Special Issue: Comparative Approaches to Studying Privacy: Opening Up New Perspectives

SM+S
social media + society

Social Media + Society
October-December 2024: 1–14

DOI: 10.1177/20563051241298042
journals.sagepub.com/home/sms
Sage

Online Privacy, Young People, and Datafication: Different Perceptions About Online Privacy Across Antigua & Barbuda, Australia, Ghana, and Slovenia

Rys Farthing[1], Katja Koren Ošljak[2], Teki Akuetteh[3], Kadian Camacho[4], Genevieve Smith-Nunes[5], and Jun Zhao[6]

Abstract

Children and young people's online privacy is increasingly challenged by the datafication of the digital world, and this is an increasingly important area of policy concern. Understanding what young people understand online privacy to be, and what they want done to protect it, is key to creating effective and rights-realizing policy responses. This article explores young people's perceptions across four countries and finds they have nuanced understandings about online privacy and clear, robust ideas about how to improve it. Context mattered, and their online privacy concerns and ideal protections were often informed by their socio-political context and awareness of and trust in datafication.

Keywords

young people, children, privacy, policy, datafication

Introduction

The experience of growing up today is imbued with digital technologies in ways that previous generations could have only imagined. Digital technologies provide access to vital education, socialization, participation, wellbeing, and entertainment opportunities. Young people's rights are now realized — or violated — as much in the digital world as they are in the analogue world.

Young People's Online Privacy and Datafication

This rapid adoption and increasing reliance on the online world have raised concerns about the effects on children and young people's online privacy and digital experiences (Livingstone & Third, 2017; Mascheroni, 2018). Children and young people's digital experiences are pervasively and aggressively recorded, tracked, aggregated, analyzed, and exploited by many commercial digital products (Zuboff, 2015). This is often described as the "datafication" of childhood (Barassi, 2020).

Datafication is an extremely common experience (Wang et al., 2022). Barassi (2020), for example, describes how children are now datafied even before they are born through the collection and harvesting of pre-natal data from parents; Mascheroni (2020) describes how this datafication continues right throughout childhood, through, for example, the use of connected baby devices and toys; and Jarke and Breiter (2019) describe how these practices continue in school through digital teaching tools.

Datafication can be a privacy harm in itself. It violates young people's reasonable expectations to be let alone and right to be free from arbitrary interference with their privacy (United Nations [UN] General Assembly, 1989). But subsequent uses of this data create additional risks to children's autonomy and safety, such as fuelling potentially harmful products (Twenge et al., 2020); enabling the delivery of potentially harmful content through content recommender

[1]Reset Tech, Australia
[2]University of Ljubljana, Slovenia
[3]Africa Digital Rights' Hub, Ghana
[4]University of West Indies, Antigua and Barbuda
[5]University of Roehampton, UK
[6]University of Oxford, UK

Corresponding Author:
Rys Farthing. Reset Tech, Australia. NSW 2000.
Email: rys@au.reset.tech

algorithms (e.g., see the study by Harriger et al., 2022); and enabling inappropriate or potentially manipulative behavioral advertising (Nairn & Fine, 2008; Verdoodt et al., 2016), leading to harm through automated decision-making (Willson, 2019).

The invisibility and frequency of datafication practices—the gathering, computation, and sharing and selling people's online data—may have become normalized and taken-for-granted conditions (Mascheroni & Siibak, 2021; van Dijck, 2014). The normalization of datafication could affect young people's understandings and expectations of privacy. In a context where datafication en masse is widely expected and normalized, it becomes challenging to anticipate privacy as it has traditionally been understood.

Datafication may be especially normalized among children and young people for two reasons. First, by virtue of their emerging capacities, young people might not have critically reflected on digital privacy concerns; they may still be developing the "citizen agency" (Kennedy et al., 2015) necessary to do so. Further complicating the matter, today's children and young people have grown up datafied from before birth (Barassi, 2020). They have not experienced a world without everyday datafication. Thus, young people's perspectives about online privacy may be profoundly different to older people's perspectives.

Three comparative factors surface in the literature as potentially important in understanding the normalization of datafication among the young. First, the level of datafication itself may be important, as young people's experience with datafication may be culture-dependent. Second, young people's awareness of datafication may differ depending on their levels of digital literacy and "citizen agency," and finally, young people's trust in datafication. Datafication can appear normalized under conditions of trust (van Dijck, 2014). Yet, there is limited understanding of how the cultural and sociopolitical context may influence the way young people perceive datafication.

