Children Designing Privacy Warnings: Informing a Set of Design Guidelines

John Dempsey*, Gavin Sim*, Brendan Cassidy*, Vinh-Thong Ta**

* ChiCI Group, University of Central Lancashire, Preston, PR1 2HE, UK.

** Department of Computer Science, Edge Hill University, Ormskirk, UK.

Abstract

Children are increasingly interacting with digital technology and there are concerns relating to their online safety. Warning signs and messages have been integrated within technology in attempt to address safety concerns, however they often use metaphors and icons that may not always be comprehended by children. This paper reports on a study with 141 UK-based school children, aged between 7 and 13 years old who were asked to design warning messages related to the disclosure of private information online. Children were asked to draw warning messages for other children utilising personas and privacy risk scenarios, which were then analysed using content analysis to identify common characteristics. This paper contributes to the protection of children's online privacy by identifying a set of guidelines that can be used when designing warning messages aimed at children disclosing data within an online setting.

1. Introduction

The child computer interaction (CCI) community has sought to improve experiences of children using a range of technology in different contexts including education (Wen, Lin, Chen, & Andersen, 2019), gaming (Read, et al., 2018, Sim and Cassidy, 2013) and communication (Fitton, Read, Sim, & Cassidy, 2018). Recently, the community has also included areas such as parental concerns and education (Assal et al., 2018, Bell, 2019, Nouwen and Zaman, 2018). Online safety will become more prominent now that the UN have adopted the General Comment 25 on Children's rights in relation to the digital environment. This will afford children the same rights in the physical and digital world with respect to privacy and protection. Governments will be accountable and thus new legislation may be required. For example, the UK had previously acknowledged aspects of this General Comment through the UK's "Digital Charter". This raised concerns about the power relationship between technology companies and citizens, and data protection legislation has been passed which identifies children as a vulnerable group that needs further protections (European Parliament and Council of European Union, 2018). As children are increasingly using technology in their daily lives to interact with people including peers and family, strategies must be developed to help children manage the risks they will face when using the Internet (Lobe et al., 2020, Smahel, et al., 2020).

Governments have focused on the "commercial-literacy" of children, and how businesses can take actions to protect children. However, "interpersonal-literacy" is also of major concern because children may tell other individuals personal and private things about

themselves (Livingstone, 2018). This has been the focus of research within CCI, educating children on aspects such as passwords (Read and Beale, 2009, Read and Cassidy, 2012) and online privacy (Dowthwaite, et al., 2020, Zhang-Kennedy, Abdelaziz, and Chiasson, 2017). This area has also been supported by government schemes including the UK Council for Internet Safety who released an educational framework that aims to help children enjoy the Internet safely, which includes helping children understand the risks associated with interpersonal communications (Safety U.K. Council for Child Internet, 2020). This framework identifies privacy and security as a key theme that should be taught to children to help keep them safer while online. Despite these interventions there is still strong evidence that children are being put at risk whilst interacting online (Office for National Statistics, 2020).

Children may be put in danger by the lack of controls offered when they share private data with others, especially on the Internet. The range of dangers and risks faced by children in today's connected world are broad and complex, ranging from stranger danger, sexual communications, cyber-bullying, and the routine collection of personal data stored for future use. In the UK around 18% of 8-to-11 year olds reported seeing online content they considered worrying or nasty (Bentley, et al., 2020), while the NSPCC estimate that 1 in 20 children have been sexually abused, with rising Internet use as one of the drivers for such high numbers (Suarez, 2019). The Office for National Statistics suggest that almost 1 in 20 children have experienced online bullying behaviour within the last 12 months (Office for National Statistics, 2020). UNICEF have issued a warning to governments worldwide after seeing the worrying trends worsen due to COVID-19 (UNICEF, et al., 2020).

The COVID-19 pandemic, subsequent lockdowns, self-isolation periods, and school closures have sent children to the Internet as their primary means of communicating with their friends. It has become common for children to communicate with others using a range of social networking sites, playing online computer games, using home-schooling programs software such as Seesaw and other online applications (Lobe et al., 2020, Ofcom, 2021). By publishing their private data through these communication tools, they are building a larger online digital footprint than ever before Children's Commissioner (2018). Young children are developing their understanding of the world, and may not have the digital literacy to identify the risks and appreciate the consequences of the harms linked to publishing personal data (Children's Commissioner, 2017, Information Commissioners Office, 2018). Helping children to manage this digital footprint will empower them to better manage online risks and ultimately stay safer (HM Government, 2017).

One solution to these privacy concerns is to help children with their privacy-literacy; to help them understand what public and private information is, and to help them understand the risks they may be exposed to when publishing information within different settings. A purely protectionist viewpoint may be to educate all children not to publish any information online, this could interfere with the freedoms that the Internet provides, preventing children from making friends or using online services that enable their personal growth. Developing privacy-literacy in children should help them to make their own decisions, potentially under adult-supervision, about what data they could publish. In addition to the work already published on improving children's privacy literacy (Knijnenburg and Cherry, 2016, Zhang-Kennedy, Baig, and Chiasson, 2017) one area that is yet to be explored is the potential to use a set of info graphics or warning symbols that could be used to intervene whenever a child interacts or publishes personal data.

The use of warning symbols and their design can be a challenge and Boto, Noriega, and Duarte (2015) suggests that no assumptions should be made when it comes to warnings and children; the pictorials used in common, well-known warning symbols could mean very different things to children and adults. For example, some children have recognised the skull and bones used to indicate poison, as "pirate food" (Boto et al., 2015). Using child-centered child-centred research methods could help alleviate this lack of comprehension, by asking children to design the characteristics of good privacy-related warning messages, to help organisations design meaningful warning signs or symbols to convey those online risks (Read, 2005).

Children have demonstrated their ability to design for others in a range of contexts (Read et al., 2009, Sim et al., 2015); the purpose of this study was to understand how children would warn other children about the consequences of disclosing private information in an online setting. This complements existing research that has focused on the educational aspects of online safety with children (Hartikainen, Iivari, & Kinnula, 2019). Researchers have developed guidelines for a wide range of interactive technologies for children, including apps for children with autism (Sofian, Hashim, & Ahmad, 2018), educational apps (Mak & Nathan-Roberts, 2017) and games (Straker, Abbott, Collins, & Campbell, 2014). Design guidelines can then be used to improve the systems for the target user, in this instance children. Therefore the assumption would be that a set of design guidelines for infographics relating to online safety will ultimately help children to make informed decisions about the management of their digital footprint, and in the process avoiding any adult-based assumptions (Boto et al., 2015).

The contribution of this paper to the CCI community is a set of design guidelines that have been informed by children. These guidelines can be utilised by designers responsible for creating applications that allow children to disclose information to others. As society grows more aware of the dangers posed by disclosing information to others, it becomes an ethical and moral responsibility to help children make informed decisions about what data or information they disclose and to whom they disclose it, while helping them understand the potential consequences of those disclosures.

2. Background and related work

2.1. Online safety

Building safe and secure systems for children is more complicated than simply placing children at the centre of any design and development task (Dempsey, Cassidy, & Sim, 2016). Online safety is mediated by parents, carers, teachers, industry and policy makers who all have a role to play in keeping children safe (Hartikainen, Iivari, & Kinnula, 2015). However, even the mediation space can pose challenges due to different perceptions and objectives with respect to children's online safety. Industry and policy makers may be taking a more holistic and societal view governed by adhering to legislation, while other stakeholders may be concerned with threats or risks to an individual child.

During their review of adolescent online safety, Pinter et al. observed that much of the child online safety and risk work had yet to change the status quo (Pinter, Wisniewski, Xu, Rosson, & Carroll, 2017), yet there have been plenty of attempts to improve different types of online safety such as stranger-danger (Badillo-Urquiola, et al., 2019), cyber-bullying (Hartikainen et

al., 2019), recognising phishing attempts (Lastdrager, Gallardo, Junger, & Hartel, 2017), and teaching children about privacy concepts (Knijnenburg and Cherry, 2016, Zhang-Kennedy, Abdelaziz, and Chiasson, 2017, Zhang-Kennedy and Chiasson, 2016). These studies had varying levels of success and online safety is still a major concern for all stakeholders.

Children do not always associate stranger-danger as an online risk and instead may associate online risks with cyber-bullying or other unwanted attention instead (Badillo-Urquiola, et al., 2019). During their cooperative inquiry session with 14 children from the University of Maryland's KidsTeam program, programme, aged between 8 years and 11 years old, Badillo-Urquiola, et al. (2019) identified that children desired different levels of agency; they wanted mediation/help when it came to dealing with stranger-danger, however, they also wanted enough personal agency to be able to cope with taking decisions and actions. While they recognised that the stranger-danger scenarios where probably not serious enough to call emergency services, they may not have the skills necessary to deal with the situation without some form of help. As an alternative to parental/mediator support, children suggested they would prefer an automated intelligent assistant detect risky content and tell them when the situation was "bad" or "dangerous". Therefore, some technology mediated intervention or assistance may be preferable for assisting children understanding online risks.

There has been considerable work looking at how to protect users, including children, from phishing emails through measures including automated detection (Bergholz, Paaz, Reichartz, Strobel, & Chang, 2008) and training interventions (Lastdrager et al., 2017). These measures are vital as children have demonstrated poor judgement in identifying phishing emails (Nicholson, et al., 2020) with recommendations made to have better training for children within schools. However, there is concern over the long-term effectiveness of training children with regards to Phishing as the learning appears to be momentary and diminishes over time. Lastdrager et al. (2017) provided cyber-security training to children that focused on the ability to detect phishing emails, and then tested the children's ability to detect legitimate or phishing emails both immediately and over different lengths of time. The children made an immediate improvement with their ability to identify phishing emails, and over time children improved their ability to identify legitimate emails but did not continue to improve identifying phishing emails. In other research looking at the retention of phishing knowledge (Kim, Lee, & Kim, 2020), it was inferred that the retention period for anti-phishing training is less than three months based on their experimental work, which demonstrated phishing deception decreased almost immediately after training, but returned to the pre-training rate after three months. Therefore, interventions or training may need to be repeated to be effective over time.

It is well documented that children engage with games within an educational context (Vitak, et al., 2018), and while not evaluated with children Chen et al. (Wen et al., 2019) developed an educational game combining role playing and interactive content to teach people about phishing and the potential consequences. The results showed that the adult participants could identify phishing emails effectively after the training but there is no evidence of whether this behaviour is sustained over time. Sun, Kuo, Hou, and Lin (2017) developed a game and evaluated it with 110 elementary school children demonstrating increased knowledge of phishing could be inculcated by a trial and error approach via repeated use. There may be potential to use educational games to help children identify phishing emails and comprehend the risks. Clearly, education plays an important role with helping children to combat the challenges of online safety, yet it is also important that facilities are provided enabling children to develop skills even after the training.

