, 'consent' type obligations and rights, a principle of information self-determination (Rouvroy and Poullett 2009: 51). For example, even if a data controller can lay claim to processing without relying on Article 7(1) (a), as may be the case when Article 7(1) (f) is relied upon, the principle of self-determination may provide the data subject with an expectation that certain wishes are respected. For example, the data subject could request access to information relating to decisions reached as a result of automated processing of personal data (Article 12(a)). Article 14(b) provides the data subject with the right to object to the processing of personal data for direct marketing purposes. This cursory overview of the EU data protection rules raises questions as to whether they impose adequate and sufficiently tailored constraints on industry data collection practices which correspond with the Commission's children's rights strategy.

3.3 Profiling and Behavioural Advertising: A Closer Look

The creation of user profiles through automated processes and targeted advertising are regulated by EU data protection law. For example, Article 15 of the 1995 Directive deals with the automated practice of constructing user profiles based on volunteered information, online activities and inferences derived from browsing history and clickstream activity. Increasingly, the development of sophisticated data analysis technologies and design of communication platforms have not only allowed for user profiles to be constructed but have also enabled advertisers to use such information to target individuals based on their personal characteristics such as age, gender, lifestyle interests and preferences and online activities. The 1995 Directive does not deal with the act of installing software onto communication devices with a view to engaging in processing of personal data. This software, also known as 'cookies', enables websites to monitor an individual's browsing activities, preferences and sites visited by users. Directive 2002/58/EC (as amended), also known as the e-Privacy Directive, deals with a particular form of information collecting practice.[17] The e-Privacy Directive transposes the data protection principles and safeguards set out in the 1995 Directive. Article 5(3) of the e-Privacy Directive permits:

17 The Directive states that users must give their consent before software can be stored on their terminal equipment, or that access to such information may be obtained. In order to do this, users must receive clear and comprehensive information about the purpose of the storage or access. These provisions protect the private life of users from malicious software, such as viruses or spyware, but also apply to cookies.

…the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing.

At first sight, it would seem that the 1995 Directive and the e-Privacy Directive would resolve concerns raised by online profiling and behavioural advertising. There are four possible arguments in favour of this view. First, control is achieved since processing of personal data will only be legitimate if one of the grounds set out in Article 7 is present (see above). Second, consent of the user and 'consent type' provisions provide an important regulatory oversight over the collection practices. Third, the principles of proportionality, purpose limitation and fairness will limit potential misuse of personal data. Fourth, the principle of information self-determination will align data controllers' processing activities to the expectations of the data subject. It is agreed that 1995 Directive has a number of provisions that directly address data protection concerns. However, the existence of these substantive safeguards does not imply that industry behaviour is constrained in practice. Additionally, the substantive principles are widely drafted and the particular type of activity covered by Article 15 is significantly limited (Robinson, Graux, Botterman and Valeri 2009: 40). As an example, consider Article 15(1) of the 1995 Directive, which provides that every person has the right:

…not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

Data subjects control over profiling is limited. Consider for example, Jenny,[18] who purchases five pizzas from a supermarket every Friday. The supermarket's computer processes the information and automatically sends Jenny some discount vouchers. Although automated processing has taken place, it would not give rise to legal effects. Neither would profiling – 'Jenny likes pizzas' – be regarded as involving an evaluation of "personal aspects relating to [her]". The decision to send Jenny discount vouchers is arguably based on objective or factual data. Similarly, automatically generated ads based on information posted on Jenny's profile page on Facebook or photos uploaded on Instagram would fall outside the mischief of Article 15. An example of a situation where automated processing produces legal effects, would be inferences drawn from Jenny's volunteered information on Facebook that she is likely to engage in criminal activity, based on racial, geographical or demographic data.

18 Jenny is a hypothetical young girl (child) used here for the sake of the argument.

A point worth emphasising is that EU data protection rules do not regard protection of personal data as an absolute right and neither is the data subject's consent essential as a ground for processing under Article 7. That said, as noted previously, Member States do provide data subjects with an opportunity to object to unsolicited direct marketing and particular forms of automated processing.[19] Behavioural advertising which relies on constructing profiles based on browsing behaviour is not covered by Article 15 of the 1995 Directive, as tracking is only made possible when software is installed onto users' computers. Article 5(3) of the e-Privacy Directive requires that users be provided with "clear and comprehensive information" and must give their prior informed opt-in consent before any cookies are set on their "terminal equipment" (e.g., computer or mobile device). This is an important safeguard, in theory. Under the previous 'cookies' rule businesses were only required to provide notice and an opt-out mechanism.[20]

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, which implements the EU rules on cookies, requires third parties delivering ads to web users, with a view to monitoring their user behaviour, to provide clear and comprehensive notices. Explicit consent is required when third parties capture all browsing activity.[21] The reality however is very different. Websites provide pop-boxes for individuals to accept the terms of service before cookies are installed. It is common to find websites providing a hyperlink to a separate page for individuals to review the privacy policy. Most users merely click the 'I Agree' box to access content and services. Where an individual does not accept the installation of cookies, access to the contents on the site is either restricted or blocked. It should not be overlooked that the mere fact a web user opts-out of online behavioural advertising does not bring to an end other forms of generic online advertising. There are other limitations to the e-Privacy Directive. Websites for example can store personal information and can collect, store and process information, which they deem to be strictly necessary in the event that services have been expressly requested.[22] On a practical level, due to the range of data collection and sharing practices, the idea of information self-determination in a networked environment may at best be unrealistic since individuals lack the time, resources and skills to identify and track their extensive digital trails being monitored by websites. This is particularly salient in relation to chil-

19 Section 12(2) Data Protection Act 1998 requires the data controller to inform the data subject if decisions have been taken through automated processing of personal information.

