"It's Your Private Information. It's Your Life." Young People's views of personal data use by online technologies

Liz Dowthwaite[1], Helen Creswick[1], Virginia Portillo[1], Jun Zhao[2], Menisha Patel[2], Elvira Perez Vallejos[1], Ansgar Koene[1], Marina Jirotka[2]

[1]University of Nottingham, United Kingdom
[2]University of Oxford, United Kingdom
{firstname.lastname}@nottingham.ac.uk, {firstname.lastname}@cs.ox.ac.uk

ABSTRACT

Children and young people make extensive and varied use of digital and online technologies, yet issues about how their personal data may be collected and used by online platforms are rarely discussed. Additionally, despite calls to increase awareness, schools often do not cover these topics, instead focusing on online safety issues, such as being approached by strangers, cyberbullying or access to inappropriate content. This paper presents the results of one of the activities run as part of eleven workshops with 13-18 year olds, using co-designed activities to encourage critical thinking. Sets of 'data cards' were used to stimulate discussion about sharing and selling of personal data by online technology companies. Results highlight the desire and need for increased awareness about the potential uses of personal data amongst this age group, and the paper makes recommendations for embedding this into school curriculums as well as incorporating it into interaction design, to allow young people to make informed decisions about their online lives.

Author Keywords

Children and young people; personal data; online technologies.

CSS Concepts

•Social and professional topics~User characteristics~Age~Adolescents •Theory of computation~Design and analysis of algorithms~Online algorithms •Information systems~World Wide Web

INTRODUCTION

Children and young people make extensive and varied use of digital and online technologies, and, as digital natives, have spent their entire lives surrounded by online services. However, children and young people are rarely part of the discussions around online data protection despite being one of the most frequent users groups; perhaps because of the complexities involved in engaging them in research. The motivation for the work described in this paper was to rectify this and include children and young people in discussions of issues that affect them when they go online.

Additionally, the UK school curriculum covers online safety in terms of protection against individuals, such as threats of "sexual predation, online bullying and harassment" (p.145) [4] but does not cover the use of personal data by corporations and online platforms or how children and young people should protect themselves. They are therefore able to talk about, for example, not sharing their location with others (by changing privacy settings and so on), but do not consider how to protect this data from the platforms themselves. This is despite (and in marked contrast to) government regulations (for example the inclusion of Age-appropriate design as a requirement in the UK Data Protection Act of 2018 [15,26] being introduced that focus on protecting children from abuses of persona data by Information System Services (e.g. online platforms) rather than people. The timely nature of this topic is also addressed by a House of Lords report 'Growing up with the Internet', which highlights the need for 'Personal, Social, Health and Economic (PSHE) curriculum in schools to be better equipped to tackle content that goes beyond the 'current e-safety agenda of risk' [24]. Existing approaches to understanding data use are often aimed at average internet users, not children, and other education programmes, such as the AI curriculum by MIT focus on algorithms, but not on the broader data ecosystem. Therefore further aims of this work were to examine what children and young people know and want to know, to begin to raise awareness of the issues, and explore ways of engaging them in the topics.

A series of youth led discussions with 13-18 year olds about their internet experiences were carried out, primarily focusing on issues engendered and perpetuated by algorithmic mediation of platform services. Facilitators worked with a group of young people to develop interactive activities for a series of 'Youth Juries' [50], designed to help young people to engage with and understand concepts more easily. As part of this, two sets of 'data cards' were created with a series of activities surrounding data harvesting and third party sharing. These cards helped the young people to visualise the kinds of data an algorithm may collect from the user, how profiling can take place through combination of data types, and the sharing and selling of data to third parties.

This paper presents the results of these 'data card' activities, especially with regards to the young people's attitudes towards sharing personal data with online technologies, and the value of personal data to the user and to others. Results are discussed in relation to raising awareness of these issues and encouraging designers of online technology to consider what young people need to know at the point of use, so that they can make informed decisions about their online lives.

BACKGROUND

The following sections introduce relevant related work across three main themes. The first two look at attitudes towards personal data collection by online platforms, in terms of profiling and sharing, by adults and youths respectively. The final section introduces the methods used for engaging young people in research around these issues.

Adults' perceptions of personal data online

People are often surprised by the type of data that platforms collect about them, and feel that the amount of data collected is unnecessary [55]. Yet even when participants are made aware and respond negatively, they continue to use the apps or disclose more information than they indicated they would be willing to, in what is referred to as the 'privacy paradox' [18,47,55,65,68]; people are often very pragmatic and are willing to trade some amount of privacy for convenience [18]. Many are also unaware that the information they put online may be shared with or sold to other platforms or companies [2,9,66], often assuming that the main source of income is from advertising [22]. Most people dislike the idea that their data is monetised in order to provide a 'free' service [9], but are also unwilling, or unable, to pay to stop companies collecting information about them [36]. People are also often unaware of the value of their personal data [22] but may be willing to pay to protect their privacy by denying permissions [42].

Attitudes towards the collection and sharing of personal data often vary depending on personal factors such as the previous experiences of the user, their opinion of what constitutes personal data, and the perceived relevance of the data being collected [1,35,36,41,42,55,66]. Perceptions of the platforms collecting the data, including the reputation and purpose of the platform also contribute to these attitudes [7]. Responses are highly varied and context specific: ranging from trust in platforms or understanding that platforms need the data to provide their services [36,55,66] to concern, outrage and a total lack of trust [36,55]. Feelings of apathy [55], uncertainty [1], 'creepiness' [55], and a lack of security [36] have also been found. Many accept that it happens but experience powerlessness, dejection, and resignation [18,55,66]. Marreiros et al categorise users as the 'scared', who are worried about their privacy, the 'naive', who do not understand how information is collected, and the 'meh' who understand but are not worried about their privacy [42]. There is also recognition of personal accountability for what data users share online, although often in combination with feeling that platforms do not take enough responsibility and make user agreements deliberately obscure in order to hide what they are collecting [18]. Younger adults also feel the need to balance their desire for privacy with their desire for 'publicity' [60].

The type of data that users are willing to share with a service also varies, often based on how long the information is stored for and the perceived sensitivity of the data [36,37], as well as the context and the risk of physical harm [36]. Personally identifiable data such as phone number or credit card details are often considered the worst, with users more willing to disclose details such as country of origin or gender [37]. Some users are willing to share their data with a service as long as it is not sold on [36]. However, when it comes to the sale of data to third parties, users have been found to be especially unhappy about 'offline' data such as gender, age, and other identity-related information [9].

Data collected about a user may be used to profile them, whether this data is from a single source or combined from several different sources; for example location data may be used to infer other sensitive details such as income or political views [38]. Little is known about attitudes towards data combination and sharing, although users have been found to be least comfortable with payment details being shared with third parties, followed by online search and browsing history; users also recognised that data sharing was more beneficial to the companies than the users [6]. There are calls for greater transparency and control over the way data is collected and used [66], with suggestions that this may temper concerns and users would be more inclined to accept that it happens [9,37]. Greater control may also mean that a user feels more comfortable and becomes more inclined to overshare [1]. However, privacy notices that explain the purpose of data collection have been shown to alert people to privacy concerns and cause them to make different decisions about sharing data [54].

