# It takes a Society to Protect Childrens' Privacy Rights

**Karen Renaud[1], Deanna House[2], Teju Herath[3]**

[1] University of Strathclyde, Glasgow, UK. karen.renaud@strath.ac.uk
Rhodes University, RSA. University of South Africa, RSA.

[2] University of Nebraska Omaha, USA. deannahouse@unomaha.edu

[3] Brock University, Canada. therath@brocku.ca

This is a peer-reviewed, accepted author manuscript of the following paper: Renaud, K., House, D., & Herath, T. (Accepted/In press). It takes a society to protect children's privacy rights. Paper presented at 2021 Dewald Roode Workshop, San Antonio, United States.

# It takes a Society to Protect Childrens' Privacy Rights

*Early Stage Research*


## Abstract

Privacy-related research spans multiple disciplines and is centuries old. The topic of children's privacy is a complicated and multi-faceted area of privacy research. The responsibility for teaching children about privacy usually falls on their parents' and carers' shoulders. This responsibility can be quite challenging for them to embrace, with rapidly changing technological advances across the globe and difficulties being exacerbated by the combined efforts of multinational organizations striving to gather their data. This research attempts, first, to explore the concept of privacy in the existing research literature, and particularly in the online context. The authors then seek to identify the challenges faced by parents related to their children's privacy. In particular: (1) what are the difficulties with respect to citizens' understanding what privacy means, and (2) in conveying its import to children? We conclude that *everyone* has a role to play in shoring up our children's privacy. It starts with the parents, but involves every one of us.


## 1. Introduction

Privacy is the universal human right to consent before personal information is collected and processed (Diggelman & Cleis, 2014). The first step towards embracing this right is to understand it, and this is where things get complicated. Post (2001, pp. 2017) argues that: "*Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and* distinct *meanings, that I sometimes despair whether it can be usefully addressed at all."* These sentiments are echoed by Thomson (1975). Even so, we *have* to address it, or risk losing our privacy altogether because privacy, once lost, cannot be retrieved. Because people don't understand privacy principles, they disclose their personally identifiable information (PII) voluntarily (Ciocchetti, 2007) and subject themselves to risks, including data breaches, identity theft, reputational damage, and/or financial damage.

The United Nations Convention on the Rights of the Child (undated) explains that: "*Every child has the right to privacy. The law must protect children's privacy, family, home, communications and reputation (or good name) from any attack.*" The problem with this statement is that when the law gets involved, a privacy violation has *already* taken place – and the law can only punish, not restore lost privacy. It is much better to act before this happens to *prevent* the loss of privacy.

Personal data is collected and monetized, making it the core product, (rather than the games or videos) (Fuchs, 2021). Of further concern is that while regulatory and legislative controls for children's data exist; the focus is mainly on protecting children's data rather than limiting the amount of data that is collected about them (Andrews et al., 2020). And lastly, of great concern is that those involved in the "data collection value chain" (Vosloo et al., 2020, pg 3) – which can include software creators and operators – may not prioritize what is best for children in relation to their data. Indeed, a study by Nairn & Monkgol (2007) explored 20 top sites accessed by children in the U.K. and found that eighty-five percent of these collected personal information from children and that provision of such information was a necessary precondition for participation. Moreover, 60% of school apps share children's data (Wodinsky, 2021). Wolf (1978) argues that a lack of privacy can contribute towards children's emotional disorders.

MacLeod (2007, pp. 3) argues that "*Children are distinct but dependent and particularly vulnerable members of the moral community.*" There is a clear responsibility to ensure that children can be online safely without losing their privacy (De Wolf & Vanden Abeele, 2020; Urban and Hoofnagle, 2014). Given the previous discussion, this is not a given. This constitutes something of a call to action, with a degree of urgency. The question is, how should we go about achieving this?

Section 2 reviews the literature on privacy, with particular attention being paid to children's privacy. Section 3 reviews related research and Section 4 proposes a methodology for carrying out an empirical investigation into parents' understanding of privacy and their current practices in conveying its principles and nuances to their children. Section 5 concludes.

## 2. Scoping Privacy

Privacy can be a difficult concept to define, particularly in the age of digital transformation. As mentioned by Pavlou (2011), it is important for Information Systems (IS) researchers to take a multi-disciplinary

approach when considering privacy-related work, which the authors took into consideration. We commence with the basics of privacy to ensure that the foundational knowledge is understood and incorporated.

The concept of privacy is very personal, while also being somewhat abstract and hard to articulate (Hart, 1954). Many global citizens do not seem to exercise their privacy rights (Renaud et al., 2015). Gross (1967) suggests that while people are often able to sense, intuitively, that their privacy is being violated, they struggle to articulate what privacy actually means to them, and to insist on their privacy rights. Gross (1967) quotes Hart (1954) who explains that, when it comes to privacy, people can "know" what privacy is without being able to define the concept. Bott and Renaud (2018) suggest that people have accepted the extensive and invisible privacy violations that occur when we are online, having gone through a grieving process and become resigned to the fact.

We will review the dimensions and nature of privacy in the next section, but at this point a broad-brush definition will serve to facilitate a link between core privacy principles, online harm dimensions and parents' risk management endeavors. We use Westin's (1968, pp. 7) definition of privacy as "*the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others*" to facilitate this.

With respect to children being online, Professor Byron (2008) explains that online harms to children can be categorized into one of the three C's: (1) Content, (2) Conduct and (3) Contact.

*Content* where the child can be exposed to unwarranted commercial, aggressive, sexual or other types of harmful information. Children are developmentally more vulnerable to the effects of digital marketing (Radesky et al., 2020), which makes this kind of contact particularly concerning. *Conduct* risks occur where a child, as a participant, may engage in activities such as communicating with strangers, bullying, or sharing information that can be harvested for a variety of purposes. C*ontact* occurs when an external agent, as an actor, may contact a child without their parents' knowledge or consent for their own nefarious purposes.

Children's privacy-related behaviors are arguably connected to the "conduct" category. Renaud and Prior (2021) suggest that online harms can be managed by parents and carers by using the three M's: **m**entoring the child, **m**itigating harms using a variety of technologies (where possible) and **m**onitoring the child's online activities to ensure their cybersecurity and cybersafety. We will align online privacy with the

"mentor" category, given that privacy is inextricably related to individual consent and not easily remediated with technical measures. Figure 1 depicts privacy as aligned with Byron's "Conduct" and Renaud & Prior's "Mentor" categories.

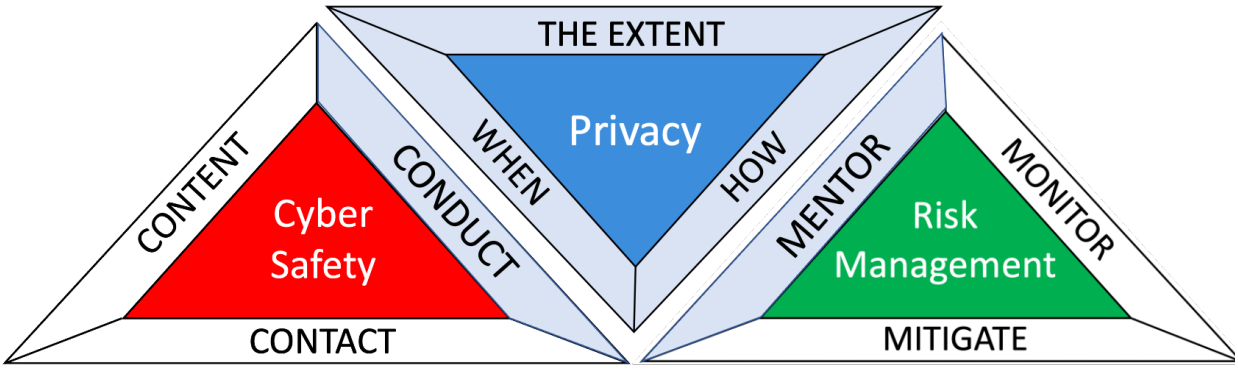



**Figure 1: Linking Privacy to Cyber Safety and Risk Management**

Table 2 in the Appendix covers key views on privacy taken from the research literature. A Word Cloud generated from the definitions is shown in Figure 2. It is interesting to note that the word "vulnerability/vulnerable" does not appear, which suggests a genericity that might well need to be abandoned in order to accommodate the differing needs and perspectives of children, when it comes to privacy.