20 The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 implemented the new rule in the UK.

21 The Advertising Standards Authority regulates online behavioural advertising in the UK.

22 See study by Mayer, J. R. and Mitchell, J. C. *Third-Party Web Tracking: Policy and Technology*, PROC. 2012 IEEE SYMP. ON SECURITY & PRIVACY 413, 415 (2012), available at https://cyberlaw.stanford.edu/files/publication/files/trackingsurvey12.pdf.

dren. Given the scale of collection and ready availability of technologies to process and analyse information, it would be impossible for data subjects (and certainly children) to detect violations of these data protection regulations or misuse of their personal information.[23]

Finally, the Commission's suggestion in the EU Strategy that data controllers observe the 1995 Directive rules, assumes that there are effective accountability mechanisms to restrict self-seeking behaviour and commercial interests. Ascertaining whether data protection obligations have been breached is far from straightforward and is contingent on individuals establishing that the grounds for legitimate processing are not present and, if legitimate, do not meet the thresholds of the guiding principles. Further complications may arise by virtue of the fact that the terms of service and privacy policies used by social media businesses and organizations invariably result in individuals ceasing to retain much control over their personal information. As Marwick and Boyd point out, many individuals turn to self-help strategies and "develop innovative mechanisms for achieving privacy in response to the technical architectures and social dynamics that underpin networked publics" (2014: 1052).

3.4 Proposals for Reform: The General Data Protection Regulations

Negotiations for the proposed reform to Directives 95/46/EC and Directive 2002/58/EC are reaching a conclusion.[24] The General Data Protection Regulations ('Regulations') aim to provide an overarching framework regulating the processing of processing of personal data in keeping with the needs of modern economies and societies. The Regulations still keep intact the sub-

23 See Reference for a Preliminary Ruling from High Court of Ireland (Ireland) made on 25 July 2014 *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14), 2014 O.J. (C 351) 5.

24 The Draft Regulation is being considered by the European Parliament, the European Commission and the Council of the European Union. Governments, industry and organizations are engaged in ongoing discussions and lobbying. The Draft Regulation will be adopted through the legislative procedure, with both the European Parliament and the Council of the European Union jointly adopting the legislation. On the position of the European Parliament see http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201, the 'Albrecht' Draft Report 2012/0011(COD), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf and LIBE Committee, Compromise Amendments on the General Data Protection Regulation (voted on 21 October 2013), http://www.europarl. europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/ comp_am_art_01-29en.pdf.

stantive principles under the 1995 Directive while including the principles of transparency and data security. For present purposes, the Chapter will highlight those that relate to the EU Strategy and the model of empowerment. 'Privacy by design' is envisaged as a measure to provide for more effective protection of the rights of data subjects, particularly children. The Commission has proposed the definition of a child for the purposes of data protection to be an individual under 18 years. The Regulations also require data controllers to adopt measures that incorporate plain language, so that the question of whether consent has been obtained is not in doubt, particularly where children are involved. More specifically, social media services will require consent of parents where the child is under 13 years old (Jasmontaite and De Hert 2015: 22-24). Article 8(1) of the Regulation states that information society services directed to a child below the age of 13 are lawful only if the child's parent gives consent. For example, 'personal data', which is processed for profiling or behavioural advertising purposes will now be subject to safeguards under the Regulation. Article 4(8) of the Regulation makes explicit the meaning of consent for the purposes of data protection:

> the data subject's consent means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

Article 20(2) of the Regulation would possibly benefit from being made clearer. There needs to be specific provision making clear the obligation that children and their parents should be provided with meaningful information, such as the types and range of profiling activity, the information collected, the use made of the information, information sharing arrangements purposes and the grounds upon which the processing can be said to be compatible with the 'best interests of the child' principle. There is an important caveat to this recommendation. It is not entirely clear the basis upon which policymakers feel confident in assuming that children or their parents can or should assume responsibility over the management of the child's personal data. Could we really expect parents and their children to monitor how companies are processing personal information?