Children and young people online

All of the research cited so far is based on studies with adults, but specific research and design is needed to support children and young people who may have less ability to comprehend the indirect implications of online privacy risks [28,49,70]. It has been estimated that one third of internet users are under 18 years old [39]. Many sign up to online services at a younger age than the minimum age requirement of platforms (often 13 years old) [34,48]. Parents often wish they had more transparency in their child's use of technology and struggle with their own unfamiliarity with technology [69]. Given that adult knowledge is often lacking, and attitudes are so varied and context specific, how can children be expected to navigate these practices? It is important that the digital world is created with young people in mind, and whilst there are guidelines for the ethical treatment of children online [62,64], several recent reports suggest that there is more to be done to ensure an internet fit for children, both in terms of regulation and design [11,12,28,39]. Additionally, as children grow up surrounded by more and more technology, how they use and understand it can provide new insights: "children represent a large, unique, and underappreciated group of users of digital technologies" (p.47) [20].

Research with children and young people often focuses on ‘stranger danger’ and threats based on other people rather than platforms or data collection [45]. Young children (aged 7 to 11) may have underdeveloped models of privacy and are unable to apply privacy to online dangers because they have not yet experienced it [70]. Among 5-11 year olds, fear of punishment, and the input of parents, rather than concern for privacy played the main role in disclosing information online [32]. Kumar et al argue that existing resources focus too much of “do’s and don’ts” rather than helping children to make their own decisions. They also conclude that “now that children use smartphones and tablets to watch movies, complete homework assignments, interact with friends, and play games, it is more important than ever for children to begin learning about privacy online from an early age. Yet privacy education is rarely a formalized part of school curricula, especially during elementary and middle school” (p.76) [33]. Online safety education usually focuses on safety from other people rather than websites. The lack of education about the digital world can have significant implications for the ongoing well-being of children and young people [20].

In research into online behaviour and privacy, adolescents in particular are often overlooked, with the focus being on the cognitive vulnerabilities of younger children. The younger age group may be seen as more at risk, and teenagers are often difficult to engage with on these issues. However, the emotional vulnerability of teenagers, together with the persuasive design of technologies [27], means they may be “more susceptible to digital marketing and data collection techniques, especially when they are distracted, in a state of high arousal, or subjected to peer pressure” (p.120) [45]. Many young people are concerned about their privacy, but are often unable to protect themselves and are unaware of privacy policies [56]. Lapenta and Jorgensen found that teenagers considered two types of privacy: ‘social privacy’ in which they managed their interactions with peers and others, and ‘data sharing’ which they saw as involuntary and necessary for social participation. They also often struggled to consider that their personal data would be important to anyone and were not concerned about its future use [34,49]. Concerns often revolve around the stealing of their data through identity theft, hacking, and fraud rather than the way their data is used by an individual platform [49]. The same study also noted the same privacy paradox that has been seen in adults. The importance of engaging young people in such research led to the development of the methodology described in the following section.

Engaging young people in research

This section situates the ‘Youth Jury’ methodology employed in this work within existing methodologies often used for engaging young people in research, particularly co-design, focus groups, and interactive workshops. Co-design workshops and co-production of materials with young people have been shown to be effective ways to engage children in research [17,44,49]. The Youth Juries have a strong co-production component. Scenarios (i.e., prompts or stimuli) are co-produced with young people to explore their personal concerns and online experiences. Co-producing scenarios with young people enhances engagement opportunities, making these more real, easier to relate to, and consequently, maximising youth involvement in discussions.

The Youth Jury format combines co-design workshops with focus group methods to create fun and engaging workshops which approach issues that young people care about in ways that they will engage with, in order to allow them to critically think about the issues. Using the terminology ‘juries’ is an important decision to help participants feel a sense of responsibility as decision makers. They are encouraged to provide recommendations and solutions, which are fed into parliamentary inquiries, reports and briefings designed for policy makers and industry chiefs [23,30,43].

Youth Juries are designed around a deliberation process of stimulus-discussion-recommendation that allows young people to receive, exchange, and critically examine information surrounding a topic, and to come to conclusions or recommendations [57]. This process is crucial. The aim of the juries is not only to identify what participants think and feel about the experiences of the digital world but also to discover what shapes their thinking and whether they are open to changing their minds in the light of discussion with peers or exposure to new information.

The method is designed to provide a robust context to ensure that children’s voices are heard and listened to. Youth Juries have previously been used to great success, for example in discussions of digital rights [13,50]. They are used here to explore the impact of algorithmic biases on young people and generate their recommendation for a fairer online world that is best aligned to young people’s expectations and concerns. The first series of juries produced a rich dataset that is continuing to showcase concerns and provide recommendations [29,31,51,52].

The second series of juries involved new co-created activities. This paper focuses on a particular aspect of these, the use of cards to facilitate critical thinking of young people about the sharing and selling of data. Different types of card activities have been used as methodological tools in many different research contexts: for example as ‘thinking tools’ aiding problem solving in design ideation [21], as a human-centered approach to addressing human values in design [19], to aid discussion of online privacy and consent [4], and to make IT law more accessible to citizens [40]. Cards have also been used to help designers to take account of the needs of children and young people, highlighting the importance of making sure materials are appropriate for the intended age group [5,10]. Ideation cards promote reflection on relevant issues, engaging a wide range of stakeholders, in particular non-experts, in generating ideas, promoting critical thinking, and allowing a focus on human values and users’ needs [46].

The contributions of this paper to research on personal data and privacy in online technologies are threefold. First, it reveals the key attitudes and experiences of an underrepresented and often vulnerable group of Internet users – young people aged 13-18 – with regards to personal data-related online privacy risks. This paper also focuses on the online platforms and the algorithms that mediate them, rather than individuals and peers, which is largely neglected in existing online safety curriculums. Second, it demonstrates how the workshops, and indeed such workshops more generally are able to raise awareness of the issues, encourage critical thinking, and identify concerns and barriers to recognising data risks. Finally, it identifies design opportunities, to foster young people's development of such risk recognition and coping skills. In particular it discusses how online spaces could be designed to allow users to make more informed decisions when interacting with technologies, and some of the complexities associated with designing digital spaces in this manner.

METHODS

Participants

A total of 116 young people from the Midlands in the UK took part across 11 youth juries, aged 13 to 18 years old with an average age of 14.5 years. They were 59.5% male. Recruitment took place through newsletters and emails to schools, and sessions were conducted at either participants' schools or the University. Participants were thanked with a £10 high street voucher, and a certificate of participation.

Design of Materials

The study was approved by the Ethics Review Board of the lead author's University Department. The key stimulus reported in this paper are "data cards" (see Figure 2). These cards were designed through several iterations of informal co-design activities with young people, and one round of piloting [16]. Researchers met with a group of approximately 5 young people, aged 16-18, over seven one-hour sessions. Although these represent the older end of the participant group, they had previously taken part in a Youth Jury, and often provided suggestions based on their interactions with younger participants, or their younger siblings and friends. In the first session, the researcher introduced the project and the workshop format, and the group members reviewed existing materials and the topics covered in the workshops. In each following session, one aspect of the workshops was targeted, and the young people produced suggestions for the activities which were refined by researchers between meetings then presented for feedback in the following meeting. The pilot study with a group of 13-17 year olds allowed examination of the use of the tools in practice, which led to further refinements by the group.

Procedure

A Youth Jury aims to provide participants a robust deliberation context to engage with a research topic through information receiving, exchange, critical examination and reflection. In this case, the study was divided into three phases: an introductory phase, a card activity phase, and finally, a scenario-led discussion phase.