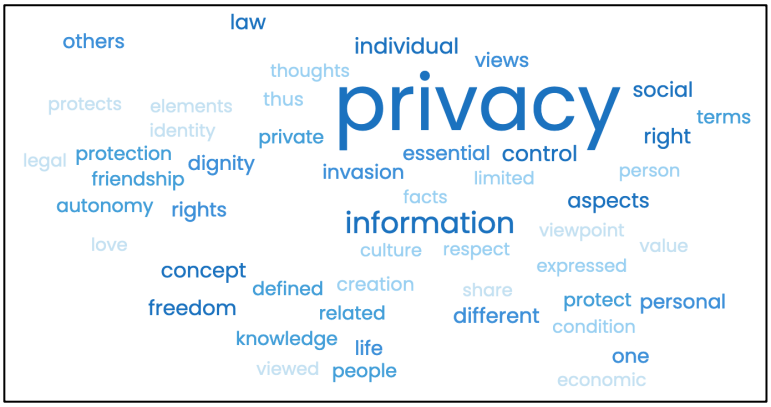



**Figure 2: Word Cloud from definitions in Table 2.**

### *2.1. Information Privacy*

A subset of privacy, information privacy, has gained some traction in privacy-related research. While traditional privacy definitions refer to the individual's rights to privacy in homes and private spaces, information privacy refers to control of "*access to individually identifiable personal information*" (Smith et al., 2011).

The concept of control is an important factor when defining information privacy. As defined by Clarke (1999), information privacy "*refers to the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use"* (pp. 60). The concept of information privacy is similar to general privacy in its subjectivity and also is influenced by external factors. According to Bélanger & Crossler's (2001) research, from an individual perspective, the differences related to gender, age, and education have been previously studied; with a need for trait-level variations to be explored in future privacy research. For example, Paine et al. (2007) have found that those in age groups younger than 20 have fewer concerns about online privacy, although this is not confirmed by the population-wide drawings gathered by Privacy Illustrated (2014).

Research has shown that when individuals have a belief and desire for privacy in the physical world, they will also have concerns about privacy related to companies/entities in the online world (Yaow et al., 2007). Yaow (2007) argues that online privacy and related research should thus be viewed in a similar light as that related to privacy; with the online context being a distinct qualifier.

### *1.1. Privacy Decisions*

Privacy is frequently rooted in ethics and ingrained in society's moral value system (Smith et al., 2011). Decisions related to privacy are not made in a black box; there are many contributing factors that may influence an individual's behavior (Mitgen & Smith, 2015). Moreover, beliefs related to privacy rights are generally subjective, while also varying between individuals (Yaow et al., 2007; Westin, 1968). They are also context dependent. The context we are interested in are: (1) online privacy, (2) for children.

Despite substantial self-reported concerns with regard to online privacy, people engage in self disclosing behaviors that do not align with their stated concerns. Several studies have investigated this so-called "privacy paradox" empirically, with a few meta-analyses (Gerber et al. 2018; Kokolakis 2017). Gerber et. al (2018) provide several explanations for this phenomenon.

The privacy calculus model suggests that if the anticipated benefits of data sharing exceed the costs, a user can be expected to give his/her data away. On the other hand, numerous studies on consumer decision making behavior have shown that the decision-making process is influenced by various cognitive biases and heuristics (Acquisti and Grossklags, 2007). Some of the psychological and individual factors influencing privacy decisions include information asymmetries between consumers and firms, bounded rationality limiting the sufficiency of processing capacity to make sense of complexities of information environment, biases. This results in the overestimation of immediate benefits and underestimation of delayed costs, bolsters an illusion of control, and encourages herding tendencies i.e. imitating other people's behaviors (Acquisti et al. 2020). Acquisti et al. (2020) argue that while privacy enhancing technologies (PETs) offer significant potential to individual and societal benefits, many do not take advantage of them, due to unawareness, distrust, or perceived (and actual) costs.

Some argue that the privacy paradox is an artefact of the methodological implementation of inquiries (Dienlin and Trepte 2015). Solove (2020) calls the privacy paradox a myth, which is created by faulty logic. Most often, the behavior involved in privacy paradox studies involves people making decisions about risk in very specific contexts, while measurements of privacy concerns, or questions about how much participants value privacy, are much more general in nature.

Privacy attitudes, concerns, and risks are closely related yet different concepts and may be operationalized in different ways. Some describe privacy concerns as "the desire to keep personal information out of hands of others" (Buchanan, Paine, Joinson, & Reips, 2007, pp. 158) with attitudes operationalizing accordingly (Jozani et al. 2020). Others describe privacy concerns as "negatively valanced emotional feelings" (Dienlin and Trepte 2015) which may operationalize differently (Malhotra et al. 2004).

Yet another challenge is related to the many dimensions of privacy. Burgoon (1982) and Dienlin and Trepte (2015) identify several dimensions: *informational privacy*, which captures the individual control over the

processing and transferring of personal information; *social privacy*, which captures the dialectic process of regulating proximity and distance toward others; *psychological privacy*, which captures the perceived control over emotional and cognitive inputs and outputs; and *physical privacy*, which captures the personal freedom from surveillance and unwanted intrusions upon one's territorial space.

Dienlin and Trepte (2015) suggest that it is important to distinguish between privacy *attitudes* and privacy *concerns* on the one hand, and between *informational*, *social* and *psychological* privacy on the other. Their study reveals that the privacy paradox can be detected in empirical data when analyzed exactly as it was carried out in prior research. However, it disappears when privacy concerns and attitudes are distinguished, or when the Theory of Planned Behavior is used as a theory-driven framework to operationalize the research design, or when privacy dimensions (informational, social, and psychological) are differentiated.

Solove argues "*Managing one's privacy is a vast, complex, and never-ending project that does not scale; it becomes virtually impossible to do comprehensively.*" In recent study, Buckman et al. (Buckman et al. 2019) show that in contrast to prior research which has found significant effects for each of the salient factors of privacy decision when studied separately, when considered together, the effects are different. Several experiments show null effects demonstrating that results from prior research on simple privacy decisions may not translate to more realistic, complex privacy disclosure decisions that involve multiple factors.

### *2.2 Responsibility for Children's Privacy*

There are several views related to children's privacy, characterized by, and differences of, opinion related to where the responsibility lies for assuring that children's privacy is maintained. Some place responsibility on the children themselves (Nairn & Monkgol, 2007; De Wolf & Vanden Abeele, 2020) or on their parents (Lwin et al., 2008; Sorensen, 2016). The latter makes sense since parents' own sharing behaviors can violate their children's privacy (Steinberg, 2016; Shmueli and Blecher-Prigat, 2010; Bessant, 2017).