That said, Article 20 of the Regulation is to be welcomed since it now introduces a specific right of an individual not to be profiled and as a result modifies Article 15 of the 1995 Directive. However, the limitations identified under Article 15 of the 1995 Directive are still present. For example, data controllers can still collect and categorise personal information under Article 20(2) of the Regulation, if it is undertaken for the purposes of entering into a contract to which the data subject is a party. Under the Regulation data controllers need only provide 'suitable' rather than 'effective' safeguards, which protect the legitimate interests of the data subject. Profiling is still permitted where it is shown that "processing is necessary for the purposes of the legitimate interests pursued by a controller". The absence of any definition of

profiling is very likely to perpetuate the asymmetrical relationship between children and data controllers. In short, the benefits to children under the Regulation are likely to be marginal, since automated processing which involves assessments or predictions based on factual data, relating to preferences, interests and movements will still be permissible.[25]

Even though the final text for the Regulation has yet to be realised, concerns have already been expressed in relation to the safeguards children can expect with regard to the management of their personal information. For example, Purtova suggests that the legitimate interests of the data controller and contractual terms may embed the imbalance and power structures that already exist as between data subjects and data controllers (Purtova 2014: 204-221). It is worth recalling that the legitimate interests ground for processing under Article 7(f) of the 1995 Directive can only be overridden if proven to erode fundamental rights.[26] Article 6(1) (f) of the Regulation leaves data controllers with the task of balancing their 'legitimate interests' against the interests of data subjects to protection of their fundamental rights and freedoms. Suggestions that individuals' in networked environments can fully assert control over their personal data do not give enough weight to the significant imbalance that exists between social media companies and individuals. Networked publics force individuals to make complex trade-offs between the desire for privacy and the need to communicate and participate (Bruns 2013: 14). There is a much broader aspect to the issue of empowerment that data protection rules have yet to fully engage with, namely, whether more can or should be done to ensure that industries assume greater responsibility in the way children's personal data is collected and used (Acquisti, Brandimarte and Loewenstein 2015: 509-514). Finally, van der Hoff, while acknowledging that great strides have been taken in bringing to the forefront of public and industry consciousness the needs and reasonable expectations of children, has questioned whether the aspirations will materialise into meaningful measures (2014: 139-140). As Gillespie observes, communication platforms are business models which continuously:

25 It is however not entirely clear whether Recital 58 of the regulation, which discourages profiling of children will be explicitly stated in the final text of Article 20 of the Regulation. See also the Article 20 Working Party Opinion 02/2013 on apps on smart devices, February 2013, www.cbpweb.nl/downloads_int/wp202_en_Opinion_on_Mobile_Apps.pdf, p. 26, and Opinion 2/2010 on online behavioural advertising, 22 June 2010, p. 17: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

26 Decision of 24.11.2011 in Case C-70/10 (Scarlet Extended v SABAM), Decision of 16.2.2012 in Case C-360/10 (*SABAM v Netlog*), CJEU in Case C-524/06 *Heinz Huber v FRG* [2008] ECR I-9705, ECtHR, and *Marper v the United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008; see also, for example, ECtHR, *MM v the United Kingdom*, No. 24029/07, 13 November 2012, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communication et al.* and *Kärtner Landesregierung et al*., judgment of 8 April 2014.

> have to strike their own balance between safe and controversial, between socially and financially valuable, between niche and wide appeal. And, as with broadcasting and publishing, their choices about what makes it onto the platform, how it is organized, how it is monetized, what can be removed and why, and what is technically possible or prohibited, are all real and substantive interventions into the contours of public discourse. (2010: 409-410)

Gillespie is also alluding to the carefully crafted relationship social media companies and organizations have with end users, advertisers and professional content producers (Ibid.). Any expectation of empowerment over personal data or privacy, and tensions created from monetizing content on social networking sites is diffused through carefully constructed terms of service and appeals to the rhetoric of placing the individual in charge.

The EU model of empowerment, against the background of EU data protection law, still leaves us with a conundrum: how should children's needs and reasonable expectations be integrated into data protection rules? Is it right that participation in online playgrounds means that children forego their reasonable expectations to privacy and rights to self-determination of their personal data? In the next section we can explore some ideas regarding the integration of children's needs and expectations into EU data protection legislation in a manner that is compatible with children's reasonable expectations and rights while being alive to the political, economic, and social drivers of the broader policy agenda in the EU.

4. A Counterfactual Analysis: What if…?

Both the EU Strategy and reform of EU data protection legislation face the challenge of enabling data controllers to fully realise the economic value of personal information, whilst at the same time ensuring that data subjects' fundamental rights are not eroded. Policymakers have been extremely keen to proclaim the importance of taking into account children's needs and expectations but fall short of articulating how economic and developmental issues that impact children can be better addressed. Positioning children's rights has been a constant preoccupation of policymakers in the realm of the networked environment ever since convergence enabled children to take advantage of the Internet and access an array of online services.[27] Even though promoting

27 See the Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU, available at: www.rcysostenibilidad.telefonica.com/blogs/wp-content/uploads/2012/01/ICT_Principles.pdf, European Framework for Safer Mobile Use by Young Teenagers and Children; http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm.

trust and confidence posed enormous challenges, solutions were eventually found by first, resisting the urge to devise policies founded on out-dated notions of the way children mediated their online interactions (Livingstone and Bulger 2013). Second, it was accepted by policymakers that responsibility for online child safety governance should be implemented by three groups of actors, and not just children and their parents: (i) those who make the technologies; (ii) those who make consumption of the technologies and services available; and (iii) those who consume the technologies and services.[28]

In the remainder of the discussion, I would like to highlight how data controllers, principally those who make the technologies and those who provide the services could use the CRC as a framework for initiating further discussions with all stakeholders with a view to developing principled and workable solutions. What follows is a sketch of some of key principles and strategies that could form the basis of future discussions when grappling with the interplay between Articles 24, 8 and 7 of the Charter within the context of data protection rules.