The full procedure and all materials can be found in a freely available Online Educational Resource [59]. Each jury began with a brief preliminary questionnaire, which enabled the research team to learn more about children's existing knowledge of algorithms and the online world. This was followed by introductory activities (30 mins) including an introduction to the concept of algorithms. Participants did two brief collaborative paper-based tasks, one exploring the kinds of activities they did online and exploring the apps or websites they used. This naturally led to discussion of how these websites work, for example how they present content to them and the role of algorithms in this. A 'black box' (see Figure 1) was used as a visual metaphor to represent an algorithm collecting and processing data. The other task introduced to the idea of echo chambers and filter bubbles by asking participants to create their own filter bubbles based on the things they commonly see online, and comparing them to those seen by their peers. These activities were vital to enable the young people to start thinking about their own online activities and how they necessarily involve the use of algorithms.

Figure 1. The 'black box' representing an algorithm collecting data.

Two card-based activities (30 minutes) followed this. The objectives of the first activity were to learn more about participants' knowledge, awareness and opinions about data collection online. Participants were asked what kind of data they thought might be collected by the platforms they use online (for example Instagram, Facebook, and YouTube). A set of 45 laminated A6-sized "data cards", each with a different type of data printed on them (for example Sexuality, Hobbies, Current location, Relationship status, Age) (see Figure 2) were then presented face up on the table in front of them, and they were encouraged to comment on them, for example data they were surprised might be collected about them. The cards were co-created as a way to visualise the type and amount of data that might be collected, and to prompt discussion of the way this data might be used, including profiling and inferring other information.

The facilitator picked on a few examples and asked how jurors felt about them being collected, and jurors were encouraged to pick their own examples. They were also used to discuss how a particular data type may relate to others (for example, sharing location may lead to a service knowing your school or home address), and how combining data types may lead to forms of profiling (for example employer, last holiday, and education level may lead to certain assumptions about income). Facilitators were careful to remain neutral, reminding participants that there were no right or wrong answers, and that there were both positive and negative aspects to the use of personal data.

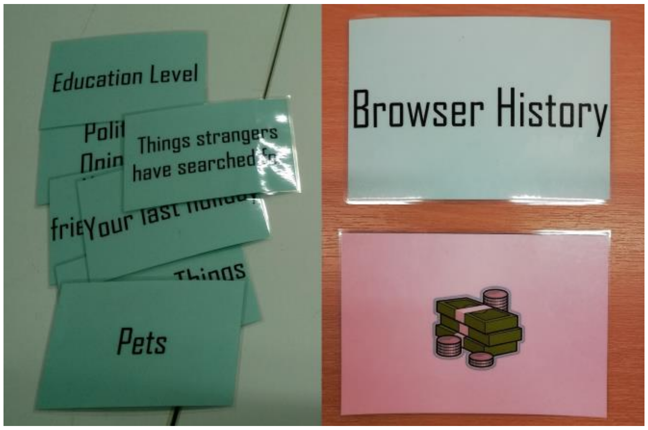

Figure 2. The two sets of cards: 'data cards' with plain backs (top right) and 'currency cards' with illustrated backs (bottom right).

The objective of the second card activity was to elicit participants' existing knowledge about the use of their data online in exchange for services, and their opinions towards this, as well as understanding whether different types of data had an effect on whether they wished to share this with online platforms. This activity used a second set of cards, identical to the first set but with an image of currency on the back (see Figure 2, bottom right). Depending on the number of participants, each juror was given a number of cards, with the data type facing up. They were asked how they thought the online platforms they used for free were able to make money. The backs of the cards were then revealed to the participants to show them how their personal data may become the 'currency' with which they paid for the online services. This useful exercise elicited discussion of the data market online and companies selling personal data to third parties. The participants were then asked to hold up the card (out of the set in front of them) which best answered the following questions:

1. Which type of data is most/least valuable to YOU?
2. Which type of data is most/least valuable to a COMPANY?

Their responses were then discussed as a group. At the end of these activities, the cards were placed into the black box, where they could no longer be seen, illustrating that an algorithm collects and processes data, but users' may be unaware of how this happens.

Following a break, participants were presented with one of two examples of algorithmically-mediated procedures leading to a bad outcome – either a school student being advertised an essay writing service and getting excluded, or a young child being shown inappropriate content on Netflix – and were asked to discuss who might be to blame and why (25 minutes). They then voted which party should be held responsible overall. Finally, the black box was used to facilitate a discussion on transparency, before they were asked for their suggestions for tackling any of the issues covered (20 minutes). This session allowed participants to reflect on what they had talked about in the rest of the workshop, and apply it to real world problems in order to come up with recommendations. A final questionnaire was completed after this to monitor any changes in attitude through the session.

All juries were audio recorded and transcribed using a University approved, GDPR compliant external company. Each transcript was thematically analysed using an inductive, data driven approach, meaning that the themes identified were strongly interrelated with the raw data [8]. A single researcher analysed and coded all the transcripts fully using NVivo software. Following this, three further researchers independently coded two random transcripts each. The research team then came together to discuss and compare their work to the coding of the original coder. The coding was validated collectively between the research team. Consistency was ensured amongst the codes from the four coders, with all minor discrepancies being discussed and resolved. The codes were then grouped into key themes.

RESULTS

The card activities were often the first time the participants had been asked to think about their interactions with the online platforms and companies themselves. The focus of any education they had previously had, tended to be around other online users: *"We had a huge assembly the other day on just, like, um, you should be happy online [...] And it never once mentioned about companies or anyone. They just said, uh, your account's private, only let your friends see it and everything. But they don't mention other things like that"* (YJ1). Often when asked about the types of data they put online, or the types of data a platform might collect about them, at first, young people were unable to come up with more than two or three examples. These were often things like name, gender, and location. The data cards provided extra examples that led to deeper consideration of potential issues. They also prompted the participants to come up with their own real life examples and think about their own experiences online. They were able to apply a particular data type to their own lives and consider the benefits and drawbacks of platforms having that information. They also had immediate (positive and negative) reactions to seeing many of the data types and were able to consider types of data that they would not have otherwise. These results predominantly focus on the negative responses the young people had, as these led to greater recommendations and reflections.

Recognition of the types of data that are collected

The participants were often surprised about the sheer amount of data that might be collected about them. There were also often comments on how *"in depth"* (YJ8) the data could be, with everything from relationship status to whether or not someone had tattoos. Others were not surprised at the types of data that are collected, with one pointing out that the Internet has a potentially unlimited capacity for collecting user information: *"...the internet is quite powerful, and like if there are cookies and stuff, it can pretty much see everything you are doing, so it can store it all and use it"* (YJ11). Whether or not they were surprised, there was quite a lot of concern from jurors in relation to the collection of their data: *"it's your private information. It's your life"* (YJ9), and the feeling that they would not have ownership and control over their own data.

The reasons why certain types of data may be collected was sometimes obvious, but others caused confusion and bafflement: *"Yes some of them make sense because like, because they want to know what your name is. They want to know what your email address is, but [...] there are some of them that don't make sense"* (YJ2). There was less concern about information that was necessary for a service, for example giving their home address when ordering goods; however, they strongly believed that this information should not be sold on to third parties. There was also some apathy surrounding why companies might want to collect so much data: *"Well you don't know why but, and just like in the grand scheme of things, you don't know why a lot of things happen but you're like, you don't question really, because it, it sounds bad but like it's not your job to know why"* (YJ4). Seeing the quantity of data that could potentially be collected helped some jurors to make further reflections on other concerns that they had in relation to their data, such as how their data was being stored, and whether it was indeed secure: *"But if these people know all these things I want to know how secure my data is"* (YJ5). If their data was not secured properly, they might face a personal danger where *"people can just go and come to your house"* (YJ9).