Others believe that industry or software developers should regulate their own privacy practices in this respect (Hertzel, 2000; Nairn & Monkgol, 2007; Miyazaki et al., 2009; Tahaei and Vaniea, 2021). This is unlikely to work, given that these companies pay only a pittance in fines for violating customers' privacy (Kafka, 2019; Short & Toffel, 2007). Yet others place responsibility on teachers (Cucinelli, 2015), schools

(Berson & Berson, 2006; Finkelhor et al., 2021); governments (Hertzel, 2000); or on the family unit (Todres, 2019).

Most intriguing is the suggestion that responsibility be placed on the child's community (MacLeod, 2007; Barbovschi, 2014). This approach would place a lesser burden on children as individuals and instead incorporate a "balance of responsibilities" (pp. 572). In this model, parents would be expected to assure their children's privacy while also extending that role to other trusted individuals (Fahlquist, 2015).

Steeves and Webster (2008) point out that supervision by parents and teachers cannot protect children's privacy completely. Children are frequently able to easily disclose personal information without parental knowledge or consent (Nairn & Monkgol, 2007). Making it a community responsibility would seem to be a much more realistic option.

This leads us to the conclusion that children themselves need to understand privacy, and they can only do so if everyone in their support network helps them to understand the concept and gives them the tools to exercise their rights to privacy. The responsibility to teach children these principles currently lies with parents (Desimpelaere, 2020), who hold the right to consent on their children's behalf in many countries (Gligorijević, 2019).

Yet, leaving it to the children, even if they know how to exercise their rights, will never be enough. In 2020, Bryan et al. (2020) reported that UK betting companies had been given access to the names, ages and addresses of 28 million British children. These kinds of actions violate children's privacy in a way that neither parents, teachers nor children are able to prevent. It is clearly time for children's privacy to be taken far more seriously by *everyone* in society.

### *2.3 Children & Privacy*

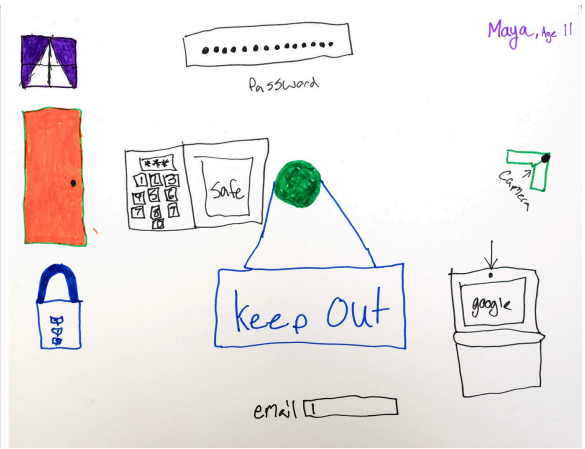
The UK's Information Commissioner's Office (2018) explains that "*Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.*" As discussed in the previous section, parents have a specific responsibility to ensure that their children's privacy is protected (De Wolf & Vanden Abeele, 2020) and to teach them privacy principles. It is going to be difficult for parents to help their children to understand their privacy rights if they themselves

have difficulty defining privacy or explaining what privacy rights are, which is certainly an issue based on the discussion earlier in this section.

Children are exposed to electronic devices at an increasing and somewhat alarming rate, at ever younger ages. There are some protective measures in place, but they are generally limited and often ineffective. Remote learning during the COVID-19 pandemic has created a backlog for privacy challenges, as many children who previously did not have access to devices were suddenly provided with a tablet or laptop. The quick shift to remote learning created new ways to access existing data (that was previously not easy to access) in addition to new data sources that did not exist prior to the COVID-19 pandemic (Sella-Villa, 2020/2021). Expectations of screen time and aspects of media consumption were undoubtedly adjusted as a result of the educational and social challenges of the COVID-19 pandemic (Willett, 2021). Parents were forced to work remotely and try to balance work and educational requirements (Bhamani, 2020). In light of these considerations, security and privacy may not have been a priority. While many schools are moving back to face-to-face mode, there is a concern that entrenched bad habits will be difficult to eradicate (Richtel, 2021).

Carnegie Mellon University publishes a website called “Privacy Illustrated” from a project which collects images of privacy drawn by people across the life span. Their privacy-related images provide us some insights into children’s understanding of privacy. Cranor et al. (2014) categorized the hundreds of drawings they collected into themes, one of which was online privacy, which seemed to be a particular theme of teens’ drawings. Figure 3 shows two drawings taken from the 9-12 age group on the website, showing that an understanding of privacy is often merged with concepts related to online security/safety. While these are inter-related, they have distinct differences which both adults and children need to understand. Interestingly, in the Word Cloud depicted on their website, the theme “teach” does not appear, which underlines the need for this investigation. Moreover, if you click on the tag “parents”, both images were drawn by children and reflect physical privacy (29 June 2021).


Privacy drawing reflecting a security mechanism (password).




Privacy drawing reflecting a security mechanism (password), physical privacy (keep out) but also mentioning Google, demonstrating an understanding of online privacy as well.

**Figure 3: Drawings from Carnegie Mellon's "Privacy Illustrated" Corpus**

## *2.4 What are Parents Doing?*

As discussed earlier, parents are initially tasked with the responsibility for the management of their children's online data (Desimpelaere, 2020). This increasingly pressures them to stay up to date on the latest technologies and online data collection tactics (Subrahmanyam & Greenfield, 2008).

This can be challenging due to issues related to parental self-efficacy, which, as discussed by Bélanger et al. (2013), is the capability of parents to provide privacy protection. This suggests that such self-efficacy in the privacy domain is by no means a given, for reasons we covered in the introduction.

Based on a Google trends search, it does not seem as if parents are looking for guidance in this respect, either (Figure 4).

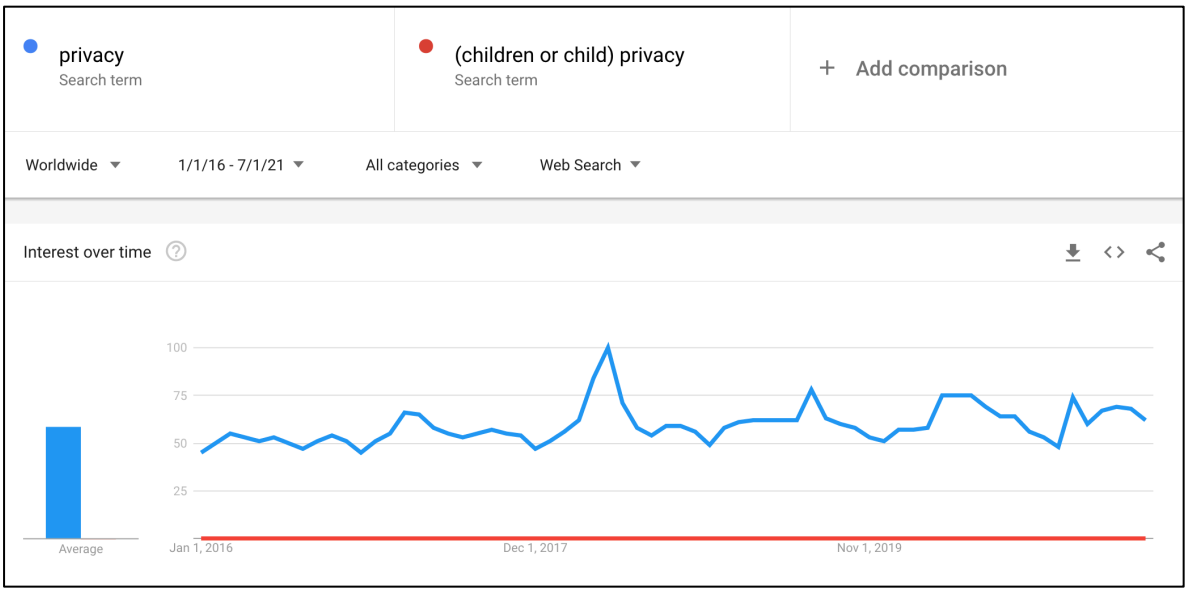



**Figure 4: Google Trends search on the 30 June 2021**

If parents do search online, what would they find? We carried out a search for "children privacy" using Google on the 3rd July 2021. Three million results were returned, which is bound to be daunting to the uninitiated. We focused on the first two pages only, given that very few searchers go beyond the first page (Cutrell & Guan, 2007). The appearance of Walt Disney's privacy policy on the first page is interesting, given that they experienced a large data breach in 2019 (Volf, 2019).