4.1 Applying the Convention on the Rights of the Child to the protection of children's personal data

The CRC continues to provide "basic standards that apply without discrimination to all children worldwide" as well as informing frameworks for governance (Livingstone and Bulger 2013: 2). Livingstone and O'Neill argue that even though the CRC does not provide strong guarantees and its rules are unevenly implemented, it does provide an admirable touchstone and logic that is difficult to ignore (2014: 19-38). The CRC sets out basic standards and specifies minimum standards that help steer policymakers towards developing principled and sustainable strategies. There is general consensus that its well-established principles are coherent and conceptually defensible. The Commission's Communication *An Agenda on the Rights of the Child* ascribes to this view in its statement that "[t]he standards and principles of the CRC must continue to guide EU policies and actions that have an impact on the rights of the child" (Commission 2011a:3). The CRC's emphasis on the value of personhood, encapsulated in the best interests of the child principle, is indispensable to the information management dilemmas facing children in networked publics, even where conflicts in interests may arise between data controllers and data subjects. Forging a consensus and devising credible and

28 On the issue of self-regulation and co-regulation see Rubinstein, I. (2011) Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes. In: *A Journal of Law and Policy for the Information Society* 6 I/S pp. 355-423.

sustainable strategies is an immediate challenge. One advantage policymakers have and which was unavailable during the mid-1990s is that we have come to utilise various regulatory techniques and strategies in reaching our goals. The success of the online child safety governance model cannot be disassociated from the value placed by all stakeholders to the norms and principles of the CRC and its continued influence.

The provisions in the CRC have natural affinity with the participatory opportunities provided by the Internet and communication technologies. Personhood, in view of the CRC will also include freedoms such as autonomy, dignity, identity and privacy as they are essential to enabling children to develop into rational mature adults. The CRC can be seen as providing minimal standards, which organizations and adults in society are expected to adhere to, where these impact children. The best interests of the child principle also encourages businesses to take positive measures that promote well-being, development and fulfilment. As the Committee on the Rights of the Child reminds us, we must not readily assume that the opportunities for economic growth will result in children's rights being advanced (Committee on the Rights of the Child 2013). The concerns raised in this chapter would be met if:

> …in the context of business activities and operations … all business-related policy, legislation or administrative acts and decision-making [are] transparent, informed and include full and continuous consideration of the impact on the rights of the child. (Committee on the Rights of Child 2013: paragraph 26)

What must businesses do? It is perhaps here that the CRC norms can be used to develop a principled and coherent response, which overcomes some of the problems with the EU Strategy and the empowerment model. The communication spaces that define social media business models need to better reflect children's expectations when participating in networked publics. New technologies and access to diverse media enable children to assume multiple roles, and create opportunities for association and expression. Consideration also needs to be given to the value of selfhood. Profiling, online advertising practices and web-tracking practices should not be regarded as simply another transactional opportunity.[29] As Carr observes:

> The self is rarely fixed. It has a protean quality. It emerges through personal exploration, and it shifts with circumstances. That's especially true in youth, when a person's self-conception is fluid, subject to testing, experimentation and revision. To be locked into an identity, particularly early in one's life, may foreclose opportunities for personal growth and fulfilment. (Carr 2015: 206)

29 See empirical work done by Rader, E: *Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google* (Conference Paper) available at https://www.usenix.org/system/files/conference/soups2014/soups14-paper-rader.pdf; Bonneau, J and Preibusch, S. (2009) The Privacy Jungle: On the Market for Data Protection in Social Networks, in: *Workshop on the Economics of Information Security* (WEIS), May 2009.

It should also be borne in mind that children do not intuitively regard their online interactions as being subjected to ongoing monitoring. Addressing the needs of children requires an appreciation of the context, which defines children's lifeworld in networked publics (Nissenbaum 2010: 241-243). We can now turn to the pathways which provide a coherent and principled as well as being alive to commercial reality.

4.2 'What if'?

Two avenues could provide the basis for developing opportunities for demonstrating commitment to CRC Principles: (i) Codes of Practice; and (ii) Privacy by Design (PbD).