Perception and concerns of profiling

Discussion of the types of data available to companies led to consideration of how this data might be used to make inferences about users, which may then be used to profile them. For example, the 'Relationship status' data card was used to explain how Facebook was able to tell when a user was going to be in a relationship with another [3]. This led one participant to state that *it knows you before you even know yourself"* (YJ8). There was however, recognition that profiling of personal data can be used to *"make the service better"* (YJ3), and that there are benefits and drawbacks to how these services work: *"I mean, what music you listen to, I want them to collect that data, because they can recommend me better music. But then you can probably guess someone's personality from the music they listen to, so it's kind of like a double-edged sword"* (YJ8). Another juror pointed out that *"you've got to put this on the internet in the first place for them to know it, so if you put it on then you can't really be surprised if they use it"* (YJ9).

Particular concerns were expressed about the 'Current location' data card. This card was used as an example of how inferences might be built up about the users' day-to-day activities, even if they had not shared this information explicitly. For example, if they were in the same place every weekday between 8:30 and 3:15, where they go to school may be obvious. This provoked anxiety and concern from many, who found it *"disturbing"* and *"creepy"*. One participant remarked *"In a way you're being watched. [...] Like they know where you are like most of the time and you keep on doing it, like the same pattern so they're going to like know a little bit more and that's kind of going to be a little bit weird"* (YJ2). Concern about their movements being tracked was common across many youth juries. Other cards related to location, such as 'Who you are with', also prompted reaction: *"I'm worried about the who you're with one and how they'd find that out. [...] Because if they can find out who you're with then it's just... I don't know... It's just, it's just... It's creepy"* (YJ5).

Being able to physically pick up and combine cards to consider what might be learnt about them was very effective. The idea of small pieces of information adding up to an illustration of a users' day-to-day life, and how inferences may be made prompted a lot of discussion. This also often led to discussions about privacy, as one participant remarked that on some forms of social media *"you don't have any privacy on exactly everything you do. It's a bit strange"* (YJ5). Another explained that they felt that the companies using information to make inferences was *"a bit creepy. [...] They have information about you that you possibly don't even know about yourself"* (YJ7).

Some participants saw the dangers of profiling, pointing out that vulnerable groups such as migrants might be disadvantaged if they are profiled negatively which could be *"completely misleading"* (YJ6). Others were also concerned about inaccurate profiling as the algorithm could *"get some of them wrong"* (YJ7), or cause offence to the user or others. For example, one participant explained that 'clothes size' may cause offence if it then linked this to adverts for weight loss groups. Another suggestion of targeting shoppers based on inferences from their income, leading some to pay more than others for items online, was met with the response: *'you are taking advantage of people"* (YJ11). A third example of bias in profiling was provided by another juror: *"I went to a school that wasn't really good, and if employers were to know that I went to this school then they would probably look at me in a bad way"* (YJ1).

Views on sharing data

The cards helped participants to evaluate the kinds of data they would and would not wish to share with a company. Responses were very individualised. Data such as current location, criminal record, information relating to health and bank details were commonly data that they did not wish to share. One participant explained that they did not wish to share their previous internet searches because they should be *"private to yourself"* (YJ2). Home address was key to these discussions, as participants had significant concerns about their privacy and safety: *"I guess it could get to anyone really and then, um, they'd be able to know where you lived and everything"* (YJ1). Such discussions also elicited further conversations on how many of the participants felt, with words such as *"creepy"* and *"weird"* being used frequently to describe how they felt about this data being collected about them, often whether or not they had explicitly shared it themselves.

Many jurors felt that they were happy to share the data if it was not deemed too personal, such as their shoe size ("*like what, what are they going to do with that information, it doesn't affect me"* (YJ11)", or if it was information that might be established elsewhere anyway. If the consequences of a company holding and sharing the information was seen as inconsequential, participants also seemed unaffected.

The cards also helped to encourage participants to reflect further on who they were sharing their data with: *"To be honest all of this information I'm fine with someone having it and knowing what it all is, it just depends on who it is. I think that an issue that needs to be raised in parliament or whatever is we should have more knowledge or accessibility of knowing who's got the information and why they have it and if we can manage that"* (YJ5). However, when asked if it bothered the participants that a platform or piece of code had access to the information on the data cards, rather than an individual, a juror responded that they were unconcerned unless they used it *"to blackmail you"* (YJ11). This indicates that they were unable to consider dangers that extended beyond any personal, direct effects of data sharing between individuals. This type of response was common across juries.

Responses to companies selling their data

When participants were asked how companies make their money, it was common for the first reply from participants to be that they make their money through advertising: *"Every time somebody clicks on their website they get money from it"* (YJ2), *"Um, they'll probably be with advertisements mainly unless they're paid services"* (YJ3). The jurors were largely split between whether or not they knew that companies sold their data to third parties. Some were aware that the data was collected but not sold on to others: *"I mean, I knew that, um, they, kind of, gathered the information, but I didn't realise that they sold it to other companies"* (YJ11). The idea of their data being sold to other companies who might also use it to profile them was also discussed with concern: *"I'm just really baffled in all of this. Wow. I have no privacy"* (YJ8).

Amongst those who were not aware of data selling to third parties, it was not always a surprise: "*Because it's like if you sign up to a website or something and you give, if you put the information onto that website on the internet where it's easy access by anybody, then it's obviously, something is obviously going to happen to it"* (YJ2). However, others were surprised about the amount and depth of data that companies might be able to sell: *"Not to such an extent that, you know, they go into, um, lots of different details about your life"* (YJ8).

Seeing the currency on the cards allowed participants to contextualise and understand their own experiences. Particularly in response to the 'Phone number' card, jurors began to ask if the sharing of their data had led to nuisance and unwanted calls from third parties *"is that how like random company numbers get your, like, ring you like the 0800?"* (YJ3) and "*is it, just out of interest, you know I've got a phone number you know when you get random phone numbers from countries like Tunisia or whatever like that…"* (YJ5). Once again, this realisation led to participants feeling that this practice was *"a bit creepy."* (YJ3).

Seeing the type of data that companies could sell caused some concern about ownership: *"I don't think it's necessarily right for other companies, especially big companies, to make money off my own information. Um, yeah, I don't think that my details and stuff should circulate so that other people can make a profit off of it"* (YJ8). Others were more apathetic: *"it doesn't really bother me"* (YJ1)*;* *"you turn a blind eye to it"* (YJ4), especially if the information collected was *"not like super personal"* (YJ4). Some believed that their data was insignificant in the great scheme of things: *"who's really gonna be bothered about me? Like, really?"* (YJ5) whilst others felt that whilst they wouldn't wish this information to be sold to a person, *"some random, like, robot is not going to really matter if it has my information"* (YJ7).

Some participants recognised benefits of their data being sold, for example if companies weren't able to sell the data they held *"they won't get as much money so they probably won't be able to make the apps as good as they are"* (YJ5). This often related to information about preferences for example the 'What music you listen to' and 'Things you like on social media'. One juror also noted that they wouldn't want to stop companies from selling their data because *"it's just how the world is. Like there's some things you can't control, if that's how businesses need to make money, then they should be able to"* (YJ2).