**Table 1: An online search for "children privacy" on the 3rd July, 2021**

| What | Description | Who |
|---|---|---|
| Children's Online Privacy Protection Act (COPPA); | Legal approach | Federal Trade Commission; Winston & Stawn LLC; Wiki |
| Role of Parental Consent | Legal Aspects in European Court of Human Rights | Gligorijević (2019) |
| Child Privacy Policy | Legal document laying out privacy rights | Walt Disney ViacomCBS |
| Guidance for companies related to children's privacy rights | What they can collect and what the rules are about doing this | UNICEF |
| Children's Privacy Policy | What they collect and whom they share with | Google |
| Children's privacy from their parents | | Shmuel & Blecher (2011) |
| Global information privacy community and resource | Legal approaches and news reports | https://iapp.org/ |
| Children's need for privacy | Explaining about age differences | Morelli (undated). |
| Do's and Don'ts for parents | Tips for parents to follow | Goldstein. (undated). |
| Children's Privacy Rights | Advice for companies in collecting children's data, laws around their data in the UK; obtaining parental consent | UK's Information Commissioner; United Nations Human Rights |
| Protecting Children's Privacy Online | Hints & Tips | Attorney General California |

Goldstein (on the second page), offers some valuable tips for parents: (1) bone up on security, (2) secure connections, (3) do your homework, (4) understand privacy settings, (5) respect the child's privacy, which includes asking their consent and asking family and friends not to post photos of the child online. She also recommends monitoring the child's digital footprint. California's Attorney General (on the second page) advises discussing privacy with children before they go online and explaining why personal information is not to be divulged. Finally, he suggests surfing the Web with children initially to show them how to do this privately and safely. Both of these fall into Renaud & Prior's "mentor" category. Yet, parents might well not have continued to the second page, and missed these hints and guidelines, which Cutrell and Guan (2007) suggest is likely. They might also have been so overwhelmed by the number of results and all the law-related links on the first page and abandoned the search altogether.

Parental mediation strategies and interventions with children have been studied extensively with respect to media usage. The strategies are generally categorized as either active or regulated, with regulated being a more restrictive mediation and active being a more proactive and involved mediation (Nathanson 2001a; Nathanson 2001b; Miyazaki et al., 2009). Lwin et al. (2008) studied children's online privacy with mediation strategies that were further categorized into (1) laissez-faire – no mediation, (2) promotive – (high active/low regulated) (3) restrictive (low active/high regulated and (4) selective (high active/high regulated). The researchers found that overall active mediation was more effective. However, in cases where active mediation was non-existent or even low, safeguards resulted in a negative reaction from older teens and an increase in disclosure of information. Strong family social cohesion has been shown to reduce risky online behavior (Sasson & Mesch, 2014).

Research by Desimpelaere (2020) found that parents mainly had concerns around "stranger danger" situations (the "Contact" aspect of Byron's online harms). While undeniably significant, these violations are far less likely to occur than privacy violations related to data being improperly collected and/or leaked by institutions who violate online users' privacy invisibility, pervasively and seemingly with impunity.

The rules related to limiting time on a device are no longer adequate for keeping children safe online. It is essential that parents warn their children about the risks related to disclosure of sensitive information

(Lwin et al., 2008) and also that their information that may be tracked in the background during time spent online (Smith & Shade, 2018). As stated by Ciocchetti (2007), individuals provide personally identifiable information (PII) voluntarily without really knowing or understanding the risks. A multitude of risks exist such as data breach, identity theft, reputational damage, and/or financial damage. With these risks comes the responsibility to ensure that children can be online safely and with children's privacy protected (De Wolf & Vanden Abeele, 2020).

### *2.5 At what age should we start teaching privacy principles?*

There is evidence that when children that are taught skills to improve autonomy, they will likely be more skilled at making decisions to protect their privacy (Kumar et al., 2018). Youn (2009) also finds that early privacy-related education will result in a greater likelihood of self-protective privacy behaviors in later adolescent years. In fact, later year/older teen (ages 15-17) regulated (restricted) parental mediation has been shown to actually result in bypassing safeguards and an increase in information disclosure (Lwin et al., 2008). Fahlquist (2015) voiced concerns surrounding overuse of protective technologies and the reduction of children's freedom; which can inhibit growth as "*independent, creative, and responsible individuals*" (pg. 44). As stated by Fuchs (2021), restriction of technology is not the answer but rather helping children achieve balance and the necessary skills for appropriate media usage. While this is a complicated area of research to explore, it is important that both technical and nontechnical solutions be taken into consideration (Berson & Berson, 2006).

Differences in judgments, based on a specific context or actor and related to risks/benefits can also influence a privacy decision (Finkelhor et al., 2021). Building upon some of the prior privacy seminal papers and research, it is important that the concept of autonomy also be taken into consideration.

This suggests that privacy principles ought to be introduced at a young age, and then augmented as children age, while at the same time relaxing controls as they mature into adolescence (López de Ayala López et al., 2020). A one-size-fits-all-ages approach is clearly inappropriate in this space.

### *2.6 Summary*

We have reviewed the literature on children's privacy rights and discovered that the burden for assuring these is generally placed on parents' shoulders. Yet, in the same way as it takes a village to raise a child, we need everyone to help to assure the privacy of our children: this is a societal problem, not only something parents need to be concerned about. Because we care about vulnerable members of society, including children, we ought to take this responsibility seriously.

## 3 Related Research

Previous research into children's perceptions of privacy was frequently carried out with older children (12+), were limited to a small sample size (Stoilova et al., 2021; Adorjan and Ricciardelli, 2019), or didn't draw upon the vast and difficult to articulate literature surrounding privacy, information privacy, and online privacy. Sun et al. (2021) interviewed 26 children about their privacy perceptions and concludes that there should be better support to children so that they can reason more effectively about privacy-related decisions.

Studies such as Zhang-Kennedy & Chiasson (2016) explored younger children (age 7-9) and the use of an interactive e-book. The researchers found that children's knowledge of privacy was improved and retained, and parents were able to engage in discussions surrounding privacy. Kumar et al. (2017) found that, for privacy, the subjects (age 5-11) leaned on their parents for privacy support. Moreover, parents were likely to focus on the future rather than the present, in regards to privacy education.