4.2.1 Codes of Practice

Data protection rules provide a general framework of duties and obligations. The Regulation explicitly identifies children's needs as an important consideration to be taken into account. Codes of practice provide businesses with one instrument through which commitments to CRC can be demonstrated. There are three specific benefits in using codes of practice. First, we need to recognise that children are not a homogenous group of individuals and their needs may vary according to the activity or sector (e.g. education, play, exchanging information and accessing content). Codes of practice provide businesses with a degree of flexibility and adaptability. Second, self-regulation enables businesses to assume direct responsibility for managing children's concerns and needs, and with the added benefit that business practices may even exceed regulatory baselines, for example, as those set out in Articles 6 and 7 of the 1995 Directive. Third, steps can be immediately taken to initiate self or co-regulatory standard setting measures that integrate CRC principles into industry or sector specific codes of practice (Savirimuthu 2012: 242-262). The use of codes of practice is already regarded as an accepted regulatory mechanism under Article 27(1) of the 1995 Directive:

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have

drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Rather than leave industry to determine what it regards as the standards for accommodating children's needs and interests, CRC principles could be regarded as providing the 'bright-line' of standards, which are commensurate with the information management dilemmas encountered by children. Codes of practice can supplement existing 1995 Directive protections and offer one possible avenue through which we can begin to establish the level of standards deemed to be appropriate for children (Information Commissioner's Office 2010: 17).

4.2.2 Privacy by Design

Policymakers and scholars have turned to engineering solutions to help address information self-management and related dilemmas. This solution is described as 'Privacy by Design' (PbD).[30] PbD is based on the premise that businesses consider privacy anxieties and risks at the outset, rather than leave that question to be addressed after privacy concerns emerge when individuals use the product or services.[31] PbD can be viewed as one regulatory strategy, through which CRC principles and values can be promoted. There is some evidence suggesting that shifting the mindset of product developers and innovators to think about privacy and consumer concerns at the outset may have trust generating properties (Cavoukian 2012). Rubinstein and Good for example, using Google and Facebook as a case study, demonstrated that many of the privacy incidents could have been avoided by introducing design solutions and taking into account consumers use of products and services at

30 For a recent overview of the state of play on this issue, see Danezis, G. et al. (2014) *Privacy and Data Protection by Design – from policy to engineering*, EU, ENISA; Castelluccia, C. and Narayanan, A. (2012) *Privacy considerations of online behavioural tracking*, EU, ENISA; Cavoukian, A. and Prosch, M. (2010) *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, Office of the Information and Privacy Commissioner of Ontario available online at http://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf.

31 Directive 1995/46/EC, recital 46, which deals with the interpretation of Article 17, indicates that security measures cannot simply be added into systems, but should already be incorporated when designing the processing system and the processing itself, a principle known as 'privacy-by-design'. Article 14(3), e-Privacy Directive, can be interpreted in a similar manner; the Commission has the power to set out rules on designing terminal equipment in such "a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications".

the outset (Rubinstein and Good 2012: 1333-1414). Swire, in his examination of social networking sites, identifies the role played by designs of communication spaces in users' decision to share or withhold information (Ibid.: 103-105). He observes that individuals tend to be relatively uninhibited in social networking sites and the absence of any constraints in the design of communication platforms may at times lead to bad information sharing practices that in some instances result in privacy harms such as loss of reputation, dignity and respect. Both examples illustrate that a balance has to be struck between the use of design and adoption of other strategies such as education.

It should also be borne in mind that engineering solutions are not necessarily the best way of addressing all problems resulting from youth indiscretions and information sharing norms that expose children to privacy harms. Swire also makes another pertinent observation – the model of empowerment may not always be appropriate, as the restriction on flows of information may also collide with fundamental rights such as the freedoms of association and expression (Ibid.). One could interpret Swire's conclusions as reminding policymakers of the dangers of imposing additional regulatory burdens when other optimal measures should be considered. Brown, in a recent study on the UK approach to the introduction of smart meters in households highlighted the economic and social costs from the failure of policymakers to integrate meaningful data protection measures during the product development phase (Brown 2014: 172-184). One conclusion that could be drawn is that failure to implement privacy enhancing protections at the outset may be counterproductive since they may alter business incentives, increase compliance costs, heighten consumer mistrust and ultimately deprive industry from unlocking the value of persona data (Savirimuthu, 2013: 161-186).

The use of engineering solutions to address some social problems within the context of children's engagement with new communication technologies is not new. Design solutions have been long been used by Internet Services Providers to ensure that children do not gain access to illegal or inappropriate content and services. Finding the right balance between integrating privacy values at the developmental phase and at the user phase may appear to be burdensome. This however is not necessarily true. For example, in relation to products such as smartphones, tablets or Apps, developers can easily consider at the outset whether the privacy risks are of such a nature to justify PbD. Even in this sector specific area solutions are already being made available. The UK's Information Commissioner's Office, recently provided guidance to app developers of mobile devices, including game consoles and smart TVs, highlighting simple design solutions that could be adapted to take into account the lifecycle of personal data and users' needs.[32]

32 Information Commissioner's Office, Privacy in mobile apps: Guidance for app developers, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/online-and-apps/. A global survey of mobile apps discovered that over 85% of mobile apps did not provide

It is particularly instructive to note that the specific measures identified in the guidance enable app developers to accommodate the needs of users such as children through a mix of design and awareness creating solutions: (i) use of language that the target audience understands; (ii) stating how personal data is collected and will be used; (iii) ensuring that notices enable meaningful choices to be made; and (iv) layering notices (ICO 2013: 8-9). A broader lesson to be learnt is that targeting the right activity and audience will be important. If implemented correctly at the outset, PbD can avert mistrust and support children who may be vulnerable or impulsive. We can see the value of PbD in recent examples involving concerns relating to in-app purchases made by children, as noted in the EU Strategy. This outcome could have been anticipated by designing payment authorisation and certification solutions, which require prior adult authorization. It is after all conceivable that children engaged in playing games would end up making in-app purchases on mobile phones.