While training/education is clearly part of the solution, there is also evidence to suggest that children would prefer the ability to mediate their own online interactions, perhaps with the help of an automated intelligent assistant (Badillo-Urquiola, et al., 2019). While not focused on children, there is also evidence to suggest that a "paternalistic nudge" can help move users towards taking safer decisions with their online activities (Acquisti, et al., 2017). Having an automated intelligence assistant would also provide help and protections where children cannot rely on the safety of those responsible for their safety; not all parental relationships are safe.

Adults may not always be able to mediate or keep children safe online. There are challenges related to becoming an effective mediator; mediators need to develop subject knowledge, relying on information and education sources that they may not be equipped to understand (Burušić et al., 2019, Shin, 2018). However, children need to remain safe even when those mediating their interactions are insufficient, and therefore there is a need to provide children with conditions that will help them to make safer decisions.

Mediating online interactions to ensure that children remain safe may be a viable option. However, there is often a different attitude taken between child and mediator, whereby the child believes the mediator should ask their opinion, yet the mediator believes it is their responsibility and therefore permission need not be sought (Moser, Chen, & Schoenebeck, 2017). The disagreements between child and mediator can often lead to boundary turbulence where the child and mediator disagree, ultimately leading to mistakes being made (Ammari et al., 2015, Zhang-Kennedy et al., 2016).

The challenge of providing an environment where children can explore and take advantage of the opportunities offered by the Internet, while keeping their interactions safe and secure is indeed complex. While the solution is likely to involve a mixture of effective mediation, industry/regulation, and education of the children we are trying to protect, it is also imperative that children are equiped equipped with the ability to independently take safer decisions relating to online safety.

2.2. Privacy

Privacy takes on a different meaning for different people from within different cultures, and while there have been many different attempts to define privacy within the literature, there is no "one size fits all" definition. It is worth referring to Solove's work on "Conceptualising Privacy" which examines and evaluates different concepts/viewpoints of privacy within the legal literature (Solove, 2002). When discussing privacy, it is related to an individual's attitude towards privacy, which may or may not be reflected in their actions. This paper will not seek to define privacy, but assumes that individuals, be they children or their mediators, have an attitude towards how much they can control the information that is available about them; it also will acknowledge that this concept is flexible and may be different from moment to moment.

Hartikainen, Kinnula, Iivari, and Rajanen (2017) describe online safety as having different divisions such as content, contact, conduct, and computer usage threats. They interviewed 141 children aged between 10 and 12, and discovered they had been subject to disturbing or scary videos, scary photographs, stranger danger, cyber-bullying, sexual content, or something else; the essence of these findings are that our children are subject to lots of different threats in an online connected world (Hartikainen et al., 2017). While some of these online threats might be avoided with more careful privacy control, using those privacy controls may cause further problems down the line. Children need to learn how to manage their own privacy, not just by using privacy controls, but by assessing the risks and making informed decisions about subsequent actions.

There have been efforts to teach children about concepts relating to privacy, and how to make privacy-saving choices (Egelman et al., 2016, Zhang-Kennedy and Chiasson, 2016). It has been suggested that everybody has their own attitude towards privacy (Bryce & Fraser, 2014), and their attitude may not be reflected in their actions (Barth & de Jong, 2017), for example people may believe that they are private individuals yet they publish intimate details of themselves on social media. Children may self-report attitudes that have been heavily influenced by those mediating online privacy interactions, and those providing the mediation of online privacy interactions may have an entirely different attitude towards privacy; for example, a parent may think it is important that information is not published, but a service provider enables details to be published. It may be important that any solution does not attempt to impose an attitude towards privacy onto those that it is seeking to help, otherwise the solution may become unusable. The "tacit" nature of privacy means that no single solution will fit all.

"Boundary turbulence" occurs when children and mediators are responsible for taking a common attitude towards privacy (Ammari et al., 2015). There are likely to be disagreements and potentially inconsistencies when children have multiple mediators. Children are conscious of the "internal threat", for example older siblings who may learn their password, or parents who may ask them not to play on a game; whereas mediators are more aware of the "external threat" (Zhang-Kennedy et al., 2016) such as sexual predators. While parents identify privacy as their main barrier to Internet use (Livingstone, Blum-Ross, & Zhang, 2018), they are also often responsible for sharing more information than their child would like through so-called "sharenting" (Steinberg, 2017). Children are having very different experiences with their mediators with respect to their privacy boundary.

Privacy education is important and within the UK there have been attempts to standardise the syllabus for children relating to privacy. Egelman et al. (2016) took a risk-focused approach whereby the syllabus was influenced through ten principles. These ten principles identified threats that could occur because of risky behaviour. For example, principles included "you're leaving a footprint", "there's no anonymity" and "information is valuable" (Egelman et al., 2016). The UK Council for Internet Safety have recently released a framework to be used within schools to provide the scaffolding around what should be taught to children of different age groups, privacy and security is one of eight aspects of online education (Safety U.K. Council for Child Internet, 2020). Despite these positive moves, it is still open to individual educators/schools to interpret and provide learning materials and experiences for the children. This reintroduces the problem of consistency, not only with the educator's attitude towards privacy, but also with the materials and approaches used to educate the children. There have been several attempts to provide privacy-related materials that are child-friendly and effective (Di Gioia et al., 2019, Knijnenburg and Cherry, 2016, Zhang-Kennedy, Baig, and Chiasson, 2017, Zhang-Kennedy and Chiasson, 2016).

Zhang-Kennedy and Chiasson (Zhang-Kennedy & Chiasson, 2016) used an interactive book to teach privacy related concepts to children aged between 7 and 9 years old. The results of the evaluation of the book suggested that children found the book engaging, fun, easy to use, good for learning, the characters were likeable, and they were happy to tell other kids about their experience. However, this was about teaching children about somebody else's attitude towards privacy. This may be problematic because it attempts to impose a view of privacy rather than teaching them to reflect on their own attitudes to what should be private. As children start to get older, they will manage their own privacy choices more independently, and therefore it becomes even more important that they are able to manage their own privacy. Children may use the Internet to explore their identity, and by having their Internet usage mediated this may prevent this exploration from happening in the first place (Blackwell, et al., 2016). It is imperative that children not only learn about privacy concepts,

but they should also learn how to take decisions relating to their privacy. We want children to have the ability to take informed decisions in the absence of mediation; there are situations where online interactions should not be mediated by adults, for example when children are exploring their own identity.

It is not only apps that children interact with that raises privacy concerns, there has been an increasing number of interactive toys collecting and sending data to third parties over Internet connections; the children who own these toys probably have not read the privacy policy which means the children are at risk of telling their toys private information directly, or by the toy overhearing private conversations accidentally (Jones and Meurer, 2016, Mcreynolds, et al., 2016). Holtz et al. developed a set of privacy icons that would help people understand data practices, although these icons were not developed specifically for children (Holtz, Nocun, & Hansen, 2011).

Privacy policies are the way businesses explain to customers what data is collected about them, who has access to the data, and for what purpose they collect that data; yet this information is not suitable for children (Children's Commissioner, 2018). People are interested in privacy, but not interested in privacy policies (Hagan and Way, 2016, Silva et al., 2017). A privacy policy is often a monolithic document that uses legalistic and unfriendly language not understandable to most children (Children's Commissioner, 2018). The Children's Commissioner had some children look at a simplified privacy policy, and even then, some of the children believed it was written in an overly-complex way so that people could not understand it, and would be put off reading it therefore allowing data processors to do whatever they want with their data (Children's Commissioner, 2017). Privacy policies are written by lawyers, not by children, and typically not by people who know what will work well with children. Research has demonstrated that privacy policies are generally not read by anyone, let alone children (Staddon, Huffaker, Brown, & Sedley, 2012). Privacy policies can also change, and it is difficult to make people aware of what parts of a privacy policy has changed. For example, a person could read a privacy policy, agree to the terms and conditions, and then disclose personal/private information. If the company was then bought by a new owner, who operated a different privacy policy, then any disclosed personal data could suddenly be treated in ways that the user has not previously agreed to Children's Commissioner (2018).

To aid children, a solution should be provided which complements existing work but also does not attempt to impose a particular attitude towards privacy, else it risks being at odds with the child and their mediators. Not all children will understand the concepts involved, so the solution needs to provide access to developmentally appropriate education to help children understand the key issues in such a way that will help them to engage with making privacy-enhancing decisions.

2.3. Privacy interventions

The work undertaken to educate children about privacy concepts (Knijnenburg and Cherry, 2016, Zhang-Kennedy, Baig, and Chiasson, 2017) was designed to intervene near the beginning of a child's journey of understanding privacy concepts; these almost monolithic interventions demonstrated that education plays a key role, however the benefits are often short-lived (Kim et al., 2020). Unlike these comic-book style monolithic interventions, it may be possible for technology to identify when a child is about to disclose potentially private data and intervene, at that moment, to encourage them to take mindful decisions that are appropriate for their own attitude towards privacy for that situation.

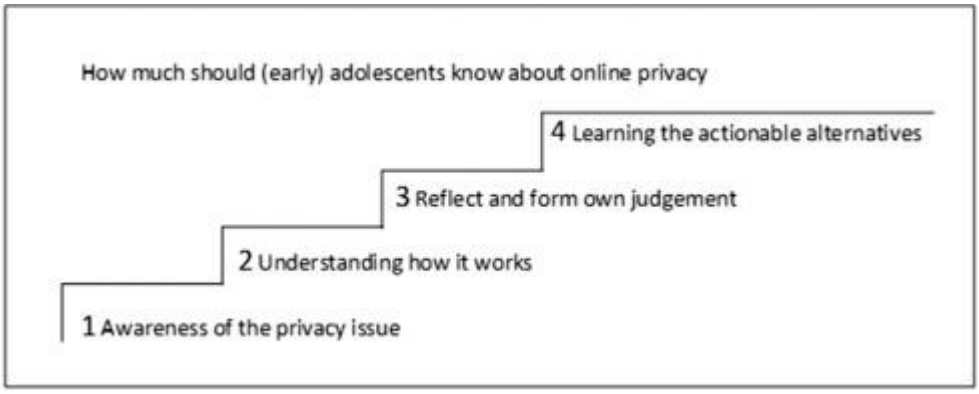
There have been other interventions designed to enhance privacy-related decisions, although these are not generally aimed at children. Balebako et al. (Mcreynolds, et al., 2016) and Egelman

et al. (Jones & Meurer, 2016) have both tested the impact of the timing of privacy interventions and their evidence suggested that intervening during app usage, or just-in-time, improved the salience of the intervention (Balebako et al., 2015, Egelman et al., 2009). While Patil's suggestion that moderately delaying feedback would avoid an overly alarming reaction to end-user privacy management (Patil, Hoyle, Schlegel, Kapadia, & Lee, 2015), it also risks imposing a personal attitude towards different privacy risks. Alohaly and Takabi suggested that privacy decisions can be taken based on first impressions of an app, and using a "privacy grade" before an end-user installs software can impact on that first impression (Alohaly & Takabi, 2016), however this approach while much more simple is still monolithic in approach. Egelman et al. created "Privacy Finder" a search engine which employed a set of privacy indicators help to quickly identify a mismatch between personal privacy choices and a website's published privacy policy (Egelman et al., 2009); however, this approach assumes that you are already educated and understand your own attitude towards privacy and that you are able to take decisions about potential mismatches. Children may not be able to comprehend the information presented.