Research by Zhao et al., (2019) explored aspects of explicit privacy awareness and risks – such as in-app pop ups, stranger danger, and in-game promotions – and implicit privacy awareness and risks – such as third-party tracking, promotions and recommendations based on online activities, and collection of personal data that can be used to drive decision-making. They found that the more obvious behavior such as oversharing and disclosing real identities were easier for children to articulate and be aware of versus tracking/promoting/recommendation-based aspects. These aspects may be easier to communicate first from a parental influence. Family rules/values/morals surrounding privacy can be influential factors in

providing children with guidance. Respect for privacy is also key to understanding privacy-related implications for youth/adolescents (Bauwens, 2020).

Children also have challenges understanding privacy risks related to both internal and third-party use (Desimpelaere et al., 2020). Research by Livingstone et al., (2019) found gaps in children's knowledge of institutional and commercial privacy in addition to data profiling. This is concerning due to the more ubiquitous practices surrounding data collection. While several of the current rules/guidelines set to address children's data privacy place the protective measures on the parent, children are frequently able to easily disclose personal information without parental knowledge or consent (Nairn & Monkgol, 2007).

If children are to become privacy literate, there is an assumption that they will know how to manage their own privacy (De Wolf & Vanden Abeele, 2020). This assumption is unlikely to be accurate, for a number of reasons. It can be particularly difficult for children under 11 to understand concepts of data privacy and related data collection (Zhao et al., 2019). In the second place, even with an understanding of privacy, children are unlikely to have the skills to action any understanding of their privacy rights, once again due to their tender years. Having the agency to claim their privacy rights may be challenging, especially when an adult in a position of authority is demanding disclosure. Given that many adults do not understand privacy, it seems unrealistic to expect children to have a nuanced understanding of this complex topic.

# 4 Methodology

The main aim of this research program is to understand parental influence on inculcating privacy awareness in their children. The current state of privacy protection mechanisms draws our attention to inadequacy of technologies, platforms, regulations, and human capacities to think and manage privacy. The review of literature highlights the complexities revolving around examination of privacy in terms of varied views on what privacy is, the dynamic and time shifting nature of privacy, understanding of what privacy values are, and how it can be protected to name a few.

Considering the mixed and inadequate understanding of this topic, this research finds itself in a relative novel area of research. Thus, an exploratory inquiry is warranted, which will focus on parents' own understanding of privacy and their communication with their children about privacy-related issues. In particular, the research questions we seek to explore, given our review of the literature:

**RQ1:** How do parents understand privacy in the context of digital technology?

**RQ2:** Who do parents believe is responsible for protecting children's digital privacy?

**RQ3:** How do parents believe children's digital privacy can be protected?

**RQ4:** How do parents act to teach privacy principles to their children, and to preserve their children's online privacy?

Because of the relatively unexplored nature of this research, few context-specific variables or theoretical structures are available. We will use both a semi-structured case study approach that follows the multiple-case methods (Yin, 1989) and the grounded approach suggested by Eisenhardt (Eisenhardt, 1989) using in-depth interviews. The strength of this qualitative approach lies in the depth of understanding it provides (Doty & Glick, 1998). Focus groups facilitate gathering information from a cross-section of the community of interest and collecting multiple points of view at one time and collective brainstorming, as a comment from one member can spark ideas in other members. In this study, we plan to undertake data collection through interviews, focus groups, and survey techniques that incorporate open ended questions and other brainstorming methods.

Considering the diverse views and behaviors related to privacy protection, prior research (Posey 2010) and (Posey et al. 2013) provides a guidance on employing methodology of qualitative and quantitative approaches to develop a taxonomy. These approaches integrate the classification techniques of multidimensional scaling (MDS), property fitting (ProFit), and cluster analyses.

A six step approach is recommended by (Posey et al. 2013):

**Step 1**: Behavior elicitation with initial in-depth review of the unique behaviors.

**Step 2**: Removal of Redundant Behaviors through Two New Sets of Expert Review

**Step 3**: Acquisition of Similarity Ratings through a Survey using panel service.

**Step 4**: Use of MDS to Determine the General Structure and Dimensionality of Perceptual Map

**Step 5:** Using ProFit Analysis to Label the Dimensions

**Step 6**: Using Cluster Analysis to Find Classes or Subgroups

***Step 1: Behavior elicitation with initial in-depth review of the unique behaviors.***

**Table 2: Research Step 1 Stages**

| | |
|---|---|
| 1 | Defining privacy in their own words (Open ended) |
| 2 | Scanning of the literature reveals that there are many different definitions of privacy, defined by academics, regulatory agencies, and privacy watchdog organizations –<br>Using a few prevalent definitions ask respondents to rank which one (most) closely fits.<br>Also ask respondents to tell how closely each definition fits their view of privacy |
| 3 | Regulations try to protect privacy rights (values) of their citizens – But what do they value?<br>Understanding underlying privacy values/principle of privacy<br>(ask opinions about which ones are most important)<br>Using online brainstorming techniques as the respondents to identify (/categorize) key words/tags<br>Asking respondents to draw a picture and upload |
| 4 | Regulations try to safeguard citizen privacy with set of (protection) principles (consumer code principles) -– ask opinions about importance of each of these principles<br>If a particular principle is not present in a regulation, how they feel about it. |
| 5 | Educating and Protecting Children's privacy: Ask if they have talked to their children about privacy Guidance (social media, phone, other) |

# 5 Discussion & Conclusion

While privacy is considered as a human right, topic of privacy is laden with many challenges. These stem from the lack of universally understood and accepted definition which then compromises the ability for people to understand privacy. This includes its multiple dimensions, the complexities around privacy related behaviors and the seeming paradox that emerges from the differences between generic and context specific privacy amongst other. When dealing with children's' privacy, these issues are compounded by development stages, age-related vulnerabilities and the unwitting privacy invasive actions of the adults in their lives. Bearing in mind that responsibility for teaching children about privacy usually falls on their parents' and carers' shoulders, this study proposes an exploratory inquiry of parental views on privacy, privacy values, and privacy guidance. Yet we reiterate, as we did in the abstract, that preserving the privacy of our children can only be preserved when the whole of society combat privacy violations and help parents to preserve their children's privacy.

# References


Acquisti, A., Brandimarte, L., and Loewenstein, G. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology* (30:4), pp. 736–758. (https://doi.org/10.1002/jcpy.1191).

Acquisti A, Grossklags J. What can behavioral economics teach us about privacy. In: Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, editors. *Digital privacy: theory, technology, and practices*. Auerbach Publications; 2007. pp. 363–77.

Adorjan, M. and Ricciardelli, R., 2019. A new privacy paradox? Youth agentic practices of privacy management despite "nothing to hide" online. *Canadian Review of Sociology/Revue canadienne de sociologie,* (56:1), pp.8-29.

Andrews, J.C., Walker, K.L., & Kees, J. 2020. Children and Online Privacy Protection: Empowerment from Cognitive Defense Strategies. *Journal of Public Policy & Marketing*. (39:2), pp. 205 – 219.

Barth, S., de Jong, M.D., Junger, M., Hartel, P.H., Roppelt, J.C. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics,* 41, 55–69.

Bauwens, J., Gabriels, K., and Mostmans, L. 2020. Navigating Online Privacy: A Family Environment Perspective on Children's Moral Principles. *Media and Communication*, (8:4), pp. 185 -196.

Bessant, C. 2017. Family privacy in the internet age: Family photographs as a case study. *PLSC Europe 2017* - Tilburg, The Netherlands

Bhamani, S., Makhdoom, A.Z., Bharuchi, V., Ali, N., Kaleem, S., & Ahmed, D. 2020. Home Learning in Times of COVID: Experiences of Parents. *Journal of Education and Educational Development,* (7:1), pp. 9 – 26.