Perceptions of the value of personal data

Responses about the value of personal data largely revolved around how personal the participant felt the data was to themselves. There was not always a consensus either within juries or across them. For example, in response to the 'Political Opinions' card during one jury, a participant explained that they would not mind if that was shared as *"I probably have the same political opinions as someone else so it's not me personally, like my school or income*" (YJ5). However, in other juries some participants discussed how they saw their political opinion *"as personal"* and that it might cause them to be *"labelled and identified a certain* *way"* (YJ6). Another participant in this jury also pointed out that political opinions might change over time, meaning that such labels could be damaging to users in the future.

Often jurors felt that the most valuable types of data to them were those that had the potential to be harmful to them personally if they got into the wrong hands. There was often talk of *"stalking"* due to someone getting hold of certain types of data, for example 'School' or 'Home address'. They were also very aware of types of data which already have added layers of protection around sharing such as 'Bank details', 'Criminal Record', and 'Health Information'. They also felt other highly person information such as 'Family members', 'Current Location' and 'Phone number' were highly valuable to them.

The data that participants felt were least valuable to them tended to include appearance-related information (including 'Piercings/Tattoos' and 'Clothes size', but also 'Gender', and 'Ethnicity'), information seen as irrelevant to them (for example 'What car you drive' because they didn't own a car), or information about others (for example 'Things that friends like on social media'). Other preferences that were considered by most to be innocuous were also considered less valuable, such as 'Favourite food', 'What Films/TV you watch', and 'What music you listen to'. Finally, things that were easy to discover online were also less valuable, for example 'Number of friends on social media'.

Some had very high awareness of the need for companies that provide a 'free' service to generate revenue. The cards enabled the jurors to consider why particular types of data might be considered as valuable to a company. The majority of juries highlighted data such as 'Things you like on social media', 'Favourite things', TV, music, and Films, internet searches and 'Browser History' as most valuable to companies. Often these coincided with data they felt were not as private and least valuable to them as individuals. The currency cards also enabled further discussion about profiling, and why companies might want to find out particular pieces of information. For example, one juror explained that companies might wish to know the relationship status of users so that they could recommend dating websites and cheap holidays for couples (YJ11). Many participants found it much harder to decide which data was least valuable to companies, as they could think of reasons that different platforms would use most of the data types. Responses to this final task were very mixed but included many of the types of data that they considered less personally valuable, for example 'Pets', 'Gender', 'Ethnicity', and 'Things strangers have searched for'.

DISCUSSION

Although children and young people make up a third of internet users, they are still often overlooked in discussions of how and why online platforms collect and use our personal data. This is perhaps due to the difficulty in engaging them with the topic, and also the difficulties often involved in incorporating young people into research in the first place. This paper reports the development and use of card-based activities which enable young people to critically consider the way their data is used online, including: the types of data an algorithm may collect from them, and the implications; the sharing and selling of their data to third parties; and the value of personal data. Our findings provide insights about young people's awareness of online personal privacy and the effectiveness of our probes, which indicate the critical need for raising their awareness through education and supporting their best interests with responsible design practices.

Young people's attitude towards online personal data privacy

The participants often reported actively trying to secure their personal data whilst online, by locking down their privacy settings and not sharing their location. However, many sites use "deceptive design" methods such as privacy default settings on online platforms that are described in terms of generally limiting unwanted access to user data, but which are designed to only protect the user from other people and are no defense against the company collecting their information [14]. When asked specifically about companies they often appeared quite apathetic, and failed to consider the issues, in agreement with [55]. The reasons for this fell into two main areas: many were not aware of having experienced any personally adverse effects, and therefore were unaware of what could happen; others felt that it was just a fact of using the internet, that everyone online has to put up with, relating to feelings of powerlessness, dejection, and resignation found in [18,55,66]. Both of these relate to the fact that for many, data-related privacy issues and implications were an unfamiliar topic for the Youth Juries. The card activities allowed them to visualise, contextualise and critically examine what was happening to their data, and to reflect on the impacts this may have on their lives, often causing them to react with shock and confusion. This highlights the data cards as being an effective tool to raise awareness of such data collection practices online as well as eliciting discussion, opinions and recommendations from participants themselves.

In particular the responses from the Youth Juries indicate that participants were often unaware of the magnitude of information that is collected about them when online. The visual impact of nearly 50 different types of data being spread out before participants often caused surprise and concern. The cards also encouraged critical thinking, something which it identified as lacking in current school curriculum [24]. At the beginning of activities responses often indicated that young people believed that it was not their place to be concerned about such issues, and they had no say in how platforms use algorithms to collect and process their data. However, the lively and thoughtful discussion prompted by the activities meant they often left with more desire to have an input into their online world, and to learn more about how issues may affect them. This increase in desire for digital education can have ongoing positive effects on the well-being of these young people [20].

Participants often found it difficult to relate the issues to actions of algorithms and platforms, rather than individuals and personal safety. For example, the quantity of data being stored by platforms concerned participants due to potential security issues such as hackers getting hold of their personal information and using it in the offline world. Such responses indicate that participants continue to think about the dangers of data sharing in terms of personal risks to themselves from individual human beings, as opposed to companies.

The young people were also often unable to visualise or consider dangers that extended beyond any personal, direct effects of data sharing to themselves. They were much more confident discussing issues from these angles, because they are a large part of digital literacy education. There have been calls in the media for better education with regards to data privacy for several years [53,67], and yet the provision of such education is still not adequate and such calls continue from a wide range of parties. Online safety education may warn users not to share information about themselves online publicly, but they are not made aware of the broader implications of a platform having this information.

Effectiveness of data cards as the probe

This study has demonstrated how the 'data cards' can effectively help young people to visualise and contextualise the role of data and algorithms in their online digital space. However, a key barrier is still in comprehending any risks that do not lead to direct personal harms. This is a critical gap in their knowledge. Although the use of `black box' helped the young people to visualise the opaqueness of data collection online, they need further support to establish an understanding how such data can then be used to manipulate the information presented and recommended to them, leading to the filter bubbles or isolated digital spaces.

Given the opportunity, young people do care about issues relating to the harnessing and use of their information online. They want to know what information is being taken from them, and why. They want companies to be more open about how data is being used. However, the current lack of education leaves young people ill-equipped to defend themselves against the companies who use their data, often without their knowledge, leading to questions about their ability to give informed consent to the use of their information. Even when they think about the actions of platforms, some feel they can't do anything about it, and that's 'just the way it is'. It is vital to empower the next generation to question the way the online world functions, and to speak up when they are not happy about something. This sentiment is critical given the dominance of a data-driven ecosystem in the online platforms, and strengthens the current call for a cultural shift of the responsibility from the user to the companies collecting our data.

Some initiatives now include guidelines for topics such as 'Privacy and security' online [63], and highlighting the importance of enabling young people to find out what is happening to their data online [15]. It is not adequate for such education to be included in optional computing qualifications, such as the Computer Science GCSE, not least because uptake in such subjects is slipping (particularly among females) since the more broad ICT qualifications were scrapped [58]. Inclusion in Personal, Social, and Health Education schemes would be ideal [61], but despite policy makers often citing them as effective means for developing media and digital literacy [25], these courses are also often not compulsory, leaving the education of large numbers of young people lacking in this area.

Education should take the form of meaningful activities appropriate to different age ranges, accessed in schools and also attended to by online providers. More education about these issues should occur at the point of use, on the platforms that young people use every day, to help them to make informed decisions about their online lives. The following section considers this and other considerations for the future design of online technology.