Private data can be shared with businesses, for example by telling someone your home address, or it can be shared with individuals, for example by telling somebody your name or where you live. While it is possible to pre-determine when private data is disclosed to a business (for example, through typical data collection methods and form filling), it is not always possible to pre-determine when data will be disclosed to individuals (for example, when talking to somebody using a chat program), although AI maybe able to detect this disclosure. Intervening as the privacy risky behaviour is happening provides a contextualised, just-in-time response (Schaub, Balebako, Durity, & Cranor, 2015) making the child mindful of their interactions and its consequences. Kabat-Zinn defines mindfulness as "the awareness that emerges through paying attention on purpose, in the present moment, and nonjudgmentally to the unfolding of experience moment by moment" (Terzimehić, Häuslschmid, Hussmann, & Schraefel, 2019). Privacy interventions may need to be context sensitive and intervene before the child has disclosed private data to encourage them to take a mindful decision. This mindful approach can help to nudge children towards more privacy-enhancing decisions (Acquisti, et al., 2017).

Yap and Lee (2020) have created a four-stage engagement framework that defines how much an early adolescent knows about online privacy. While not explicitly referring to mindfulness, this four-stage model describes how a child may form their own attitude towards different privacy risks. This model is applied within an instructive/learning environment; however, it is equally suitable for just-in-time context-sensitive situations (see Fig. 1).

Based on this model interventions could intervene at the appropriate time to make the child aware that there is a privacy issue that needs to be considered. Dependent on their design they may then link to other educational resources giving the child the option to find out more if they do not yet understand the risks involved. Provided the privacy intervention intervenes at the correct and appropriate time then children can receive a context sensitive, just-in-time message that gains their attention to the current privacy risk. Kumar et al. identified that privacy-focused educational material should include relatable elements, equip children with the ability to make decisions and expose children to a range of consequences which can be accomplished by utilising the four stage engagement framework (Vitak, et al., 2018). How to make children aware and draw their attention to a possible risk has yet to be established, there are many possible solutions, including warning messages, pop ups and info graphics.



1. Download : Download high-res image (108KB)
2. Download : Download full-size image

Fig. 1. The four stage engagement framework (Yap & Lee, 2020).

A good warning message will gain the attention of the child quickly and therefore should be based on a three stage process whereby attention is gained (attention), risky behaviour is explained (knowledge), and actions that could be taken to comply to avoid that risky behaviour is provided to the user (compliance) (Laughery & Wogalter, 2014). However, care must be taken when providing warnings to children. There are many standards associated with warning signs (e.g BSI 5499-1:2002), yet it is unclear if these warning standards have been tested with children. Some of the children interviewed by Boto et al. stated that they could not understand a warning message's general meaning or purpose, and while over half of the children had learned about warnings at school, they continued to have difficulty with the vocabulary necessary to express what warnings are Boto et al. (2015). It is important that warning signs are tested with their intended audience (Wogalter, Conzola, & Smith-Jackson, 2002a), even if they follow already established guidelines. The research guidelines discussed in Wogalter, Conzola, and Smith-Jackson (2002b) contains various demographic variables, such as age, yet children were not specifically discussed, leading to the belief that children had not be specifically considered in the design and evaluation of warning designs.

2.4. Designing guidelines of warning messages in the context of children

Allowing warnings to be "contextualised" means giving designers the flexibility to accommodate their own look and feel within the presentation of privacy interventions. Therefore, rather than developing a fixed set of warnings, a set of design guidelines will be created instead. Within the Child Computer Interaction (CCI) community it is common practice to engage children in the design of systems meant for use by children; therefore, it may be possible for children to contribute to the design of a set of guidelines that can be used to implement privacy interventions.

Working with children to design guidelines relating to privacy interventions is likely to be challenging; children may not have the knowledge or experience necessary to make informed decisions about what private information to reveal online (Badillo-Urquiola, et al., 2019, Zhang-Kennedy et al., 2016). Faith Cranor, Reagle, and Ackerman (2000) have described children as being "disinterested in privacy", yet other research (Bryce & Klang, 2009) also claims that some young children have the ability to make associated judgments judgements about the risks in disclosing their data. Children are able to learn by rote what privacy means (Vitak, et al., 2018); however, they are unaware of what data can be collected without their knowledge, and expressed surprise and discomfort when it was explained what it could be used for Dowthwaite, et al. (2020). While not

focused on children, Hagan and Way designed a new set of privacy communications aimed at another disinterested group of stakeholders, 20–40 year olds, that engaged the audience by making privacy decisions more actionable (Hagan & Way, 2016).

There are many challenges identified within the CCI literature about designing for and with children. While every adult was once a child, they forget quickly and face different challenges than children, often with very different concerns (Read, 2005). A warning sign pictorial could mean something to a pre-conditioned adult yet mean something entirely different to a child whose imagination must find a meaning. For example, the skull and cross bones have often been used to identify poisonous materials whereas a child may see the skull and cross bones to mean pirate food (Boto et al., 2015). While Jeong and Chiasson focused on cybersecurity warnings, they identified differences in perception between adults and children with respect to important warning sign properties such as colour, symbols and the words used in common warnings (Jeong & Chiasson, 2020), indicating that it would be a mistake for adults to believe they can always design solutions for children.

Warning signs and labels have been designed for a wide range of different products and services. Kelley et al. developed a colour coded labelling system, they describe as a “nutrition label”, that would explain privacy policies to lay people (Kelley, Bresee, Cranor, & Reeder, 2009). While this nutrition label focused on privacy policies rather than privacy interactions, it demonstrates an approach to provide a design solution that makes the information more accessible and usable useable when presented in a different way. Privacy interventions such as “Privacy Bird” (Cranor, Guduru, & Arjula, 2006), “Privacy Grade” (Alohaly & Takabi, 2016) and “Privacy Finder” (Egelman et al., 2016) are further examples where a solution has involved the design of an intervention that provides the end-user with information before they take any action. None of these solutions had children in mind when they were developed, and as such these fixed designs are most likely not best placed to use within a child-context.

The CCI community is well-versed working with children to create solutions to technological problems. The CCI literature is full of examples of co-design, participatory design, or cooperative inquiry all of which involve working alongside children as solution designers. This approach has the distinct advantage that work is heavily influenced by those that it is designed to help; it engages children to design solutions for children. Children have demonstrated they can contribute to design guidelines for products aimed at children (Read et al., 2009, Sim et al., 2015). Vitak et al. (Zhang-Kennedy & Chiasson, 2016) developed a set of high-level guidelines about creating privacy-related games and stories for children (Vitak, et al., 2018); these guidelines are a good example where the guideline provides guidance rather than prescriptive answers. They recommend that children are equipped with the ability to make privacy-related decisions. Privacy knowledge is tacit, it means different things to different people, different people retain their own attitude towards privacy, and we are not looking to impose a view of privacy by rote. Lastly, when Vitak et al. suggest that children should be exposed to both negative and positive consequences of their actions. It is one of the key drivers for a privacy intervention that children should be able to locate related and context-sensitive situationally aware examples, so they are better equipped to take mindful decisions (Vitak, et al., 2018). It is evident from the literature that it may be feasible to design interventions with children to make them mindful about their interactions online.

3. Methodology

Based on the arguments in Section 2.4, this study produces a set of design guidelines by asking the question “how do children warn other children about the risks of disclosing data on the internet?”.

To answer this question, first, children were asked to design their own warning messages, utilising personas to help focus their design ideas for other children. These warning message designs were then analysed using content analysis (by coders or researchers), and the results are synthesised into a set of guidelines suitable for designing child friendly privacy warnings.

3.1. Participants

The study was reviewed and accepted by the University of Central Lancashire's Science and Technology ethics committee. The study involved asking children to design warning messages they would give to other children when disclosing data to other people.

As part of an outreach activity aiming to enthuse children about science and technology, several schools were invited to be part of a "MESS Day" experience (Horton, 2012). The schools were in and around the Preston area; Preston is within the 20% most deprived areas of England (Lancashire County Council, 2019). The school decided which children could attend the MESS Day, and no selection criteria was stipulated beforehand.

The format of the day was explained so that schools could plan their day in advance. Information sheets were provided to schools and parents. Prior to the event schools collected parental consent for the participation of their children, and for the collection of data produced during any studies.

On arriving at the event, using language adapted for children, assent, their right to withdraw and their right to not participate was explained. Their teachers were present should any child have any specific needs.

Immediately before the study commenced participants were reminded about their right to withdraw and their right to keep their data. At the end of the study, and before anything was collected, participants were reminded that they had the right to keep their warning message designs.

In total there were 141 participants, aged between 7 and 13 years old, with an average age of 9.8 SD 2.15. There were 63 boys, 77 girls and 1 participant did not record a gender. All the participants took part in the activity and consented to the use of their data.

3.2. Apparatus and design task

Participants had their own colouring pens and pencils and an activity booklet to create their designs in. Using a persona to focus their attention on designing for children, participants were asked to create warning messages relating to the disclosure of private data.

3.2.1. The privacy personas

Personas are commonly used by design teams to enable empathy and identification of similarities between the design team and the archetypal users of a proposed system (Salminen, 2018). A description of a persona typically contains their name, a photograph of the persona, and characteristics/details of the persona that help describe them as a typical user ((Jen) McGinn & Kotamraju, 2008). Designing for an identified persona, as opposed to a general class of "users", allows the design team to focus on the specific needs of that persona. The ethos of this study was to encourage the participants to design specifically for someone other than themselves.

Two privacy personas were developed by combining information about the typical online activities of children and their attitude towards privacy (Dempsey et al., 2018, Livingstone et al., 2017); to acknowledge the importance of mediator influence, details were added about the persona's

interests at school and details about their parents. These influential adults were synthesised by using the privacy segmentations described by Dupree, Devries, Berry, and Lank (2016), and creating a narrative around these attitudes to privacy. While it may not be typical to include information beyond the persona character themselves, it was decided to include information about mediators to provide a more life-like example of how a child may take decisions about disclosing privacy. While children are able to understand various concepts related to privacy (Dempsey et al., 2018), they are often disinterested in privacy (Bryce & Klang, 2009), or do not have the vocabulary or ability to articulate their knowledge (Boto et al., 2015). This would suggest that children are likely to fall within Dupree's "marginally concerned" group. However, children will often demonstrate behaviour which depends on a mediator's attitudes towards privacy (Dupree et al., 2016).

To help give the participants a focus for their design task, two personas were created that described an archetypical child-computer user. The personas were called Logan and Vienna. Logan was in year 4 at school (8 years old), was white British and did not have any siblings. Vienna was in year 6 at school (11 years old), was British African-Caribbean and had 1 younger sister. Fig. 2 contains the persona description of Logan.