Bott, G.J. and Renaud, K. 2018. June. Are 21st-century citizens grieving for their loss of privacy?. In *2018 Dewald Roode Workshop on Information Systems Security Research*. IFIP Working Group 8.11/11.13.

Bélanger, F. & Crossler, R.E. 2001. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly,* (35:4), pp. 1017 – 1041.

Bélanger, F., Crossler, R.E., Hiller, J.S., Park, J.M., Hsiao, M.S. 2013. POCKET: A Tool for Protecting Children's Privacy Online. *Decision Support Systems,* (54:2), pp. 1161 – 1173.

Bryan, K. Griffiths, S. and Ungoed-Thomas, J. 2020. *Revealed: betting firms use schools data on 28m children*. Retrieved 2 July 2021 from: https://www.thetimes.co.uk/article/revealed-betting-firms-use-schools-data-on-28m-children-dn37nwgd5

Buchanan, T., Paine, C., Joinson, A. N., and Reips, U.-D. 2007. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, (58:2), 157–165. doi:10.1002/asi.20459

Buckman, J. R., Bockstedt, J. C., and Hashim, M. J. 2019. "Relative Privacy Valuations Under Varying Disclosure Characteristics," *Information Systems Research*, (30:2), pp. 375–388. (https://doi.org/10.1287/isre.2018.0818).

Byron, T. 2008. *Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun*. Department for Children, Schools and Families. Retrieved 31 May 2020, from https://childcentre.info.

Ciocchetti, C. 2007. The Privacy Matrix. *Journal of Technology Law & Policy* (12), pp. 245 – 331.

Clarke, R. 1999. Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM,* (42:2), pp. 60 – 67.

Cranor, L-F., Balebako,R., Kurilova, D & Sleeper, M. 2014. *Privacy Illustrated Book Chapter*. http://studioforcreativeinquiry.org/projects/deep-lab

Cucinelli, G., Kozma, M., Arabuli, N. & Christiaans, J. 2015. Youth, media practices, and privacy: Working with high school teachers to co-create curriculum for better awareness and practice. In S. Carliner, C. Fulford & N. Ostashewski (Eds.), *Proceedings of EdMedia 2015--World Conference on Educational Media and Technology* (pp. 1965-1970). Montreal, Quebec, Canada: Association for the Advancement of Computing in Education (AACE). Retrieved July 3, 2021 from https://www.learntechlib.org/primary/p/173231/.

Cutrell, E. and Guan, Z. 2007. What are you looking for? An eye-tracking study of information usage in web search, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, San Jose, California, pp. 407–416.

De Wolf, R., Vanden Abeele, M.M.P. 2020. Editorial: Children's Voices on Privacy Management and Data Responsibilization. *Media and Communications,* (8:4), pp. 158 – 162.
DeCew J. 2018. Privacy. *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition).
Desimpelaiere, L., Hudders, L., & Van de Sompel, D. 2020. Childrens' and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. *Media and Communication,* (8:4), pp. 163 – 174.
Dienlin, T., Trepte, S. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology* (45:3), pp. 285–297.
Diggelmann, O., Cleis, M.N. 2014. How the right to privacy became a human right. *Human Rights Law Review,* (14:3), pp. 441–458.
Doty, D. H., & Glick, W. H. 1998. Common methods bias: Does common methods variance really bias results? *Organizational Research Methods*, (1:4), pp. 374-406.
Eisenhardt, K. M. 1989. Building theories from case study research. *Academy of Management Review,* 14(4), 532–550.
Equality and Human Rights Commission: *Article 8: Respect for your private and family life* (2021), retrieved 19 June from: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life
Fahlquist, J.N. 2015. Responsibility and Privacy – Ethical Aspects of Using GPS to Track Children. *Children & Society,* (29), pp. 38 – 47.
Finkelhor, D., Jones, L., & Mitchell, K. 2021. Teaching Privacy: A Flawed Strategy for Children's Online Safety, *Child Abuse & Neglect,* (117:3), pp. 1-6.
Finn R.L. & Wright D. & Friedewald M. 2013. Seven types of privacy. *European Data Protection*, 3-32
Foster, S.P. 2000. The Digital Divide: Some Reflections. *International Information & Library Review,* (32:3-4), pp. 437 – 451.
Fried C. 1968. Privacy. *Yale Law Journal*, 77(3), 475- 493.
Fuchs, M. 2021. Problematic Technology Use Needs to be Tackled so that Children and Adolescents Can Reap Positive Benefits During the COVID-19 Pandemic. *ACTA Paediatrica*, 110, pp. 1401 – 1402.
Gavison R. 1980. Privacy and the limits of law. *Yale Law Journal*, 89(3), 421-471
Gerber, N., Gerber, P., and Volkamer, M. 2018. "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior," *Computers & Security*, (77), pp. 226–261. (https://doi.org/10.1016/j.cose.2018.04.002).
Gerety T. 1977. Redefining privacy. *Harvard Civil Rights-Civil Liberties Law Review*, 12(2), 233-296
Gligorijević, J., 2019. Children's privacy: The role of parental control and consent. *Human Rights Law Review,* (19:2), pp.201-229.
Goldstein. (undated). I'm a Mom and a Children's Privacy Lawyer: Here's What I Do and Don't Post About My Kid Online. Retrieved 3 July from: https://www.parents.com/kids/safety/internet/im-a-mom-and-childrens-privacy-lawyer-what-i-do-and-dont-post-online/
Gross, H., 1967. The concept of privacy. *NYUL Rev*., (4), pp. 34-54.
Hart, H.L.A. 1954. "Definition and theory in jurisprudence", *Law Quarterly Review*, (70:277), pp. 37-60.
Information Commissioner. 2018. *Children*. https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/children/
Jozani, M., Ayaburi, E., Ko, M., Choo, K.K.R. 2020. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior,* (107), pp. 106260.
Kafka, P. 2019. *The US government isn't ready to regulate the internet. Today's Google fine shows why*. Retrieved 3 July 2021 from: https://www.vox.com/recode/2019/9/4/20849143/youtube-google-ftc-kids-settlement-170-million-coppa-privacy-regulation
Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security,* (64), pp. 122–134.
Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L., & Vitak, J. 2017. 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *PACM on Human-Computer Interaction,* (1:64), pp. 1-21.
Kumar, P., Vitak, J., Chetty, M., Clegg, T.L., Yang, J., McNally, B., & Bonsignore, E. 2018. Co-Designing Online Privacy-Related Games and Stories with Children. *IDC,* June 19-22, Trondheim, Norway.
Leino-Kilpi H. & Valimaki M. & Dassen T. & Gasull M. & Lemonidou C. & Scott A. & Arndt M. 2001. Privacy: A review of the literature. *International Journal of Nursing Studies*, (38:6), pp. 663-671
Li, H., Luo, X.R., Zhang, J., Xu, H. 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management,* (54:8), pp. 1012–1022.

Livingstone, S., Stoilova, M., & Nandagiri, R. 2019. *Talking to Children About Data and Privacy Online: Research Methodology*. London: London School of Economics and Political Science.

López de Ayala López, M.C., Haddon, Leslie, Catalina-García, B. and Martínez-Pastor, E. 2020. The dilemmas of parental mediation: continuities from parenting in general. *OBServatorio* (OBS*), (14:4), pp. 119 - 134. ISSN 1646-5954

Lwin, M.O., Stanaland, A.J.S., & Miyazaki, A.D. 2008. Protecting Children's Privacy Online: How Parental Mediation Strategies Affect Website Safeguard Effectiveness. *Journal of Retailing,* (84:2), pp. 205 – 217.