The idea of a counterfactual is not as fanciful as it might seem. The Digital Agenda for Europe, which is one of the European Commission's initiatives under the Europe 2020 Strategy, can be regarded as preferring PbD as an important part of the regulatory toolkit which enable the 1995 Directive rules to promote users confidence and safeguard their fundamental rights (Commission, 2010b: 17). Codes of practice and PbD encourage a process-oriented mindset but in slightly different ways. These pathways direct businesses towards the value of identifying and implementing measures that are not only feasible but principled and responsive to children's needs and expectations.

Acting 'as if' would also shift the responsibility onto businesses to devise, in collaboration with other stakeholders, creative approaches to vesting children with rights to information self-determination, in the sense of what Altman regards as "selective control of access to the self" (Altman 1997: 67). Codes of practice and PbD could be used to deal with the practice of online profiling and web advertising through the provision of information and meaningful choices.[33] Inferring patterns of behaviour with a view to attaining commercial objectives would have to be justified and moderated by assessments on the impact of decisions made on children. Codes of practice could augment current 1995 Directive rules and design solutions. For example, codes of practice could make explicit the specific responsibilities and obligations with a view to demonstrating commitment to recital 58 of the Regulation:

Every natural person should have the right not to be subject to a measure which is based on profiling by means of automated processing. However, such measure should be allowed

adequate privacy notices, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/09/global-survey-finds-85-of-mobile-apps-fail-to-provide-basic-privacy-information/.

33 See above note.

when expressly authorised by law, carried out in the course of entering or performance of a contract or when the data subject has given his consent. In any case, such processing should be subject to suitable safeguards, including specific information of the data subject and the right to obtain human intervention and that such measure should not concern a child.

Without a principled default position for children, market incentive structures by themselves will fail to provide an effective constraint on industry's desire to leverage the economic value of personal information. Both codes of practice and PbD, it should be stressed, are not the panacea.[34] The aim in this section is to go beyond the model of empowerment and suggest how initiating dialogue and collaboration could help minimise the differences between data controllers and data subjects in a way, which is principled and alive to political and economic realities. More importantly, the discussion leaves open the question of the extent to which CRC principles can be creatively utilised as default principles either in codes of practice or PbD.

Conclusion: Where is Empowerment Taking our Children?

Empowerment is a powerful ideological and rhetorical gambit. As a statement of policy intent it captures our attention. Online playgrounds, like a glass cage, are not neutral environments (Carr 2011: 206). Consent and control are illusions. A fully filled Facebook profile page contains at least forty items of personal data that can be easily processed, used and shared (Grimmelmann 2009: 1149). Once personal data is posted, the reality is that individuals have little or no control over its subsequent use. Consent is rarely meaningful, since many individuals do not read privacy terms when signing up for commercial services. A failure to accept the contractual terms of service will invariably prevent them from participating in networked publics or accessing content or services. Device identifiers, cookies and web beacons, are also redefining spatial privacy in online playgrounds. Every digital footprint is collected, stored and analysed. These technologies now join the list of technologies embedded in networked environments to create a communication space where critical tensions between information self-determination and information access are endemic and mediated in favour of data controllers. The recent experiment by Facebook to gauge the moods of its users by ma-

34 See the correspondence between Article 29 and the advertising industry: Article 29 Data Protection Working Party, Letter to the online advertising industry (OBA) Industry regarding the self-regulatory Framework (August, 2011), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf.

nipulating the messages they were presented with on their news feeds illustrates the growing power imbalance between data controllers and data subjects (Kramer et al. 2014). There is no doubt that networked environments create considerable new opportunities – but there are undesirable characteristics that cannot be ignored. Control and consent are far from being ideal proxies for autonomy and empowerment.

The EU Strategy model of empowerment appears to gloss over the reality of networked environments. Data protection policymakers should not overlook the 'autonomy trap' – children will now be placed in the invidious position of making complex trade-offs. Expecting children to make rational choices and behave responsibly at all times is both unrealistic and burdensome. This chapter has identified shortcomings in the model of empowerment in both the EU Strategy and data protection laws. Easy solutions are difficult to find and formulate. The allure of economic and innovation potential in providing children with online playgrounds has perhaps contributed to the rather rash nod towards data protection laws, without providing any principled basis for ensuring that there is a 'bright-line' of children's needs and expectations that cannot be diluted through appeals to contractual terms and business interests.

It is suggested that the model of empowerment is indeed the wrong solution to some real dilemmas encountered by children in networked environments. The alternative approach of integrating CRC principles more explicitly into the design architecture of networked environments and codes of practice may impress upon everyone of society's collective responsibility towards fulfilling children's developmental needs and expectations rather than being content with defining them by market values and preferences. It is true that even if CRC principles were integrated into codes of practice and design solutions, there is no guarantee of compliance. This is why collaboration and engagement with all stakeholders is critical to creating a regulatory space for ongoing dialogue under the mantle of the CRC.