Logan

Age: 8 Years Old
Ethnicity: White (British)
Brothers and Sisters: None
School: Year 4 (ages 8 and 9)

Attitude Towards Technology
Logan **has had an iPad** since his parents bought it for his 6th birthday present. He likes to play computer games he has downloaded for free from the App Store, and he has over 100 games currently installed. His favourite game is "Fortnite" because it **allows him to talk with other players while he is playing**, which makes the game so much more fun.

His parents have also paid for a Netflix account where he can access his favourite TV programmes such as "Teen Titans Go"; however, his **favourite activity is using YouTube** to watch how other people complete his favourite computer games.

He **occasionally uses Skype for video chats** with his grandparents, who live quite far away in Scotland. Logan **has an Instagram account that he created but doesn't yet use**, but he does use **snapchat filters to make funny pictures of himself** and his friends.

School
Logan enjoys going to school where he is on the school council and is a **member of the computer club**. He has recently started to learn how to use a BBC micro:bit during computer club. He really enjoys using computers to **help him complete his schoolwork** and will often hand in homework that he has created using "Notes" on his iPad.

Logan really enjoys playing football and is in the after-school football club. He only likes to play with his friends at school and doesn't want to play more seriously in a weekend league.

The Parents
Logan's Dad uses a computer for his job every day. He has a work laptop that he occasionally brings home, but he doesn't tend to spend that much time on his computer during the evening and weekend. His Dad is a big Preston North End fan and **encourages Logan to go outside and play**. Logan's Dad is **quite strict when it comes to using a computer** and sets times when Logan can use his iPad. He allows Logan to use his **iPad between 7pm and 8pm on a weekday**, and no longer than 3 hours at the weekend.

Logan's Mum is a teacher who uses a computer every day. She **knows the name of many apps** that help Logan to understand how to answer Maths questions and to learn phonics, and she has always encouraged him to play with technology to learn new skills. Logan's Mum **doesn't allow Logan to use his iPad just before bedtime.**

1. Download : Download high-res image (1MB)
2. Download : Download full-size image

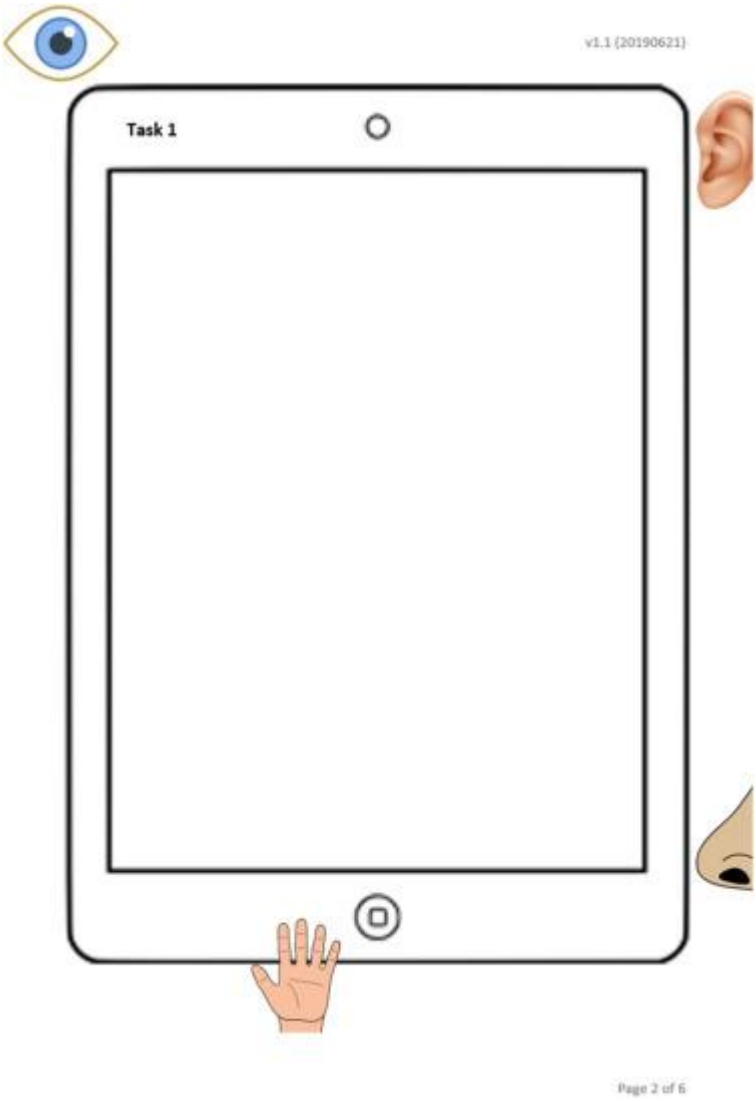
Fig. 2. Logan's persona description.

3.2.2. The activity booklet

An activity booklet was created for the children to design warning messages within. It contained 5 pages of A4 sized paper. Page 1 was a cover page with the title “Design Workbook” and space for the participants to record their age and gender. Pages 2, 3 and 4 contained a drawing space for the participant designs. Page 5 contained a word search puzzle with the names of superheroes (e.g., cyborg, ironman, and superman).

Fig. 3 shows the participant drawing space. This was enclosed by a table device outline, to help focus their attention to designing warning messages for a computing device (e.g., PC, tablet, mobile phone). Annotated around the tablet outline was an eye, an ear, a nose, and a hand, which were added to encourage participants to think about what a warning might look like, sound like, smell like or feel like; so that they did not feel constrained to visual warning designs. The design of the booklet was influenced by the concept of prime design (Fitton & Read, 2016), helping and encouraging the children to think about the different possibilities within the capabilities of the technology.

The activity booklet contained spaces for up to three designs, and the word search for any participants who either did not wish to participate or who finished earlier than the other participants.



1. Download : Download high-res image (148KB)

2. Download : Download full-size image

Fig. 3. Participant design space from the activity booklet.

3.2.3. Privacy risk scenarios

Solove's "taxonomy of privacy" classifies threats to privacy when disclosing data to others (Solove, 2006). These classifications cover a broad range of scenarios for when people disclose data. The risk of "surveillance" is when someone is watching, listening to, or recording data that is submitted. The risk of "interrogation" involves various forms of questioning or probing for information. Using these classifications and linking them to the prevalence of bullying in an online context (Office for National Statistics, 2020), two scenarios were created (described below) that children could have experience of. Instagram was used within the scenarios as the underlying technology/online service provider.

The risky behaviour within design task 1 (surveillance) is when Logan or Vienna are about to upload a photograph to Instagram. Many cameras can encode the GPS coordinates of where the camera was when the picture was taken and uploading a photograph to social media may mean that other people are able to probe the data for the location of Logan or Vienna. The photograph itself may also reveal information about Logan or Vienna but could also provide location information (for example their school or home address).

The risky behaviour within design task 2 (interrogation) is when Logan or Vienna are about to send a direct message to someone over Instagram. Even when you are "friends" with someone online through social media, you do not really know who you are talking to unless you are in their presence. A message sent to a friend may be intercepted by somebody else for example a parent or sibling.

3.3. Study procedure

The study was conducted over several weeks at the University. Upon arrival, the participants went to a computer room for a briefing on the day's activities. This included being introduced to the various researchers and then various concepts were explained to them. The idea of a scientific study, data, and assent was explained using child-friendly language and examples. This format has been used in previous studies within the institution (Horton, Read, Mazzone, Sim, & Fitton, 2012). Participants were told that the University was paying for this study, and that they could choose to participate and could decide if researchers could keep any data produced.

The participants were separated into small groups by their teachers, and each group went to their first activity. For this activity, each desk had an activity booklet and lots of different pens and pencils of different colours. A PowerPoint presentation was readied on the data projector containing information about both the persona they were designing for, and details of the design task. Each desk also had a printed copy of the persona information should the participant need a reminder.

When participants arrived, the researcher introduced himself and explained the aims of the study. The persona was explained, and the participants were engaged about how they had similar hobbies or experiences as the persona. For example, the participants would volunteer information about the type of videos they were watching on YouTube (often "slime" or "satisfying" videos).

The design task, including the privacy risky behaviour, was then described. The privacy risks were discussed with participants to make sure they understood them. The participants were given approximately 10-15 min 10–15 minutes to complete their designs/ drawings. Each participant had their own desk which encouraged them to work independently. The researcher did not stop them

from talking to their friends, however, often a teacher would suggest that they focus on their own work.

There were two personas and two risky behaviours, and the researcher would preselect which persona and which risky situation each group would work with. By preselecting which persona and which risky behaviour would be used, it allowed the researcher to collect a balanced set of data from the participants.

Some participants finished with time to spare and created a second design (the activity booklet had spare pages for this reason). A word search was provided, as an additional activity, for those that did not want to create designs, or who finished the task early. Once the task was finished, the participants were reminded that they could keep their activity booklets if they did not want us to keep their data. The activity booklets were collected, and the participants thanked. The participants were then taken to their next study/activity, and the room was set up again for the next group of participants.

3.4. Data analysis

Participants managed to create 162 individual drawings. 12 of those drawings were either incomplete, or the participant had decided to draw something not related to the task, and they could not be analysed; therefore, only 150 drawings contributed to the analysis. These drawings were analysed using content analysis to produce both quantitative and qualitative data that identified characteristics from within the drawings (Neuendorf, 2001). A "coding book" was created that dictated how the research would analyse these designs. Analysis of the designs was completed in two phases where the first phase involved analysing the "manifest" content, and the second phase involved analysing the "latent" content.

3.4.1. Phase one analysis — manifest content

Manifest content analysis quantifies a set of characteristics from across all the designs. These quantities can then be compared to draw conclusions. Analysis of the manifest content was achieved in two passes. The first pass built a "coding book", and the second pass used the coding book to quantify the characteristics within the designs.

Laughery and Wogalter (2014) suggested that an effective warning message would contain three different parts. The "attention" part will draw attention and make it clear there is an issue that should be considered. The "knowledge" part will explain the risks and dangers associated with continuing without taking avoiding actions. The "compliance" part will explain what actions should be taken to avoid or minimise the risks associated with that behaviour.

During the first pass the researcher examined each design and looked for characteristics within the attention, knowledge, and compliance parts. As the list of characteristics was created, the researcher compiled a list of potential values for those characteristics. These characteristics and potential values where then compiled into the coding book. Each identified characteristic is described and justified within Table 1, Table 2, Table 3.

3.4.1.1. Coding and reliability — manifest content.

The coding book contained instructions that explained what to look for and how to analyse the designs; the instructions included how to record the results of the analysis into a spreadsheet so that further analysis/quantification of the data could be carried out later. Two independent coders analysed the data. The first coder examined each of the children's designs one-by-one and following

the instructions in the coding book they quantified the characteristics for the attention, knowledge, and compliance parts of the designs.

Table 1. Description of attention characteristics.