Implications for the design of online technology

It is clear given the key findings of this paper, that the current design of online platforms does not adequately put children's best interests first, or arm young people with the knowledge to understand and make informed decisions surrounding the use of their personal data. In particular, participants' reactions indicate an asymmetry between young people and platforms in the comprehension of *how* their data are processed and used: such as the commerciality of their data and the pervasiveness of algorithms. Such issues are exactly what the Information Commissioner's Office in the UK aims to address by publishing the ground-breaking Age Appropriate Design Code [26].

The core of the code aims to enforce data minimisation, demanding online service providers that are likely to be used by anyone under the age of 18 to collect only data that is necessary. Although the tech industry is concerned that such practices may encumber innovation, protecting children's best interests is both a legal and moral obligation. Furthermore, by increasing the transparency of data collection and use practices, the industry will be better positioned to create value from data that is higher quality and more reliable, as well as potentially increase user trust and confidence.

The key in this process is working alongside children and young people. In this way, platforms and designers could collect evidence through direct interaction with this group, to make specific decisions surrounding how such visibility of data collection and associated procedures be incorporated into the design of their spaces. Such co-creation and user generated work is crucial as it is important that any design alterations are both contextual and generic, and meaningful and understandable to these users.

The new ICO code emphasises transparency and age-appropriate design. This is exactly aligned with the young people's demand to know more about what data is used, why, and how they may gain control of it. Such transparency must be provided with care, to avoid any misunderstandings or even perpetuating existing issues that undermine user perceptions of what happens to their personal data. For example, it would be important for any explanatory language used to be accessible to this age-group to be positioned appropriately in a particular digital space. Interactive workshops based on the 'Youth Jury' with data or ideation cards, or other user-centred mechanisms provide a means through which this may be accomplished. It is important that issues are understood from the perspectives of young people themselves rather than assumed, and generalisations made across different age groups.

It is important to acknowledge, and unfortunately so, that it may be complex or infeasible to encourage design changes directly to digital spaces given various tensions that exist: such as that between commercialisation and transparency. Thus awareness-raising and educational mechanisms such as those identified in the prior section go hand-in-hand with recommendations for design. Platforms should consider how they can incorporate educational mechanisms within the design of their spaces. Education and awareness are fundamental so that young people have an appropriate foundational understanding of issues to be able to make informed decisions about their navigation in these spaces; and also, be active participants in discussion surrounding problematic issues in relation to the use of their personal data.

The (re)design of online spaces to address the concerns of young people is a complex and multi-dimensional task. The new ICO code provides a strong framework for designers to gauge data privacy risks for children and young people, and explore new approaches to support specific challenges. This study has demonstrated that this new child-specific regulation is a necessity. Despite the associated difficulties with engaging young people in user-studies, this is an extremely important area that should be addressed with some urgency.

Limitations

It is important to note the limitations of this study. The amount and types of data that were presented to participants was by no means exhaustive, as they were designed to promote discussion amongst the group. During the data-as-currency activity, each participant was dealt a limited number of cards (normally three each) and so was responding to the questions about data valuation on a very limited set. The answers therefore will not have been representative of the participant's feelings more generally across the whole 'dataset', but of their feelings in relation to very particular examples. However, certain cards did get chosen more, no matter what combination of other cards they appeared with.

Moreover, whilst the cards proved highly beneficial in promoting discussion and critical thinking, they perhaps did not go far enough in ensuring that the young people were focused on the effects of algorithms or the platforms using them. Although improvements in the broader education of young people will help with deepening their knowledge of these issues, the contributions stemming from the existing activities would be strengthened if considered as part of a suite of activities and interactions aimed at increasing understanding, as previously recommended.

Finally, as discussions were left open and participants were encouraged to talk to each other rather than facilitators, it was often unclear exactly what some participants meant to when referring to 'the internet' or 'companies'. Although they were clear about their opinions in terms of, for example, that these entities should not sell their data to others, it would be interesting to investigate further perceptions of who exactly these entities are. Are they singular corporations like Facebook? A system like a government? When 'the internet' collects their information, who do they mean?

CONCLUSIONS

This paper presents an analysis of a rich corpus of material, collected through a series of Youth Juries attended by 13-18 years old. Specifically, findings from the use of a co-designed activity using 'data cards' are reported, which were designed to elicit discussion around the types of data which may be collected online and how it might be used, and the sharing and selling of data. The engagement elements of the Youth Juries, including the co-design and co-production of educational materials, bring young people to the forefront of the debate, and help to overcome some of the challenges of working with this age group. Understanding their online experiences will provide substantial evidence to ensure that the design of future digital services and products is appropriate for children and young people.

The results highlight that young people are about the potential consequences of online platforms collecting and using their personal data, and they desire to know and understand how this affects their online lives. All young people should be able to question the way the online world functions, including issues of data harvesting, profiling, and third party data sharing. This study marked the first time that many of the young people were asked their opinions on such matters. Co-created activities such as those in this research are engaging and effective ways to approach this.

This work highlights the need for not only the careful design of technologies that are respectful to the rights and needs of young people, especially surrounding transparency in the use of their data, but also age appropriate education about these issues.

ACKNOWLEDGMENTS

This work formed part of the EPSRC funded UnBias project (grant number EP/N02785X) based at the Horizon Digital Economy Research Institute, University of Nottingham. It was also supported by the EPSRC funded ReEnTrust project (grant number EP/R033633/1) based at the University of Oxford. Elvira Perez Vallejos also acknowledges the financial support of the NIHR Nottingham Biomedical Research Centre.

SELECTION AND PARTICIPATION OF CHILDREN

Children who participated in this research were recruited via their schools, and the sessions were conducted at either the participants' schools or the University. For all participants under 16, parental or guardian consent was obtained, as well as the consent of the child. Consent forms, information sheets, and privacy notices were sent to parents and children prior to the work being carried out, and children's consent was attained prior to the start of each workshop. The research was cleared by the University Ethics Committee of the first author, which includes commitment to adhere to Data Protection legislation. A teacher was present at all times and all researchers were DBS checked.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and Human Behavior in the Age of Information. *Science* 347, 6221 (January 2015), 509–514. DOI:https://doi.org/10.1126/science.aaa1465

[2] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *SOUPS'13 Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM Press, Newcastle, United Kingdom, Article No. 12. DOI:https://doi.org/10.1145/2501604.2501616

[3] Aral Balkan. 2014. Free is a Lie. RSA House, London. Retrieved September 7, 2018 from https://www.thersa.org/discover/videos/event-videos/2014/04/free-is-a-lie

[4] David Barnard-Wills and Debi Ashenden. 2015. Playing with Privacy: Games for Education and Communication in the Politics of Online Privacy. *Political Studies* 63, 1 (March 2015), 142–160. DOI:https://doi.org/10.1111/1467-9248.12049

[5] Tilde Bekker and Alissa N Antle. 2011. Developmentally Situated Design (DSD): Making Theoretical Knowledge Accessible to Designers of Children's Technology. In *CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Vancouver, BC, Canada, 2531–2540.