References

Acquisti, Alessandro; Brandimarte, Laura and Loewenstein, George (2015) Privacy and human behavior in the age of information, in: Science 30, January, pp. 509-514.

Altman, Irwin (1977) Privacy Regulation: Culturally Universal or Culturally Specific?, in: Journal of Social Issues, 33, 3, pp. 66-84.

Andrejevic, Mark (2007) iSpy, Lawrence KS, University Press of Kansas.

Article 29 Working Party (2013) Opinion 02/2013 on apps on smart devices WP 202, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-3.

Bailey, Reg (2011) Letting Children be Children: Report of an Independent Review of the Commercialisation and Sexualisation of Childhood, London, TSO.
Boyd, Danah and Marwick, Alice (2014) Networked privacy: How teenagers negotiate context in social media, in: New Media & Society, 16, 7, pp. 1051-1067.
Brown, Ian (2014) Britain's Smart Meter Programme: A Case Study in Privacy by Design, in: International Review of Law, Computers and Technology, 28, 2, pp. 172-184.
Brownsword, Roger (2009) Consent in data protection law: Privacy, fair processing and confidentiality, in: Gutwirth, S. et al. (eds) Reinventing data protection?, Dordrecht, Springer.
Bruns, Axel (2013) From Homepages to Network Profiles: Balancing Personal and Social Identity, in: Hartley, J., Burgess, J. and Bruns, A. (eds) A Companion to New Media Dynamics, London, Wiley-Blackwell.
Carr, Nicholas (2015) The Glass Cage: Automation and Us, London, Bodley Head.
Cavoukian, Ann (2012) Operationalizing Privacy by Design: From Rhetoric to Reality, Office of the Information and Privacy Commissioner, Ontario, Canada available online at: http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1254.
Cohen, Julie (2012) Irrational Privacy, in: Journal On Telecommunication and High Technology 10, pp. 241-250.
Cohen, Julie (2013) What is Privacy For?, in: Harvard Law Review 126 pp. 1904-1933.
Cohen, Julie (2014) Configuring the Networked Self. Law, Code, and the Play of Everyday Practice, New Haven, Yale.
Committee on the Rights of the Child (2013) State obligations regarding the impact of the business sector on children's rights, General comment No. 16 CRC/C/GC/16.
Communication from the Commission (2010a) Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth, COM (2010) 2020, final.
Communication from the Commission (2010b) A comprehensive approach on personal Data Protection in the European Union, COM (2010) 609, final.
Communication from the Commission (2011a) An EU Agenda for the Rights of the Child COM (2011) 60, final.
Communication from the Commission (2011b) Protecting Children in the Digital World COM (2011) 556, final.
Communication from the Commission (2012a) European Strategy for a Better Internet for Children COM (2012) 196, final.
Communication from the Commission (2012b) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data COM (2012) 11, final.
Communication from the Commission (2012c) Safeguarding privacy in a connected world: A European data protection framework for the 21st century COM (2012) 09, final.
De Hert, Paul and Papakonstantinou, Vagelis (2012) The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals, in: Computer Law and Security Review 28, 2, pp: 1-13.
De Schutter, Olivier and Ringelheim, Julie (2008) Ethnic Profiling: A Rising Challenge for European Human Rights Law, in: Modern Law Review 71, 3, pp. 358-384.
EU Kids Online (2014) EU Kids Online: findings, methods, recommendations, London, LSE.
Fortin, Jane (2009) Children's Rights and the Developing Law, Cambridge, Cambridge University Press.
Federal Trade Commission (FTC) (2012) Protecting consumer privacy in an era of rapid change – Recommendations for businesses and policymakers, FTC Report, March 2012.
Fuster, Gloria Gonzalez and Gutwirth, Serge (2013) Opening up personal data protection: a conceptual controversy. In Computer Law & Security Review 29, pp. 531-539.

Gellert, Raphaël and Gutwirth, Serge, (2012) Beyond accountability, the return to privacy?, in: Guagnin, D. et al. (eds) Managing Privacy Through Accountability, Basingstoke, Palgrave Macmillan.

Grimmelmann, James (2009) Saving Facebook, in Iowa Law Review 94, pp. 1137-1206.

Gutwirth, Serge (2012) Short Statement about the Role of Consent in the European Data Protection Directive, in: The Selected Works of Serge Gutwirth, available from: http://works.bepress.com.ezproxy.liv.ac.uk/serge_gutwirth/80.

Schmidt, Jan-Hinrik, (2014) Twitter and the Rise of Personal Publics, in: Weller, K. et al. (eds) Twitter and Society, New York, Peter Lang.

Information Commissioner's Office, (2013) Privacy in mobile apps: Guidance for app developers, available at https://ico.org.uk/for-organisations/guide-to-data-protection/online-and-apps/

Johnson, Neil and Jajodia, Sushil (1998) Exploring steganography: seeing the unseen, in: Computer 31, 2, pp. 26-34.

Jasmontaite, Lina and De Hert, Paul (2015) The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet, in: International Data Privacy Law 5, 1, pp. 20-33.