Characteristic	Justification
Location	Where the attention part was displayed. For example, top, middle, bottom, pop-up.
Size	The size of the attention part. For example, small, medium, large.
Colours	The most prominent colours. For example, red and black.
Contrast	If contrast was used to gain attention, how that contrast was achieved.
Format	The way in which attention was achieved. For example, words, sound or pictorials.
Signal words	The words that were used to grab attention. For example, warning, stop, danger.
Pictorial	Any pictorials that were used to gain attention.

Table 2. Description of knowledge characteristics.

Characteristic	Justification
Terms used	The key words that were used to explain the risks. For example, “hacked”, “stranger” or “bully”.
Format	The way in which the risk was described. For example, words, pictorials or sounds.
Pictorials	Any pictorials that were used to explain the risks and consequences.
Risk made explicit	If the risk was made explicit during the description (y/n)

Table 3. Description of compliance characteristics.

Characteristic	Justification
Terms used	The key words that were used to explain how to avoid the risks. For example, “think”, “permission”, “get help”.
Style	The way in which compliance behaviour was explained. For example, vague, direct or cartoon.
Pictorials	Any pictorials that were used to explain how to avoid the risk.
Instructions explicit	Are the compliance instructions made explicit to the user? (y/n)
Child-friendly language	And do those instructions use child-friendly language? (y/n)

To check if the coding book was reliable, a sample of 10 randomly chosen designs were analysed by a second coder/researcher using the same coding book. The codes from the first researcher/coder were compared with the second researcher/coder and a percent agreement calculated using Holsti's method. A 92% agreement was achieved between researchers, suggesting that the coding book provided intercoder reliability.

After the coding had been completed, the first coder grouped some of the characteristics together to draw more abstract conclusions that drew together lots of slightly different characteristics together. For example, the terms "bully", "scammed" and "inappropriate" were grouped together and described as a "threat of a person".

3.4.2. Phase two analysis — latent content

Latent content relates to the underlying meaning of the design, rather than the explicitly clear characteristics of the designs. Characteristics identified during the latent content analysis will inform the design principles within the design guidelines. Rather than having a set list of characteristics to identify within the designs, latent content is first identified and then quantified. To achieve this, two further passes were made.

The first coder examined each of the designs to look for underlying meanings or qualities within the designs. During the second pass, the coder then quantified each of these qualities to understand how widespread they were within the designs.

The first pass identified the latent qualities listed in Table 4:

Table 4. Description of latent characteristics.

Characteristic	**Justification**
Fun/Engaging	16 out of 162 tried to engage the audience by making their designs fun, colourful or humorous
Real world	35 out of 162 included real-world apps, such as Instagram
Character type	48 out of 162 used characters within their designs; some were animals, some were people
Emotion	27 out 162 used "fear" of bad things happening
Stories	33 out of 162 focused on a story where things happened in sequence
Instructive	64 out of 162 were instructive and told the audience what to do

4. Results

The results of the analysis of the 150 drawings are presented below.

4.1. Quantitative data manifest content

The characteristics identified in Table 1, Table 2, Table 3 were quantified by examining each design.

4.1.1. Having attention, knowledge and compliance

The coder recorded if the design had an attention part, knowledge part and compliance part. Identifying this enabled the other characteristics to be focused on. For example, if there was no attention part then the attention characteristics were not examined further.

While we were not testing to see if children could design warnings that contained all aspects of what is perceived to be effective warning message (Laughery & Wogalter, 2014), we could still draw some conclusions from this data. For example, Fig. 4 identifies that only 37 of the 150 designs contained all three important aspects of an effective warning sign (e.g. attention, behaviour, compliance parts). Most of the warning designs contained something to grab user attention; however, providing knowledge was present in only 73 of 150 (48.67%) designs.

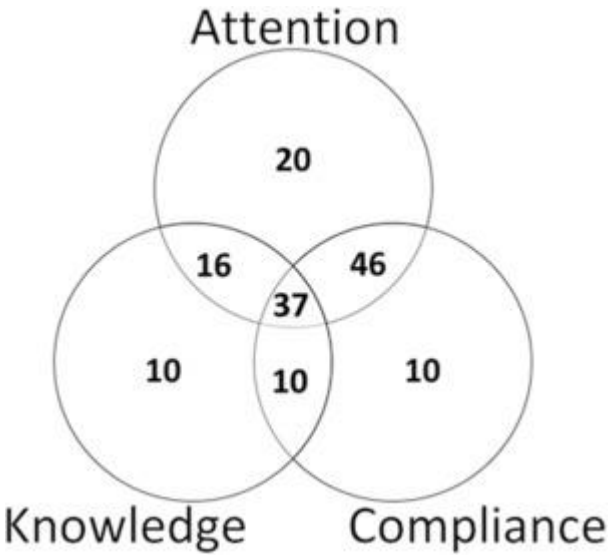


Fig. 4. Venn diagram describing who has attention, knowledge and compliance.

4.1.2. Attention part characteristics

While the participants had different strategies for gaining user attention, only 5 of those designs the location appeared to be important, as the position of the pop-up warnings was displayed over and above the rest of the warning message. There were only 4 designs where the size appeared to be an important part of grabbing attention; therefore, the researcher determined that size may not necessarily be important due to this low frequency.

As may be expected with UK participants, red was the predominant colour, used as an important part of gaining attention in 63 of the designs. This may be attributed to the fact that red is used within other warning signs and is associated with negative consequences, for example in food labels and road traffic signs. Black was the second most used colour on 17 designs, followed by yellow (7), multi-colours (6), blue (2), green (1) and orange (1). The selection of many of these colours may simply be attributed to the pen they originally selected. Contrast was difficult to analyse and was not evident in all the drawings as some children only used one colour to draw, as shown in Fig. 6. The background colour of the paper would also influence contrast as black on white, or warnings on a light background were the most popular.

The format of the attention part was grouped, pictorials were the most common method of grabbing attention (10), followed by sound (7) and then words (5). Signal words were grouped, words that related to valuing the risk (such as “warning” or “careful”) were the most popular with 54

occurrences; words indicating a time or delay (such as “stop” or “wait”) had 29 occurrences, and words relating to cognitive action (such as “think”) had 10 occurrences.

Fig. 5. Example design where the threat “of” a person was made.

4.1.3. Knowledge part characteristics

Terms used to describe the knowledge were grouped and threat “of” a person had the most occurrences with 36 occurrences; cyber-related threats occurred 18 times and threats “to” the person occurred 17 times. In the example in Fig. 5 there are three instances where the child makes comments about being bullied, being rude and being told where to go.

Participants used “words” to communicate the risk in 60 of the pictures, whereas pictorials were only used 13 times. The most common words were related to a threat of a person, for example “bully”, “track you down”, “stranger”, “track you”, and “could hurt”. The most common pictorial involved a character who represented an actor involved in the risky situation.

4.1.4. Compliance part characteristics

Terms used to describe how to avoid/mitigate the consequences/risk were grouped and “not doing something” occurred the most often with 37 times; to “stop and think” occurred 36 times, and “to ask someone” occurred 27 times.

The style of the compliance part was mostly “instructive” where the participants were given a set of instructions to follow to avoid the consequences. Vague instructions were also given on several occasions where the instruction related to avoidance techniques without being explicit on what needed to be done. For example, “be careful” or “stop, think”.

The most common pictorial involved the central character/actor taking action to avoid the risks (see Fig. 6).

Fig. 6. Example design depicting a character involved in the risky behaviour. The story for this character involved having a stranger arrive at their front door after uploading a photograph to social media.(For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

4.2. Qualitative data - latent content

Qualities of the designs, outside of the “attention, knowledge, compliance” structure of a warning message were quantified. The most frequent quality was that the warning messages were “instructive”, telling the reader what they should or should not do. Other frequent qualities indicated that warnings should include a person, within a real-world setting, and should tell a story. One quality that was not clear was “fear” which was used to promote an action (e.g. avoid doing this action otherwise something bad will happen) (see Table 5).

Table 5. Quantities of latent qualities.

Quality	Quantity
Instructive	64
Person	45
Real World	35
Story	33
Fear	27
Fun	16
Animal	3

5. Discussion and guidelines

The analysis of the data focused on the model for developing warning signs (Laughery & Wogalter, 2014) and this model will be adapted to inform design guidelines from the results of this study and literature (Grammenos and Stephanidis, 2002, Mcknight and Fitton, 2010, Waterson and Monk, 2014). The adaptation is based on the children's drawings, the literature with the model (Egelman et al., 2009) being extended to encapsulate the key characteristics depicted by the children. The cross validation from the literature is essential to ensure there are theoretical underpinnings to the proposed guidelines. Despite only a third of the participants having an attention, knowledge, and compliance part to their warning signs, over 50% had two of the three characteristics. The data provided by the participants offered valuable insights into their comprehension of the risks and how this might be mitigated through warning messages (see Fig. 7).

Fig. 7. Example design where a character is used to describe how to avoid the risk.

5.1. Design principles (latent analysis results)

Outside of the attention, knowledge and compliance areas all privacy intervention warning messages should have similar qualities.

- warning messages should be instructive
- warning messages should avoid using vague terms; make any actions to avoid or mitigate risks clear and specific
- actions should be concrete in nature and avoid abstract terms to comply with the developmental needs of children at this age (Lee, 2000)
- warning messages should contain pictorials that include children in real-world settings
- stories should be used to help children understand the knowledge and compliance parts (Vitak, et al., 2018, Zhang-Kennedy, Baig, and Chiasson, 2017, Zhang-Kennedy and Chiasson, 2016). From the children's drawings 35 of the designs contained a real-world setting, with 33 of them setting the warning against a story backdrop.

Despite “fear” being identified in several of the designs, the researcher believes that fear is not a suitable means to achieve a desired outcome, although this has been used globally on products such as cigarette package (Brewer, et al., 2016). 27 of the designs included a portrayal of fear or need to fear the outcomes, while only 16 designs illustrated that the solution could also be fun. The purpose of any warning message should be to help a child make a mindful decision about what data to disclose, causing fear and obeyance to a pre-determined action would not encourage children to make mindful decisions. Fig. 8 is an example of a design which contains an undercurrent of fear; in this design the central character is holding what appears to be a knife dripping with blood, while the character on screen has crosses for their eyes.

While 64 designs suggested any solution should be instructive, it is the researchers belief that children should be empowered to make their own decisions towards privacy therefore warning messages should facilitate the child to make their own decision; the knowledge part will educate the user about the risks of their behaviour, and the compliance part will instruct the child how to avoid those risks, however the warning message should not prevent a child from taking any action.

Fig. 8. Example design with an undercurrent of “fear”.(For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

5.2. Design guidelines for attention (manifest analysis results)

The intervention should gain the child’s attention quickly; and this may mean drawing their gaze away from where it would have been without the intervention. Research has highlighted the problem with digital warning messages often being ignored (Livingstone et al., 2017) including the

fact users are accustomed to warning messages and these are often ignored (Egilman & Bohme, 2006). Table 1 justifies the important characteristics of the attention part, guidelines for which are synthesised below after the analysis has been compared to the available literature.