MacLeod, C.L. 2007. Raising Children: Who is Responsible for What? In *Taking Responsibility for Children.* Brennan, Samantha., and Robert Noggle (Eds.). Waterloo, Ont: Wilfrid Laurier University Press. pp. 1 – 17.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," Information Systems Research (15:4), pp. 336–355. (https://doi.org/10.1287/isre.1040.0032).

Maqsood, S. and Chiasson, S. 2021. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-17).

Miltgen, C.L. & Smith, H.J. 2015. Exploring Information Privacy Regulation, Risks, Trust, and Behavior. *Information & Management,* (52:6), pp. 741 – 759.

Miyazaki, A.D., Stanaland, A.J.S., & Lwin, M.O. 2009. Self-Regulatory Safeguards and the Online Privacy of Preteen Children. *Journal of Advertising, (*38:4), pp. 79 – 91.

Moor J.H. & Tavani H.T. 2001. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *ACM SIGCAS Computers and Society*, (31:1), pp. 6-11.

Morelli, A. (undated). Children's Need for Privacy. Retrieved 3 July 2021 from: https://www.gracepointwellness.org/1262-child-development-parenting-middle-8-11/article/38377-childrens-need-for-privacy

Nairn, A. & Monkgol, D. 2007. Children and Privacy Online. *Journal of Direct, Data, and Digital Marketing Practice,* (8:4), pp. 294 – 308.

Nathanson, A.I. 2001a. Parent and Child Perspectives on the Presence and Meaning of Parental Television Mediation. *Journal of Broadcasting and Electronic Media,* 45(Spring), pp. 201 – 220.

Nathanson, A.I. 2001b. Mediation of Children's Television Viewing: Working Toward Conceptual Clarity and Common Understanding. In *Communication Yearbook,* Vol 25, William B. Grudykunst (Ed.), Hillsdale, NJ: Lawrence Erlbaum, pp. 115 – 151.

Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T. 2007. Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'. *Human-Computer Studies* (65:6), pp. 526 – 536.

Parent W.A. 1983. Privacy, morality, and the law. *Philosophy & Public Affairs*, (12:4), pp. 269-288

Pavlou, P.A. 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly,* (35:4), pp. 977 – 988.

Posey, C., Roberts, T., Lowry, P.B., Bennett, B. and Courtney, J. 2010, October. Insiders' Protection of Organizational Information Assets: A Multidimensional Scaling Study of Protection-Motivated Behaviors. In *Dewald Roode Workshop on IS Security Research, Boston, MA, USA*.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly,* (37:4), pp. 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09.

Posner R.A. 1978. The right of privacy. *Sibley Lecture Series*. 22.

Post, R.C. 2000. Three concepts of privacy. *Georgetown Law Journal*, (89), pp. 2087-2098.

Privacy Illustrated. 2014. https://cups.cs.cmu.edu/privacyillustrated/

Radesky J., Chassiakos, Y., Ameenuddin, L.R., Navsaria, D. 2020. AAP COUNCIL ON COMMUNICATION AND MEDIA. Digital Advertising to Children. Pediatrics, (146:1), pp. 1-8.

Ravi, A., Agha, Z., Chatlani, N., & Wisniewski, P. 2020. Privacy Challenges for Adolescents as a Vulnerable Population. *Networked Privacy Workshop of the 2020 CHI Conference on Human Factors in Computing Systems,* April 26.

Renaud, K., Flowerday, S., English, R. and Volkamer, M. 2016. Why don't UK citizens protest against privacy-invading dragnet surveillance? *Information & Computer Security*, (24:4), pp. 400-415.

Renaud, K. and Prior, S., 2021. The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor. *Information & Computer Security*. To appear. https://doi.org/10.1108/ICS-07-2020-0115
Richtel, M. 2021. Children's Screen Time has Soared in the Pandemic, Alarming Parents and Researchers. *New York Times,* January 16.
Rumbold, B. & Wilson, J. (2019). Privacy Rights and Public Information. *The Journal of Political Philosophy*, (27:1), pp. 3-25.
Sasson, H. & Mesch, G. 2014. Parental Mediation, Peer Norms, and Risky Online Behavior Among Adolescents. *Computers in Human Behavior,* (33), pp. 32 – 38.
Sella-Villa, D. 2020/2021. An Early Evaluation of the Privacy Impacts of the COVID-19 Pandemic. *The Business Lawyer*, (76:1), pp. 261 – 267.
Shmueli, B. and Blecher-Prigat, A. 2010. Privacy for children. Colum. *Hum. Rts. L. Rev*., (42), pp. 759.
Short, J.L. and Toffel, M.W., 2007. The Causes and Consequences of Industry Self-Policing. HBS *Technology & Operations Mgt. Unit Research Paper*, (08-021).
Smith, H.J., Dinev, T., & Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly,* (35:4), pp. 989 – 1015.
Smith, K.L. & Shade, L.R. 2018. Children's Digital Playgrounds as Data Assemblages: Problematics of Privacy, Personalization, and Promotional Culture. *Big Data & Society,* (5:2), pp. 1 – 12.
Solove D.J. 2002. Conceptualizing Privacy. *California Law Review*, (90:4), pp. 1087-1155.
Solove D.J. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, (154:3), pp. 477-564
Solove D.J. 2010. *Understanding Privacy*. Harvard University Press
Solove, D. 2014. *10 Reasons Why Privacy Matters*. Retrieved 28 June 2021 from: https://teachprivacy.com/10-reasons-privacy-matters/
Solove, D.J. 2020. The myth of the privacy paradox. Geo. Wash. L. Rev. (89), pp. 1–46.
Sorensen, S., 2016. Protecting Children's Right to Privacy in the Digital Age: Parents as Trustees of Children's Rights. *Child. Legal Rts. J*., (36), pp. 156-176.
Stoilova, S., Nandagiri, R., & Livingstone, S. 2021. Children's Understanding of Personal Data and Privacy Online – A Systematic Evidence Mapping. *Information, Communication, & Society* (24:4), pp. 557–575.
Subrahmanyam, K. and Greenfield, P. 2008. Online Communication and Adolescent Relationships. *The Future of Children,* (18:1), pp. 119–146.
Steeves, V. and Webster, C. 2008. Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society,* (28:1), pp. 4-19.
Steinberg, S.B. 2016. Sharenting: Children's privacy in the age of social media. *Emory LJ*, (66), p.839.
Sun, K., Sugatan, C., Afnan, T., Simon, H., Gelman, S.A., Radesky, J. and Schaub, F. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-34).
Tahaei, M. and Vaniea, K. 2021, May. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-11).
Thomson, J.J. 1975. The right to privacy. *Philosophy & Public Affairs*, (4:4), pp. 295-314.
Todres, J. 2009. Family Integrity and Children's Rights A UN Convention. *Faculty Publications by Year*. (36:6), pp. 20.
Tuttle R.W. 1999. Reviving privacy. *George Washington Law Review*, (67:5), pp. 1183-1196.
United Nations. Undated. *The Convention on the Rights of the Child: The children's version*. Retrieved 28 June 2021 from: https://www.unicef.org/child-rights-convention/convention-text-childrens-version
Urban, J.M. and Hoofnagle, C.J., 2014. July. The privacy pragmatic as privacy vulnerable. In *Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS)*.
Volf, S. 2019. *Earl Restaurants Data Breach Affects Many*. Retrieved 3 July 2021 from: https://www.secureforensics.com/blog/disney-springs-data-breach
Vosloo, S., Penagos, M., & Raftree, L. 2020. *COVID-19 and Children's Digital Privacy*. UNICEF Office for Global Insight and Policy. Retrieved June 28, 2021 from https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy.
Warren S.D. & Brandeis L.D. 1890. The right to privacy. *Harvard Law Review*, (4:5), pp. 193-220.
Westin, A. F. 1968. Privacy and freedom. *Washington and Lee Law Review*, (25:1), pp. 166–170.