Kramer A. D. I., Guillory, J. E. and Hancock, T. J (2014) Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks, in: Proceedings of the National Academy of Sciences, 111, pp. 8788-90.

Lamont, Ruth (2014) Article 24 – The Rights of the Child, in: Peers, S. et al. (eds) The EU Charter of Fundamental Rights: A Commentary, Oxford, Hart.

Kang, Jerry (1998) Information Privacy in Cyberspace Transactions, in: Stanford Law Review 50, p. 1193-1294.

Livingstone, Sonia (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression, in: New Media & Society, 10, 3, pp. 393-411.

Livingstone, S. and Bulger, M. (2013) A global agenda for children's rights in the digital age: recommendations for developing UNICEF's research strategy, Florence, UNICEF Office of Research.

Nissenbaum, Helen (2010) Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford, Stanford Law Books.

OfCom (2014): The Communications Market Report, available at: http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr14/uk/

O'Neill, Brian; Staksrud, Elisabeth and McLaughlin, Sharon (2013) Introduction, in: O'Neill, B. et al. (eds) Towards A Better Internet For Children? Policy Pillars, Players and Paradoxes, Goteborg, Nordicom.

Piper, Christine (2010) Investing in a Child's Future: Too Risky?, in: Child and Family Law Quarterly, 22, pp. 1-20.

Purtova, Nadezhda (2011) Property rights in personal data: A European perspective. Kluwer Law International, The Netherlands.

Purtova, Nadezhda (2014) Who decides on the future of data protection? Role of law firms in shaping European data protection regime, in: International Review of Law Computers and Technology, 28, 2, pp. 204-221.

Richards, Neil (2015) Intellectual Privacy: Rethinking Civil Liberties in the Digital Age, Oxford, Oxford University Press.

Robinson, Neil et al. (2009) Review of the European Data Protection Directive: Technical Report Prepared for the Information Commissioner's Office, Cambridge, Rand.

Rouvroy, Antoinette and Poulett, Yves (2009) The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Gutwirth, S. et al. (eds) Reinventing Data Protection?, Dordrecht, Springer.

Rubinstein, Ira and Good, Nathaniel (2013) Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents, in: Berkeley Technology Law Journal 28, 6, pp. 1333-1414.

Schwartz, Paul (1999) Privacy and Democracy in Cyberspace, in: Vanderbilt Law Review 52, pp. 1607-1702.

Schwartz, Paul (2000) Internet Privacy and the State, in: Connecticut Law Review 32, p. 815.

Simitis, Spiros (1987) Reviewing privacy in the information society, in: University of Pennsylvania Law Review 135, 3, pp. 707-46.

Stalford, Helen (2012) Children and the European Union Rights, Welfare and Accountability, Oxford, Hart.

Solove, Daniel (2001) Privacy and Power: Computer Databases and Metaphors for Information Privacy, in: Stanford Law Review 53, pp. 1393-1462.

Solove, Daniel (2002) Conceptualizing Privacy, in: California Law Review, 90, pp. 1087-1156.

Solove, Daniel (2013) Privacy Self-Management and the Consent Dilemma, in: Harvard Law Review 126, pp. 1880-1903.

Sweeney, Latanya (1997) Weaving Technology and Policy Together to Maintain Confidentiality, in: Journal of Law, Medicine and Ethics 25, 2 and 3, pp. 98-110.

Swire, Peter (2012) Social Networks, Privacy, and Freedom of Association: Data Empowerment vs. Data Protection, in: North Carolina Law Review 90, 5, pp. 101-143.

Tarleton, Gillespie (2010) The Politics of Platforms, in: New Media & Society 12, 3, pp. 347-364.

Tene, O. (2011) Privacy: The New Generations, in: International Data Privacy Law 1, 1, pp. 15-27.

Turow, J. (2011) The Daily You: How the new advertising industry is defining your identity and your worth, New Haven, Yale University Press.

Van der Hof, Simone and Prins, J (2008) Personalization and its Influences on Identities, Behaviour and Social Values, in: Hildebrandt, M. and Gutwirth, S. (eds) Profiling the European Citizen: Cross-Disciplinary Perspectives, Dordrecht, Springer.

Van der Hof, Simone (2014) No Child's Play: Online Data Protection for Children, in: van der Hof, S., van den Berg, B. and Schermer, B. (eds) Minding Minors Wandering the Web: Regulating Online Child Safety, Dordrecht, Springer.

Vincent, J. (2015) Mobile opportunities: Exploring positive mobile opportunities for European children, London, POLIS, LSE.

Westin, Alan (1967) Privacy and Freedom, New York, Atheneum.

Zarsky, T (2003) Mine Your Own Business: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, in: Yale Journal of Law and Technology 5, 1, pp. 1-56.

Zarsky, T (2004) Desperately Seeking Solutions: Using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society, in: Maine Law Review 56, 1, pp. 13-60.

Zwick, Detlev; Bonsu, Samuel and Darmody, Aron (2008) Putting consumers to work, in: Journal of Consumer Culture 8, 2, pp. 163-196.