Location: Without the designs showing a physical interface it was difficult to judge whether children meant the warnings to be central with a user interface or to one side. The children may have focused on the content of the warning rather than the location of the warning. Despite this there were 7 messages that clearly represented a physical location within a screen. From these 5 out of 7 warning messages "popped up over the top". Although this is a small number of the children's design, there is evidence from a larger study with 667 adults that showed warning signs may be more effective when placed in the middle of the screen rather than in the periphery (Gainsbury, Aro, Ball, Tobar, & Russell, 2015).

Guideline A1: When privacy interventions appear, they should be separate from the action they are intervening and should appear in the middle of the screen.

Colours and Contrast: Red was used the most common colour used to grab attention and is associated with warnings in western cultures, but also recognised in other culture for example Hong Kong (Siu, Lam, & Wong, 2017). Red has been recognised as an effective warning message (Laughery, Young, Vaubel, & Brelsford, 1993) however, other primary colours may be suitable for a global market. For example in a study looking at colour in warning messages between the US and India, red, green, yellow were demonstrated to be effective at keeping participants from continuing with non-compliant actions (Silic, 2016). In addition, any message needs to ensure sufficient contrast between the foreground and background, black was the most common colour used to provide contrast between foreground and background within the children's drawings.

Guideline A2: Privacy interventions could use primary colours to attract attention; the contrast between foreground and background should be enough to identify that the intervention is separate; colour choice can be made using cultural norms.

Format: The main formats used to obtain attention were words, sounds and pictorials; however, only 22 out of 119 designs that were coded with attention characteristics used formatting to obtain attention and most of the time attention was obtained by the fact there was a warning message appearing. The most common shape to gain attention, used 57 out of 119 times, was to display a warning message within the shape of a triangle with an exclamation mark at the top.

Guideline A3: Privacy interventions could be encapsulated within a shape such as a triangle with an exclamation mark placed at the top.

Signal Words: Words such as "warning", "danger" or "stranger danger", or words which quickly describe the risk associated with the situation were used in 59 out of 119 designs and were the most common type of signal word. Secondly most common words included "stop", "think" or "wait" which encourage a pause before any further action is taken. The use of signal words such as danger, warning and caution has been recommended by the American National Standards Institute (ANSI, 2015) and maybe effective within this context.

Guideline A4: Use words that alert children to the risk (such as "warning" or "careful") and consider using phrases relating to time or delay before taking physical or cognitive action. If signal words are presented through sound then the emotional voicing may have greater impact (Barzegar & Wogalter, 1998).

5.3. Design guidelines for knowledge

The knowledge part should give information about the risk and consequence. Researchers have attempted to educate children about the adverse consequences concepts (Knijnenburg and Cherry, 2016, Zhang-Kennedy, Baig, and Chiasson, 2017). Where possible both positive outcomes and negative outcomes should be communicated so that children are knowledgeable about the risk and the range of consequences (Vitak, et al., 2018).

Terms used: From the data children used lots of different terms to describe the risky behaviour, so the risks were categorised into smaller subgroups. Children used a wide range of different terminology to describe the risks within the 73 designs that were coded with knowledge characteristics. For example, in 36 of the designs they contained some kind of “threat of a person”, this is where the threat came from a character within the design and 18 of the designs contained some kind of “cyber threat” which had terms that could easily relate to the Internet for example, “private”, “track you down” or “hacked site”. Whilst 17 of the designs contained a “threat to the person” which involved terms such as “kidnap”, “bully” or “scam”.

Guideline K1: Designers should use plain and clear language that relate directly to the threat the risky behaviour has towards the child. For example, this may be a direct threat to the child because the action they are undertaking reveals their location or whereabouts.

Format: Children tended to use words or pictorials to impart knowledge about the risky behaviour whilst they did not use sound at all. 60 out of 73 designs used words and 13 designs used pictorials. Where pictorials were used the majority contained a central character to explain the risky behaviour. The use of characters has been used with children in other research were comics depicted the scenarios (Children’s Commissioner, 2018).

To describe the risky behaviour words should be used to describe the risky behaviour. If pictorials are to be used, it may be advisable to have a central character that can be consistently presented across different risky behaviours to form some sort of narrative/story. Age needs to be considered as it has been suggested that younger children have been found to respond better to animals than characters (Waterson & Monk, 2014). Cartoon characters have also been shown to be effective at communicating risk (Zhang-Kennedy, Baig, & Chiasson, 2017).

Guideline K2: Use words to describe the risky behaviour, if pictorials are also be used then include a central character across all pictorials.

Risk Made Explicit: 41 out of 73 designs made it clear/explicit what risk was associated with continuing the behaviour. For example, in Fig. 5 you can see that the child has clearly stated “people may cyber bully you”; this text clearly states that continuing to behave in the same way may lead to cyber bullying.

Guideline K3: The risk associated with continuing their behaviour should be made clear. A selection of both positive and negative outcomes should be presented within the privacy intervention (Vitak, et al., 2018).

5.4. Design guidelines for compliance

The compliance part of the privacy intervention should provide instruction/assistance so that the end-user knows what they can do to avoid taking the risky behaviour. While the purpose of the compliance part is to inform what actions can be taken to avoid the risky behaviour, the compliance

part should also be educational and provide an opportunity for both the child and mediator to learn (Badillo-Urquiola, et al., 2019).

Terms used: There were a range of different terms presented in the designs and these were categorised into three broader categories. The three categories are: What not to do based on 37 of the designs suggesting that the compliance terms should expressly tell the user what not to do; stop and think with 36 of the designs recommending the end-user should stop and think before they continue with their action; ask somebody else with 27 of the designs suggesting they should seek advice from another. These three categories encapsulate good advice where we want children to make mindful decisions (stop and think), avoid risky behaviours where they are confident (what not to do) and ask advice from a mediator when they are less confident (ask somebody else).

Guideline C1: The privacy intervention should encourage all children to pause, think and take mindful decisions; for those that are confident enough they should be directed to clear and easy instructions that avoid the risky behaviour (for example, “do not tell someone where you live”), but for those who are not as confident it should direct them to speak with a mediator.

Style: Children had many different styles for presenting compliance behaviour, with the “giving clear instructions” the most common style found in 46 out 103 designs. Other suggestions included “giving explicit instructions”, “using cartoons” and “asking a question”.

Guideline C2: Any compliance behaviour should be clearly stated using child-friendly language, but it should be instructional making it clear what actions to take to avoid the risky behaviour. Compliance behaviours could be portrayed and explained to facilitate dual processing of the information (Mayer & Moreno, 1998). This should help facilitate their comprehension by using multiple channels to process the information.

Pictorials: Children are emergent readers; therefore, assumptions cannot be made about whether the children can read and comprehend written text. Therefore, pictorial representation is recommended and widely used in info graphics and warning signs (Boto et al., 2015, Schaub et al., 2015, Wogalter et al., 2002b). Where language is used this should be moderated to ensure it is at the appropriate level for the children. In the children’s designs they largely omitted pictorials to communicate compliance, those that did use pictures had a central character or an animal within the pictorial.

Guideline C3: Like Guideline K2, privacy interventions could include characters, but a central character should be used across all pictorials. Where possible, link the warning message with the real-life context. These need to demonstrate how to avoid the risk for example, not uploading the image or accepting the friend request.

5.5. Using the guidelines to design privacy interventions

When using these guidelines, the designer must be working within a specific context; for example, they may be designing privacy interventions for a child’s online chat programme.

The “design principles” describe the general properties of the privacy interventions; for example, the design principles state that privacy interventions should be instructive/educational because all privacy interventions should aim to help children (and their mediators) learn about privacy, and to take mindful decisions about their own attitudes towards privacy.

The “design guidelines” describe the characteristics of the three parts of a privacy intervention. A privacy intervention should contain an attention part, knowledge part and compliance part; the guidelines describe how these three parts should be presented to the user.

It is essential to understand that the designer should be working within a specific context. All privacy interventions should be instructional/educational no matter the context, however, the privacy intervention may look very different for a child’s online chat program for a mobile phone environment versus an online chat program on a PC-based Windows 10 environment.

6. Conclusions and future work

This paper has contributed a set of design guidelines informed by children to aid the creation of online safety interventions. The research has shown that children can design warnings for each other, and the design guidelines generated provides designers with a basis for creating child-focused and child-informed “privacy interventions”.

The design guidelines produced adhere to the issues raised earlier in this paper. They follow warning message principles and have an “attention, knowledge and compliance” part (Laughery & Wogalter, 2014). By using the guidelines to create interventions it should facilitate children to develop their own education, abilities and will encourage them to take mindful decisions in the disclosure of any data (Yap & Lee, 2020). The guidelines can be used in any situation where private data is disclosed, and not just when submitting private data to businesses (Information Commissioners Office, 2020). While the guidelines have been written by an adult, they have been crafted by children identifying the things that will work best for other children, thus will meet the legal obligations placed by GDPR requiring data processors to use child-friendly language (Information Commissioners Office, 2019).

Further research is required to understand if the guidelines are effective within a global market. The guidelines have been developed with children in the UK and it is unclear whether these would transcend to other cultures or address the needs of children with cognitive or physical disabilities.

There are many different privacy risk situations and interaction styles that could be accounted for, so to test the viability of the design guidelines, a context must be given to the design task. For example, one context might be the warning messages found within an online chat program used on a computer. Any privacy warning symbols can be tested to see if the encourage children to think about the consequences of their actions before it is too late. Further work will look at the creation of interventions using the guidelines and their effectiveness with children.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors would like to express thanks to the schools and children who took part in these MESS days and contributed their thoughts and efforts to this study.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., et al. (2017). Nudges for privacy and security. ACM Computing Surveys, 50, 1–41. http://dx.doi.org/10.1145/3054926.

Alohaly, M., & Takabi, H. (2016). Better privacy indicators: A new approach to quantification of privacy policies. In Twelfth symp. usable priv. secur.. https://www.usenix.org/conference/soups2016/workshop-program/wpi/presentation/alohaly.

Ammari, T., Kumar, P., Lampe, C., & Schoenebeck, S. (2015). Managing children ' s online identities : How parents decide what to disclose about their children online. In Chi 2015 (pp. 1895–1904). http://dx.doi.org/10.1145/2702123.2702325. ANSI (2015). ANSI Z535 safety alerting standards.

Assal, H., Imran, A., & Chiasson, S. (2018). An exploration of graphical password authentication for children. International Journal of Child-Computer Interaction, 18, 37–46. http://dx.doi.org/10.1016/j.ijcci.2018.06.003.

Badillo-Urquiola, K., Smriti, D., McNally, B., Golub, E., Bonsignore, E., & Wisniewski, P. J. (2019). Stranger danger! Social media app features co-designed with children to keep them safe online. In Proc. 18th ACM int. conf. interact. des. child. (pp. 394–406). http://dx.doi.org/10.1145/3311927.3323133.