[6] Igor Bilogrevic and Martin Ortlieb. 2016. "If You Put All the Pieces Together...": Attitudes Towards Data Combination and Sharing Across Services and Companies. In *CHI '16 Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, San Jose, California, USA, 5215–5227. DOI:https://doi.org/10.1145/2858036.2858432

[7] Reuben Binns, Jun Zhao, Max Van Kleek, Nigel Shadbolt, Ilaria Liccardi, and Daniel Weitzner. 2017. My Bank Already Gets this Data: Exposure Minimisation and Company Relationships in Privacy Decision-Making. In *CHI EA '17 Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ACM, Denver, Colorado, USA, 2403–2409. DOI:https://doi.org/10.1145/3027063.3053255

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (January 2006), 77–101. DOI:https://doi.org/10.1191/1478088706qp063oa

[9] Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. 2013. Your Browsing Behavior for a Big Mac: Economics of Personal Information Online. In *WWW '13 Proceedings of the 22nd international conference on World Wide Web Pages 189-200*, ACM, Rio de Janeiro, Brazil, 189–200. Retrieved September 3, 2018 from http://arxiv.org/abs/1112.6098

[10] Brendan Cassidy, Dipti Saurabh Antani, and Janet C C. Read. 2013. Using an open card sort with children to categorize games in a mobile phone application store. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, ACM Press, Paris, France, 2287. DOI:https://doi.org/10.1145/2470654.2481315

[11] Children's Commissioner for England. 2017. *Life in "Likes": Children's Commissioner Report into Social Media Use Among 8-12 Year Olds*.

[12] Children's Commissioner for England. 2017. *Growing Up Digital: A Report of the Growing Up Digital Taskforce*.

[13] Stephen Coleman, Kruakae Pothong, Elvira Perez Vallejos, and Ansgar Koene. 2017. *The Internet on Our Own Terms: How Children and Young People Deliberated About Their Digital Rights*.

[14] Commission Nationale de l'Informatique et des Libertés. 2019. *Shaping Choices in the Digital World. From dark patterns to data protection: the influence of ux/ui design on user empowerment*. Retrieved January 23, 2020 from https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf

[15] Department for Digital, Culture, Media and Sport and The Rt Hon Matt Hancock MP. 2017. Children to be Given Extra Protection Online. *Gov.uk*. Retrieved September 13, 2018 from https://www.gov.uk/government/news/children-to-be-given-extra-protection-online

[16] Liz Dowthwaite, Helen Creswick, Virginia Portillo, Monica Cano, Elvira Perez Vallejos, Ansgar Koene, and Menisha Patel. 2018. Work-in-Progress: UnBias Youth Juries. In *#SMSociety18 Proceedings of the 9th International Conference on Social Media & Society*, ACM, Copenhagen, Denmark, 276–280. DOI:https://doi.org/10.1145/3217804.3217928

[17] Allison Druin. 2002. The Role of Children in the Design of New Technology. *Behaviour & Information*

Technology 21, 1 (2002), 1–25. DOI:https://doi.org/10.1080/01449290110108659

[18] Casey Fiesler and Blake Hallinan. 2018. “We Are the Product”: Public Reactions to Online Data Sharing and Privacy Controversies in the Media. In *CHI ’18 Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, Montreal QC, Canada, Paper No. 53. DOI:https://doi.org/10.1145/3173574.3173627

[19] Batya Friedman and David Hendry. 2012. The Envisioning Cards: a Toolkit for Catalyzing Humanistic and Technical Imaginations. In *CHI ’12 Proceedings of the SIGCHI Conference on Human Factors in Computing System*, ACM, Austin, Texas, USA, 1145–1148. DOI:https://doi.org/10.1145/2207676.2208562

[20] Jenna K. Gillett-Swan and Jonathon Sargeant. 2018. Voice Inclusive Practice, Digital Literacy and Children’s Participatory Rights. *Children & Society* 32, 1 (2018), 38–49. DOI:https://doi.org/10.1111/chso.12230

[21] Michael Golembewski and Mark Selby. 2010. Ideation Decks: a Card-Based Design Ideation Tool. In *DIS ’10 Proceedings of the 8th ACM Conference on Designing Interactive Systems*, ACM, Aarhus, Denmark, 89–92. DOI:https://doi.org/10.1145/1858171.1858189

[22] José González Cabañas, Ángel Cuevas, and Rubén Cuevas. 2017. FDVT: Data Valuation Tool for Facebook Users. In *CHI ’17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, Denver, Colorado, USA, 3799–3809. DOI:https://doi.org/10.1145/3025453.3025903

[23] Horizon Digital Economy Research Institute, UnBias, and CaSMa. 2018. *Response to Information Commissioner’s Office “Age Appropriate Design Code” consultation*.

[24] House of Lords Select Committee on Communications. 2017. *Growing up with the internet. 2nd Report of Seesion 2016-2017*. Retrieved January 23, 2020 from https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm

[25] Jeremy Hunt. 2011. Letter to Sonia Livingstone. Retrieved September 19, 2018 from https://www.scribd.com/document/54695321/Hunt-Letter-to-Livingstone-Media-Literacy

[26] Information Commisioner’s Office. 2020. *Age appropriate design: a code of practice for online services*. Retrieved January 23, 2020 from https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

[27] Baroness Kidron, Alexandra Evans, and Jenny Afia. 2018. *Disrupted Childhood: The Cost of Persuasive Design*. 5Rights Foundation.

[28] Beeban Kidron and Angharad Rudkin. 2017. *Digital Childhood: Addressing childhood development milestones in the digital environment*. 5Rights Foundation.

[29] Ansgar Koene. 2017. Algorithmic Decision-Making: Fairness, Bias and the Role of Ethics Standards. In *European Big Data Value Forum*. Versailles, France.

[30] Ansgar Koene. 2017. *Response to Commons Culture, Media and Sport Committee “Fake News” inquiry*.

[31] Ansgar Koene, Elvira Perez Vallejos, Helena Webb, and Menisha Patel. 2017. Human Agency on Algorithmic Systems. In *AoIR2017 Association of Internet Researchers Conference*, AoIR, Tartu, Estonia.

[32] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. “No Telling Passcodes Out Because They’re Private”: Understanding Children’s Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (November 2017), Article No. 64. DOI:https://doi.org/10.1145/3134699

[33] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *IDC ’18 Proceedings of the 17th ACM Conference on Interaction Design and Children*, ACM, Trondheim, Norway, 67–79. DOI:https://doi.org/10.1145/3202185.3202735

[34] Gry Hasselbalch Lapenta and Rikke Frank Jørgensen. 2015. Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday* 20, 3 (March 2015). Retrieved September 4, 2018 from http://firstmonday.org/ojs/index.php/fm/article/view/5568

[35] Linda Naeun Lee, Richard Chow, and Al M. Rashid. 2017. User Attitudes Towards Browsing Data Collection. In *CHI EA ’17 Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ACM, Denver, Colorado, USA, 1816–1823. DOI:https://doi.org/10.1145/3027063.3053078

[36] Pedro Giovanni Leon, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. 2015. Privacy and Behavioral Advertising: Towards Meeting Users’ Preferences. In *SOUPS’15 Proceedings of the Eleventth Symposium on Usable Privacy and Security*, ACM, Ottowa, Canada, 1–15.

[37] Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. 2013. What matters to users?: factors that affect users’ willingness to share information with online advertisers. In *SOUPS ’13 Proceedings of the Ninth Symposium on Usable Privacy and Security*, ACM, Newcastle, United Kingdom, Article No. 7. DOI:https://doi.org/10.1145/2501604.2501611

[38] Ilaria Liccardi, Alfie Abdul-Rahman, and Min Chen. 2016. I Know Where You Live: Inferring Details of

People's Lives by Visualizing Publicly Shared Location Data. In *CHI '16 Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ACM, San Jose, California, USA, 1–12. DOI:https://doi.org/10.1145/2858036.2858272

[39] Sonia Livingstone, John Carr, and Jasmina Byrne. 2015. *One in Three: Internet Governance and Children's Rights*. Global Commission on Internet Governance. Retrieved from https://www.cigionline.org/sites/default/files/no22_2.pdf

[40] Ewa Luger, Lachlan Urquhart, Tom Rodden, and Michael Golembewski. 2015. Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process. In *CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM, Seoul, Republic of Korea, 457–466. DOI:https://doi.org/10.1145/2702123.2702142

[41] Miguel Malheiros, Sören Preibusch, and M. Angela Sasse. 2013. "Fairly Truthful": The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. In *Trust and Trustworthy Computing: 6th International Conference, TRUST 2013, London, UK, June 17-19, 2013. Proceedings*, Michael Huth, N. Asokan, Srdjan Čapkun, Ivan Flechais and Lizzie Coles-Kemp (eds.). Springer Berlin Heidelberg, 250–266.