Willett, R. 2021. 'In our family, we don't watch those things': parents' discursive constructions of decision-making connected with family media practices, *Journal of Family Studies,* pp. 1 – 16.
Wodinsky, S. 2021. 60% of School Apps Are Sharing Your Kids' Data With Third Parties. Retrieved 1 July 2021 from: https://gizmodo.com/60-of-school-apps-are-sharing-your-kids-data-with-thir-1846819024
Wolfe, M., 1978. Childhood and privacy. In *Children and the Environment* (pp. 175-222). Springer, Boston, MA.
Yao, M.Z., Rice, R.E., & Wallis, K. 2007. Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science and Technology,* (58:5), pp. 710 – 722.
Yin, R. K. 1989. *Case study research – design and methods*. Newbury Park: Sage Publications Inc.
Youn, S. 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs,* (43:3), pp. 389 -418.
Zhang-Kennedy, L. & Chiasson, S. 2016. Teaching With an Interactive E-book to Improve Children's Online Privacy Knowledge. *IDC 2016,* June 21–24, Manchester, U.K.
Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Kleek, M.V., & Shadbolt, N. 2019. 'I Make Up a Silly Name': Understanding Children's Perception of Privacy Risks Online. *CHI 2019 Glasgow, Scotland,* May 4-9, pp. 1–13

# Appendix A

**Table 2. Privacy Definitions from the Research Literature**

| Author/ Citation | Views on Privacy |
|---|---|
| Warren & Brandeis (1890). | Privacy is defined as the right to being let alone. It indicates the need for law to protect the right for thoughts, emotions, and sensations where expressed in writing, in conduct, in conversation, in attitudes, or in facial expression. The right to privacy will however cease when the facts are published with the individual's consent. |
| Gross (1967). | Privacy is the condition of human life in which acquaintance with a person or with affairs of a person's life which are personal to are limited. Privacy is also related with the Bill of Rights. |
| Fried (1968). | Privacy is needed not from the perspective of law to protect the information, but it is an essential element in our culture to build respect, love, friendship, and trust in society. Privacy is a control of private information, where friendship implies a voluntary relinquishment of private information about others because we would not want to know something our friends are not willing to share with us. Viewpoint that love and friendship involve the initial respect for the rights of others. |
| Gerety (1977). | Privacy is an autonomy or control over the intimates of personal identity. Privacy derives value by attaching to the possibility of the conditions it protects instead of creating its own significance. An invasion of privacy is defined as deprived of control over the intimacies of our bodies and minds as to offend what are ultimately shared standards of autonomy. |
| Posner (1978). | Privacy viewed as the withholding or concealment of information. The economic interest of privacy is discuseed in terms of "privacy" and "prying". The essential elements of a legal right of privacy based on economic efficiency are: (1) the protection of trade and business secrets by which businessmen exploit their superior knowledge or skills, (2) generally no protection for facts about people, and (3) the limitation of eavesdropping and other forms of intrusive surveillance to surveillance of illegal activities. |
| Gavison (1980). | Privacy should be discussed in two types of questions (1)Status of the term, and (2) The characteristics of privacy. The three elements related to privacy are secrecy, anonymity, and solitude. Privacy can be described as the information known about an individual, attention paid to an individual, and the physical access to an individual. Legal protection is limited as law cannot compensate for losses of privacy, and law is committed to other ideals that sometimes override the concern for privacy. Thus, we cannot expect law to fully or adequately protect our privacy in our lives. |

**Table 2. Privacy Definitions from the Research Literature**

| Author/ Citation | Views on Privacy |
|---|---|
| Parent W (1983). | Privacy defined as the condition of not having undocumented personal knowledge about one possessed by others. Definitions of privacy in terms of control should be jettisoned - because people can and do choose to give up privacy for many reasons. An adequate conception of privacy must allow for this fact; control definitions do not. |
| Tuttle (1999). | Views of expressivist individualism - one among many visions - each with its own viewpoint and own legitimate claim of culture is permitted as long as others' views are not excluded. |
| Leino-Kilpi et al. (2001). | View the concept of privacy as expressed in four dimensions: physical, psychological, social, and information privacy. |
| Moor & Tavani (2001). | Authors oppose the use of control of information to conceptualize privacy and suggest to understand the concept in terms of a theory of restricted access. For example, if a citizen surrenders his/her information to government for tax purposes, it does not mean that one gave up privacy of his/her personal information. |
| Post (2001). | Three concepts of privacy: (1) Privacy to the creation of knowledge; (2) privacy to the creation of dignity; (3) privacy to the creation of freedom Privacy blocks the flow of information to avoid error and misrepresentation. Privacy as dignity suggested the mutuality of social life and the invasion of privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect. Privacy as freedom suggests the differences in social life and people are autonomous and self-defining. Privacy as dignity safeguards the socialized aspects of the self; privacy as freedom safeguards the spontaneous, independent, and uniquely individual aspects of the self. Privacy as dignity seeks to eliminate differences by bringing all persons within the bounds of a single normalized community; privacy as freedom protects individual autonomy by nullifying the reach of that community. |
| Solove (2002). | Views the method of conceptualizing privacy thus far to be problematic and unsatisfying. Uses a pragmatic approach to conceptualizing privacy in a bottom up way, and locates the starting point for theorizing in specific contexts, including social practices, historical development of privacy practices, and privacy and technological and social change. |
| Solove (2006). | Privacy is a concept in disarray. It is too vague to guide adjudication and lawmaking. Privacy disruptions (categorized into information collection, information processing, information dissemination, and invasion). Each of these categories have different privacy harming activities which are different from one another and yet share important similarities - which allows us to see privacy in a different way. |
| Solove (2010). | Privacy is a concept in disarray - it is a sweeping concept that includes many different aspects. Thus, it is difficult to conceptualize privacy. There are a number of theories about privacy, but the criticisms mostly claims that the theories are too narrow, too broad, or too vague. Also, some theorist claim that privacy can be socially detrimental. Privacy is a fundamental right, essential for freedom democracy, psychological well-being, individuality, and creativity. It is proclaimed inviolable but decried as detrimental, antisocial, and even pathological. |
| Finn et al. (2013). | Define privacy in seven aspects: (1) privacy of the person, (2) privacy of behavior and action, (3) privacy of communication, (4) privacy of data and image, (5) privacy of thoughts and feelings, (6) privacy of location and space, (7) privacy of association. |
| DeCew (2018). | Privacy is cross-species and cross-cultural. It is not an absolute value and should be viewed as the default. Invasion of privacy can be broadly invaded. Privacy must be protected now; particularly related to modern technology/changes. |
| Rumbold & Wilson (2019). | Focus on how right-holders manage their rights within different domains. Specifically, when right-holders have or hold rights or what waives them.<br>Updated from prior views to bring in aspects of publicly available data; that a violation of privacy could occur if the activity threatens information an individual intended to keep private. |