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., & Cranor, L. (2015). The impact of timing on the salience of smartphone app privacy notices. In Proc. 5th annu. ACM CCS work. secur. priv. smartphones mob. devices (pp. 63–74). http://dx.doi.org/10.1145/2808117.2808119.

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox - Investigating discrep-

ancies between expressed privacy concerns and actual online behavior - A systematic literature review. Telematics and Informatics, http://dx.doi.org/10.1016/j.tele.2017.04.013.

Barzegar, R. S., & Wogalter, M. S. (1998). Intended carefulness for voiced warning signal words. Proceedings of the Human Factors and Ergonomics Society, 2, 1068–1072. http://dx.doi.org/10.1177/154193129804201503.

Bell, B. T. (2019). You take fifty photos, delete forty nine and use one: A qualitative study of adolescent image-sharing practices on social media. International Journal of Child-Computer Interaction, 20, 64–71. http://dx.doi.org/10.1016/j.ijcci.2019.03.002.

Bentley, H., Fellowes, A., Glenister, S., Mussen, N., Ruschen, H., & Slater, B. (2020). How safe are our children? 2020 - An overview of data on abuse of adolescents. (p. 66). https://learning.nspcc.org.uk/media/2287/how-safe-are-our-children-2020.pdf.

Bergholz, A., Paaz, G., Reichartz, F., Strobel, S., & Chang, J. H. (2008). Improved phishing detection using model-based features. In 5th Conf. email anti-spam. http://www.webcallerid.net. (Accessed 24 February 2021).
Blackwell, L., Hardy, J., Ammari, T., Veinot, T., Lampe, C., & Schoenebeck, S. (2016). LGBT parents and social media: advocacy, privacy, and disclosure during shifting social movements. In Proc. 2016 CHI conf. hum. factors comput. syst (pp. 610–622). http://dx.doi.org/10.1145/2858036.2858342.

Boto, R., Noriega, P., & Duarte, E. (2015). Warnings for children: Do they make sense? Procedia Manufacturing, 3, 6086–6092. http://dx.doi.org/10.1016/j.promfg.2015.07.753.

Brewer, N. T., Hall, M. G., Noar, S. M., Parada, H., Stein-Seroussi, A., Bach, L. E., et

al. (2016). Effect of pictorial cigarette packwarnings on changes in smoking behavior a randomized clinical trial. JAMA Internal Medicine, 176, 905–912. http://dx.doi.org/10.1001/jamainternmed.2016.2621.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Computers in Human Behavior, 30, 299–306. http://dx.doi.org/10.1016/j.chb.2013.09.012.

Bryce, J., & Klang, M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences. Information Security Technical Report, 14, 160–166. http://dx.doi.org/10.1016/j.istr.2009.10.007.

Burušić, J., Šimunović, M., & Šakić, M. (2019). Technology-based activities at home and STEM school achievement: the moderating effects of student gender and parental education. Research in Science and Technological Education, 39, 1–22. http://dx.doi.org/10.1080/02635143.2019.1646717.

Children's Commissioner (2017). Growing up digital. https://app-t1pp-cco.azurewebsites.net/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf.
Children's Commissioner (2018). Who knows what about me? https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf.

Cranor, L. F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction, 13, 135–178. http://dx.doi.org/10.1145/1165734.1165735.

Dempsey, J., Cassidy, B., & Sim, G. (2016). Child-centered security. (pp. 1–3).

Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for GDPR - investigating

children's understanding of privacy: A survey approach. In Proc. 32nd int. BCS hum. comput. interact. conf. (pp. 1–13). http://dx.doi.org/10.14236/ewic/HCI2018.26.

Di Gioia, R., Chaudron, S., Gemo, M., & Sanchez, I. (2019). Cyber chronix, participatory research approach to develop and evaluate a storytelling game on personal data protection rights and privacy risks. In Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics): vol. 11899 LNCS, (pp. 221–230). http://dx.doi.org/10.1007/978-3-030-34350-7_22.

Dowthwaite, L., Creswick, H., Portillo, V., Zhao, J., Patel, M., Vallejos, E. P., et al. (2020). It's your private information. it's your life.: Young people's views of personal data use by online technologies. In Proc. interact. des. child. conf. (pp. 121–134). http://dx.doi.org/10.1145/3392063.3394410.

Dupree, J. L., Devries, R., Berry, D. M., & Lank, E. (2016). Privacy personas: Clustering users via attitudes and behaviors toward security practices. In Chi'16 (pp. 5228–5239). http://dx.doi.org/10.1145/2858036.2858214.

Egelman, S., Bernd, J., Friedland, G., & Garcia, D. (2016). The teaching privacy curriculum. In Proc. 47th ACM tech. symp. comput. sci. educ. (pp. 591–596). http://dx.doi.org/10.1145/2839509.2844619.

Egelman, S., Tsai, J., Cranor, L. F., & Acquisti, A. (2009). Timing is everything? The effects of timing and placement of online privacy indicators. In Conf. hum. factors comput. syst. - proc. (pp. 319–328). New York, New York, USA: ACM Press, http://dx.doi.org/10.1145/1518701.1518752.

Egilman, D., & Bohme, S. R. (2006). A brief history of warnings. In Handb. warn. (pp. 35–48). Mahwah, NJ: Lawrence Erlbaum Associates.

European Parliament and Council of European Union (2018). Recital 38 - Special

protection of children's personal data. https://gdpr-info.eu/recitals/no-38/.

Faith Cranor, L., Reagle, J., & Ackerman, M. (2000). Beyond concern: Understanding net users' attitudes about online privacy. In Internet upheaval rasing quest. seek. answers commun. policy.

Fitton, D., & Read, J. C. (2016). Primed design activities: Scaffolding young designers during ideation. In ACM Int. conf. proceeding ser.. http://dx.doi.org/10.1145/2971485.2971529.

Fitton, D., Read, J. C., Sim, G., & Cassidy, B. (2018). Co-designing voice user interfaces with teenagers in the context of smart homes. In Proc. 2018 ACM conf. interact. des. child (pp. 55–66). http://dx.doi.org/10.1145/3202185.3202744.

Gainsbury, S., Aro, D., Ball, D., Tobar, C., & Russell, A. (2015). Determining optimal placement for pop-up messages: evaluation of a live trial of dynamic warning messages for electronic gaming machines. International Gambling Studies, 15, 141–158. http://dx.doi.org/10.1080/14459795.2014.1000358.

Grammenos, D., & Stephanidis, C. (2002). Interaction design of a collaborative application for children. In Int. work. ''interaction des. child'' (pp. 11–28). Shaker Publishing.

Hagan, M., & Way, N. A. (2016). User-centered privacy communication design. (pp. 1–7). https://www.usenix.org/system/files/conference/soups2016/wfpn16-paper-hagan.pdf.

Hartikainen, H., Iivari, N., & Kinnula, M. (2015). Children and web 2.0: What they do, what we fear, and what is done to make them safe. In Lect. notes bus. inf. process, (pp. 30–43). http://dx.doi.org/10.1007/978-3-319-21783-3_3.

Hartikainen, H., Iivari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. International Journal of Child-Computer Interaction, 22, Article 100146. http://dx.doi.org/10.1016/j.ijcci.2019.100146.

Hartikainen, H., Kinnula, M., Iivari, N., & Rajanen, D. (2017). Finding common ground: Comparing children's and parents' views on children's online safety. In HCI 2017 digit. make believe - proc. 31st int. BCS hum. comput. interact. conf. (pp. 1–12). http://dx.doi.org/10.14236/ewic/HCI2017.43.

HM Government (2017). Internet safety strategy – Green paper. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf.

Holtz, L. E., Nocun, K., & Hansen, M. (2011). Towards displaying privacy information with icons. In IFIP adv. inf. commun. technol. 352 AICT (pp. 338–348). http://dx.doi.org/10.1007/978-3-642-20769-3_27.

Horton, M. (2012). Activities with children. (pp. 2099–2104). http://dx.doi.org/10.1145/2223656.2223759.

Horton, M., Read, J. C., Mazzone, E., Sim, G., & Fitton, D. (2012). School friendly participatory research activities with children. In Proc. 2012 ACM annu. conf. ext. abstr. hum. factors comput. syst. ext. abstr. (pp. 2099–2104). http://dx.doi.org/10.1145/2212776.2223759.

J. Dempsey, G. Sim, B. Cassidy et al. International Journal of Child-Computer Interaction 31 (2022) 100446

Information Commissioners Office (2018). Guide to the general data protection regulation: Children. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/. (Accessed 14 March 2018).

Information Commissioners Office (2019). Individual rights: The right to be informed. Review of the Air Force Academy, 17, 89–96. http://dx.doi.org/10.19062/1842-9238.2019.17.1.12.

Information Commissioners Office (2020). Age appropriate design: a code of practice for online services. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/. (Accessed 7 September 2020).

(Jen) McGinn, J., & Kotamraju, N. (2008). Data-driven persona development. In Proceeding twenty-sixth annu. CHI conf. hum. factors comput. syst. (p. 1521). http://dx.doi.org/10.1145/1357054.1357292.

Jeong, R., & Chiasson, S. (2020). Lime, open lock, and blocked: Children's perception of colors, symbols, and words in cybersecurity warnings. In Conf. hum. factors comput. syst. - proc. (pp. 1–13). http://dx.doi.org/10.1145/3313831.3376611.

Jones, M. L., & Meurer, K. (2016). Can (and should) Hello Barbie keep a secret? In 2016 IEEE int. symp. ethics eng. sci. technol.. http://dx.doi.org/10.1109/ETHICS.2016.7560047.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A nutrition label for privacy. vol. 1990, In Proc. 5th symp. usable priv. secur.. http://dx.doi.org/10.1145/1572532.1572538.

Kim, B., Lee, D. Y., & Kim, B. (2020). Deterrent effects of punishment and training on insider security threats: a field experiment on phishing attacks. Behaviour and Information Technology, 39, 1156–1175. http://dx.doi.org/10.1080/0144929X.2019.1653992.

Knijnenburg, B., & Cherry, D. (2016). Comics as a medium for privacy notices. In Proc. twelfth symp. usable priv. secur.

Lancashire County Council (2019). The English Indices of Deprivation, 2019 – key findings for the Lancashire-12 and Lancashire-14 areas. https://www.lancashire.gov.uk/media/913361/deprivation2019.pdf.

Lastdrager, E., Gallardo, I. C., Junger, M., & Hartel, P. (2017). How effective is anti-phishing training for children? In Proc. thirteen. symp. usable priv. secur. (pp. 229–239). https://www.usenix.org/conference/soups2017/technical-sessions/presentation/lastdrager.

Laughery, K. R., & Wogalter, M. S. (2014). A three-stage model summarizes product warning and environmental sign research. Safety Science, 61, 3–10. http://dx.doi.org/10.1016/j.ssci.2011.02.012.