[42] Helia Marreiros, Richard Gomer, Michael Vlassopoulos, Mirco Tonin, and MC Schraefel. 2015. Scared or naïve? An exploratory study on users perceptions of online privacy disclosures. *IADIS International Journal on WWW/Internet* 13, 2 (2015), 1–16.

[43] Derek McAuley, Ansgar Koene, Elvira Perez Vallejos, Virginia Portillo, Helen Creswick, Liz Dowthwaite, and Monica Cano. 2018. *Response to Commons Science and Technology Committee "Impact of social media and screen-use on young people's health inquiry" inquiry*.

[44] Roisin McNaney, John Vines, Jamie Mercer, Leon Mexter, Daniel Welsh, and Tony Young. 2017. DemYouth: Co-Designing and Enacting Tools to Support Young People's Engagement with People with Dementia. In *CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, Denver, Colorado, USA, 1313–1325. DOI:https://doi.org/10.1145/3025453.3025558

[45] Kathryn C. Montgomery, Jeff Chester, and Tijana Milosevic. 2017. Children's Privacy in the Big Data Era: Research Opportunities. *Pediatrics* 140, Supplement 2 (November 2017), S117–S121. DOI:https://doi.org/10.1542/peds.2016-1758O

[46] Simone Mora, Francesco Gianni, and Monica Divitini. 2017. Tiles: A Card-based Ideation Toolkit for the Internet of Things. In *Proceedings of the 2017 Conference on Designing Interactive Systems - DIS '17*, ACM Press, Edinburgh, United Kingdom, 587–598. DOI:https://doi.org/10.1145/3064663.3064699

[47] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs* 41, 1 (June 2007), 100–126. DOI:https://doi.org/10.1111/j.1745-6606.2006.00070.x

[48] Ofcom. 2017. *Children and Parents: Media Use and Attitudes Report*.

[49] Luci Pangrazio and Neil Selwyn. 2017. "My Data, My Bad ...": Young People's Personal Data Understandings and (Counter)Practices. In *#SMSociety17 Proceedings of the 8th International Conference on Social Media & Society*, ACM, Toronto, ON, Canada, Article No. 52. DOI:https://doi.org/10.1145/3097286.3097338

[50] Elvira Perez Vallejos, Ansgar Koene, Chris James Carter, Ramona Statache, Tom Rodden, Derek McAuley, Monica Cano, Svenja Adolphs, Claire O'Malley, Kruakae Pothong, and Stephen Coleman. 2015. Juries: acting out digital dilemmas to promote digital reflections. *ACM SIGCAS Computers and Society - Special Issue on Ethicomp* 45, 3 (September 2015), 84–90.

[51] Elvira Perez Vallejos, Ansgar Koene, Virginia Portillo, Liz Dowthwaite, and Monica Cano. 2017. Young People's Policy Recommendations on Algorithm Fairness. In *WebSci '17 Proceedings of the 2017 ACM on Web Science Conference*, ACM, Troy, New York, USA, 247–251.

[52] Virginia Portillo, Elvira Perez Vallejos, Monica Cano, Liz Dowthwaite, and Ansgar Koene. 2017. Algorithmic Taste Management: Young People's Perspectives and Recommendations. ECREA, Stockholm, Sweden.

[53] ResourcEd. 2017. Digital Literacy in the Classroom. How Important Is It? *ResourcEd*. Retrieved September 18, 2018 from https://resourced.prometheanworld.com/digital-literacy-classroom-important/

[54] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy Tipping Points in Smartphones Privacy Preferences. In *CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ACM Press, Seoul, Republic of Korea, 807–816. DOI:https://doi.org/10.1145/2702123.2702404

[55] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *CHI '14 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Toronto, Ontario, Canada, 2347–2356. DOI:https://doi.org/10.1145/2556288.2557421

[56] Cristiana S. Silva, Glívia A.R. Barbosa, Ismael S. Silva, Tatiane S. Silva, Fernando Mourão, and Flávio Coutinho. 2017. Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case

Study on Facebook. In *WebSci '17 Proceedings of the 2017 ACM on Web Science Conference*, ACM, Troy, New York, USA, 63–71. DOI:https://doi.org/10.1145/3091478.3091479

[57] Stephanie Solomon and Julia Abelson. 2012. Why and when should we use public deliberation. *Hasting Centre Report* 42, 2 (2012), 17–20.

[58] Jess Staufenberg. 2018. The New Computer Science GCSE is Already Being Reviewed. *Schools Week*. Retrieved September 19, 2018 from https://schoolsweek.co.uk/low-uptake-for-computer-science-gcse-spurs-review/

[59] The UnBias Team. UnBias Youth Juries: An Online Educational Resource. Retrieved April 17, 2020 from https://uyj.wp.horizon.ac.uk/

[60] Zeynep Tufekci. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society* 28, 1 (February 2008), 20–36. DOI:https://doi.org/10.1177/0270467607311484

[61] June Eric Udorie. 2015. Social Media is Harming the Mental Health of Teenagers. The State has to Act. *The Guardian*. Retrieved September 19, 2018 from https://www.theguardian.com/commentisfree/2015/sep/16/social-media-mental-health-teenagers-government-pshe-lessons

[62] UK Council for Child Internet Safety. 2015. *Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services*.

[63] UK Council for Child Internet Safety. 2018. *Education for a Connected World: A Framework to Equip Children and Young People for Digital Life*.

[64] unicef. 2010. A Summary of the UN Convention on the Rights of the Child.

[65] Sonja Utz and Nicole C. Krämer. 2009. The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3, 2 (2009), Article 2.

[66] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, and Nigel Shadbolt. 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In *CHI '17 Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ACM, Denver, Colorado, USA, 5208–5220. DOI:https://doi.org/10.1145/3025453.3025556

[67] Which? Team. 2011. ICO wants UK Schools to Teach Data Privacy. *Which? News*. Retrieved September 18, 2018 from https://www.which.co.uk/news/2011/08/ico-wants-uk-schools-to-teach-data-privacy-264587/

[68] Heng Xu, Xin (Robert) Luo, John M. Carroll, and Mary Beth Rosson. 2011. The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing. *Decision Support Systems* 51, 1 (2011), 42–52. DOI:https://doi.org/10.1016/j.dss.2010.11.017

[69] Sarita Yardi and Amy Bruckman. 2011. Social and Technical Challenges in Parenting Teens' Social Media Use. In *CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Vancouver, BC, Canada, 3237–3246. DOI:https://doi.org/10.1145/1978942.1979422

[70] Leah Zhang-Kennedy, Christine Mekhail, Yomna Abdelaziz, and Sonia Chiasson. 2016. From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats. In *IDC '16 Proceedings of the The 15th International Conference on Interaction Design and Children*, ACM, Manchester, United Kingdom, 388–399. DOI:https://doi.org/10.1145/2930674.2930716