Laughery, K. R., Young, S. L., Vaubel, K. P., & Brelsford, J. W., Jr. (1993). The notice-ability of warnings on alcoholic beverage containers. Journal of Public Policy and Marketing, 12, 38–56. http://dx.doi.org/10.1177/074391569501200105.

Lee, K. (2000). Piaget's theory of cognitive development. In Child. cogn. dev. essent. readings. Blackwell Publishes Ltd.

Livingstone, S. (2018). Children : a special case for privacy? InterMedia, 46, 18–23.

Livingstone, S., Blum-Ross, A., & Zhang, D. (2018). What do parents think, and do, about their children's online privacy? parenting for a digital future: survey report 3, www.parenting.digital.

Livingstone, S., Davidson, J., & Bryce, J. (2017). Children's online activities, risks and safety A literature review by the UKCCIS evidence group. https://www.gov.uk/government/uploads/system/uploads/attachment_data/

file/650933/Literature_Review_Final_October_2017.pdf.

Lobe, B., Velicu, A., Staksrud, E., Chaudron, S., & Di Gioia, R. (2020). How children (10–18) experienced online risks during the Covid-19 lockdown - Spring 2020. http://dx.doi.org/10.2760/562534.

Mak, D., & Nathan-Roberts, D. (2017). Design considerations for educational mobile apps for young children. In Proc. hum. factors ergon. soc. 2017-Octob (pp. 1156–1160). http://dx.doi.org/10.1177/1541931213601773.

Mayer, R. E., & Moreno, R. (1998). A split-attention effect in multimedia learning: Evidence for dual processing systems in working memory. Journal of Educational Psychology, 90, 312–320. http://dx.doi.org/10.1037/0022-0663.90.2.312.

Mcknight, L., & Fitton, D. (2010). Touch-screen technology for children : Giving the right instructions and getting the right responses. (pp. 238–241).

Mcreynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2016). Toys that listen: A study of parents, children, and internet-connected toys.

Moser, C., Chen, T., & Schoenebeck, S. (2017). Parents' and children's preferences about parent s sharing about children on social media. (pp. 6–10).

Neuendorf, K. A. (2001). The content analysis guidebook [paperback] (p. 320). http://www.amazon.com/Content-Analysis-Guidebook-Kimberly-Neuendorf/dp/0761919783/ref=sr_1_1?s=books&ie=UTF8&qid=1395675490&sr=1-1&keywords=Content+analysis+guidebook+Neuendorf.

Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P. (2020). Investigating teenagers' ability to detect phishing messages. In Proc. - 5th IEEE eur. symp. secur. priv. work (pp. 140–149). http://dx.doi.org/10.1109/

EuroSPW51379.2020.00027.

Nouwen, M., & Zaman, B. (2018). Redefining the role of parents in young children's online interactions. A value-sensitive design case study. International Journal of Child-Computer Interaction, 18, 22–26. http://dx.doi.org/10.1016/j.ijcci.2018.06.001.

Ofcom (2021). Children and parents: media use and attitudes report Content consumption and online activities.

Office for National Statistics (2020). Online bullying in England and Wales. (pp. 1–13). Off. Natl. Stat., https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/onlinebullyinginenglandandwales/yearendingmarch2020#prevalence-of-bullying.

Patil, S., Hoyle, R., Schlegel, R., Kapadia, A., & Lee, A. J. (2015). Interrupt now or inform later? (pp. 1415–1418). http://dx.doi.org/10.1145/2702123.2702165.

Pinter, A. T., Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). Adolescent online safety: Moving beyond formative evaluations to designing solutions for the future. In Proc. 2017 ACM conf. interact. des. child. (pp. 352–357). http://dx.doi.org/10.1145/3078072.3079722.

Read, J. C. (2005). The ABC of CCI. Interfaces (Providence), 62, 8–9, http://www.bcs.org/upload/pdf/interfaces62.pdf.

Read, J., & Beale, R. (2009). Under my pillow – designing security for children's special things. In HCI 2009-23rd annu. conf. human-computer interact. (pp. 288–292).

Read, J. C., & Cassidy, B. (2012). Designing textual password systems for children. (pp. 200–203).

Read, J. C., Horton, M., Clarke, S., Jones, R., Fitton, D., & Sim, G. (2018). Designing for the at home experience of parents and children with tablet games. In Proc. 2018 ACM conf. interact. des. child. (pp. 441–448). http://dx.doi.org/10.1145/3202185.3202769.

Read, J. C., Horton, M., Mazzone, E., Cassidy, B., & McKnight, L. (2009). Designing for Mr Hippo - Introducing concepts of marginalisation to children designers. In IDC 2009 conf. interact. des. child (pp. 3–6). https://www.researchgate.net/publication/237293125_Designing_for_Mr_Hippo_-_Introducing_Concepts_of_Marginalisation_to_Children_Designers.
Safety U. K. Council for Child Internet (2020). Education for a connected world. (pp. 1–58).

Salminen, J. (2018). Persona perception scale : developing and validating an instrument for human-like representations of data. (pp. 1–6).

Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. In Elev. Symp. Usable Priv. Secur. (pp. 1–17).

Shin, W. (2018). Empowered parents: the role of self-efficacy in parental mediation of children's smartphone use in the United States. Journal of Children and Media, 12, 465–477. http://dx.doi.org/10.1080/17482798.2018.1486331.

Silic, M. (2016). Understanding colour impact on warning messages: Evidence from us and India. In Conf. hum. factors comput. syst. - proc. (pp. 2954–2960). http://dx.doi.org/10.1145/2851581.2892276.

Silva, C. S., Silva, I. S., Silva, T. S., & Mourão, F. (2017). Privacy for children and

teenagers on social networks from a usability perspective : A case study on facebook. (pp. 63–71). http://dx.doi.org/10.1145/3091478.3091479.
Sim, G., & Cassidy, B. (2013). Investigating the fidelity effect when evaluating game prototypes with children. In HCI 2013-27th int. br. comput. soc. hum. comput. interact. conf. internet things (pp. 193–200). http://dx.doi.org/10.14236/ewic/hci2013.62.

Sim, G., Read, J. C., Gregory, P., & Xu, D. (2015). From England to Uganda: Children designing and evaluating serious games. Human-Computer Interaction, 30, 263–293. http://dx.doi.org/10.1080/07370024.2014.984034.

Siu, K. W. M., Lam, M. S., & Wong, Y. L. (2017). Children's choice: Color associations in children's safety sign design. Applied Ergonomics, 59, 56–64. http://dx.doi.org/10.1016/j.apergo.2016.08.017.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., et al. (2020). EU kids online 2020: Survey results from 19 countries. (pp. 1–3). http://dx.doi.org/10.21953/lse.47fdeqj01ofo, EU Kids Online.

Sofian, N. M., Hashim, A. S., & Ahmad, W. F. W. (2018). A review on usability guidelines for designing mobile apps user interface for children with autism. AIP Conference Proceedings, 2016, 282–288. http://dx.doi.org/10.1063/1.5055496.

Solove, D. J. (2002). Conceptualising privacy. California Law Review, 90, 1087.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154, 477–564.

Staddon, J., Huffaker, D., Brown, L., & Sedley, A. (2012). Are privacy concerns a turn-off? In Proc. eighth symp. usable priv. secur. (p. 1). http://dx.doi.org/10.

1145/2335356.2335370.

Steinberg, S. B. (2017). Sharenting: Children's privacy in the age of social media. Emory Law Journal, 66, 839–884.

Straker, L., Abbott, R., Collins, R., & Campbell, A. (2014). Evidence-based guidelines for wise use of electronic games by children. Ergonomics, 57, 471–489. http://dx.doi.org/10.1080/00140139.2014.895856.

Suarez, Luz Yolanda Toro (2019). Statistics briefing: child sexual abuse. (pp. 1–27).

Sun, J. C. Y., Kuo, C. Y., Hou, H. T., & Lin, Y. Y. (2017). Exploring learners' sequential behavioral patterns, flow experience, and learning performance in an anti-phishing educational game. Educational Technology & Society, 20, 45–60.

J. Dempsey, G. Sim, B. Cassidy et al. International Journal of Child-Computer Interaction 31 (2022) 100446

Terzimehić, N., Häuslschmid, R., Hussmann, H., & Schraefel, M. C. (2019). A review & analysis of mindfulness research in HCI framing current lines of research and future opportunities. In Conf. hum. factors comput. syst. - proc. (pp. 1–13). http://dx.doi.org/10.1145/3290605.3300687.

UNICEF, W. C. Foundation, E. V. A. Children, ITU, UNESCO, UNODC, et al. (2020). COVID-19 and its implications for protecting children online. (pp. 1–6). https://www.end-violence.org/sites/default/files/2020-07/COVID-19 and its implications for protecting children online_Final%28003%29_0.pdf.

Vitak, J., Clegg, T. L., Yang, J., Kumar, P., Chetty, M., Bonsignore, E., et al. (2018).

Co-designing online privacy-related games and stories with children. (pp. 67–79). http://dx.doi.org/10.1145/3202185.3202735.

Waterson, P., & Monk, A. (2014). The development of guidelines for the design and evaluation ofwarning signs for young children. Applied Ergonomics, 45, 1353–1361. http://dx.doi.org/10.1016/j.apergo.2013.03.015.

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.hack: Engaging anti-phishing training through a role-playing phishing simulation game. In Conf. hum. factors comput. syst. - proc. (pp. 1–12). http://dx.doi.org/10.1145/3290605.3300338.

Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002a). Research-based guidelines for warning design and evaluation. Applied Ergonomics.

Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002b). Research-based guidelines for warning design and evaluation. Applied Ergonomics, 33, 219–230, http://www.ncbi.nlm.nih.gov/pubmed/12164506.

Yap, C. E. L., & Lee, J. J. (2020). Phone apps know a lot about you!: Educating early adolescents about informational privacy through a phygital interactive book. In Proc. interact. des. child. conf. (pp. 49–62).

Zhang-Kennedy, L., Abdelaziz, Y., & Chiasson, S. (2017). Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. International Journal of Child-Computer Interaction, 13, 10–18. http://dx.doi.org/10.1016/j.ijcci.2017.05.001.

Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2017). Engaging children about online privacy through storytelling in an interactive comic. In HCI 2017 digit. make believe - proc. 31st int. BCS hum. comput. interact. conf. (pp. 1–12). http://dx.doi.org/10.14236/ewic/HCI2017.45.

Zhang-Kennedy, L., & Chiasson, S. (2016). Teaching with an interactive E-book to improve children's online privacy knowledge. In Proc. 15th int. conf. interact. des. child. (pp. 506–511). http://dx.doi.org/10.1145/2930674.2935984.

Zhang-Kennedy, L., Mekhail, C., & Chiasson, S. (2016). From nosy little brothers to stranger-danger : Children and parents ' perception of mobile threats. In ACM SIGCHI conf. interact. des. child. 2016 (pp. 388–399). http://dx.doi.org/10.1145/2930674.2930716.