Online Privacy Policy and Young People

A growing "techlash" has challenged trust in digital actors over recent years (Weiss-Blatt, 2021), encouraging a range of different social and political responses. Many of these attempts aim to counter datafication with a range of individually-focused privacy initiatives, such as advances in critical media curriculum (e.g., Bernd et al., 2015 or Zeichner, 2019) or attempts to improve young people's online privacy skills (Wang et al., 2023). Many also attempt to mitigate the impact of datafication through regulation and legislation.

Regulations and legislations aiming to improve children's online privacy are being implemented across multiple jurisdictions. Some are international initiatives, such as the UN's General Comment (UN Committee on the Rights of the Child, 2021), while others are supra-national, such as the European Union (EU) Better internet for Kids+strategy (European Commission, 2022); national, such as Australia's proposed Children's Online Privacy Code (Australian Attorney General's Office, 2023); or state-based, such as California's Age Appropriate Design Code (State of California, 2022).

These recent policy attempts to improve children's online privacy rest on a body of regulation already in place. This includes the EU's GDPR-K (the special protections for children's data within the General Data Protection Regulation), which affords European children some additional protections (European Union [EU], 2016), and the United States' (US's) Child Online Privacy Protection Act (COPPA) (US, 1998) which provides some protections for children under 13 years of age for example.

Many of these new regulations and legislation have only recently been implemented or are yet to be implemented, and evidence shows that compliance with older existing legislation has been patchy (Irish Council for Civil Liberties, 2023; Sirur et al., 2018), leaving children largely facing datafied childhoods.

Young People's Perceptions and Expectations

Understanding young people's perceptions of datafication, privacy and ideal privacy solutions is an important part of developing effective policy responses—especially understanding how these perceptions may vary across contexts (e.g., media contexts or national/(sub-)cultures) and what this means for domestic policy. Indeed, the engagement of young people has been a cornerstone in the development of various legislations related to children, such as Ireland (Data Protection Commission, 2019) and the UK (Information Commissioner's Office [ICO] and Revealing Reality, 2019). Realizing young people's rights to be heard in these emerging and imminent policy debates is also a democratic imperative across the globe Hartung (2020).

There is increased research interest related to how children perceive their data privacy online, and many studies have shown that children and young people understand and value their privacy as a concept (Livingstone et al., 2019; Third & Moody, 2021; Wang et al., 2022). Some studies find that while valued, young people may struggle to understand the "harms" from privacy incursions. For example, research has found that young people struggle to describe potential negative consequences that may emerge from personal data collection, use, or inference (Mandell & Farthing, 2023; Sefton-Green et al., 2022; Stoilova et al., 2020) and to conceptualize the potential risks around how data might shape their future experiences and behavior (Acker & Bowler, 2017; Pangrazio & Selwyn, 2017). Research has also found that young people's perceptions of privacy are sensitive to the different actors involved in their privacy (Third & Moody, 2021)—be they commercial actors, civil society organizations, or public institutions, such as their schools—but that these understandings may be incomplete (Bowler et al., 2017; Kumar et al., 2017). (We note that this may also be true for adults in general.) Confounding this however, there is an acknowledged research gap when it comes to exploring

	Antigua & Barbuda	*Australia*	*Ghana*	*Slovenia*
Development of national privacy regulation	Emerging conversation among civil society and within the civil service	Anticipate a review of privacy regulations—specifically the *Privacy Act*	Emerging conversation between civil society and regulators	Anticipate a review of privacy regulations —specifically the European Data Protection Board's Guidance on children's data
Socioeconomic status (OECD)	Upper-middle income	High-income Category I	Lower-middle income	High-income Category I
Geographical location	North America (Caribbean)	Asia Pacific (Australia)	Africa (West)	Europe (Central)

Figure 1. Research sites selection; the socioeconomic status is based on OECD (2022).

young people's perceptions about data collection and use in commercial contexts (Stoilova et al., 2021).

Much of the research exploring young people's perspectives of privacy has been carried out with children from Western, Educated, Industrial, Rich, Democratic (WEIRD) countries. Studies about how datafication is perceived by children from non-WEIRD countries are scarce. This limitation could potentially limit the effectiveness of global regulatory initiatives. Recent research has shown that children from different cultural and social political contexts could exhibit different approaches toward data ownership and privacy incursions. For example, a recent study with UK and Chinese young children has identified that Chinese children are more likely to take a more pragmatic stance while children from the UK exhibited higher demand for data autonomy (Zhou et al., 2023). Similarly, international research exploring young people's perceptions about their rights in relation to the digital environment noted regional variations, especially around privacy (Third & Moody, 2021). While privacy was widely valued, understandings differed. For example, "children in high-income countries such as Canada and New Zealand tended to demonstrate a higher level of privacy literacy than those in low-income countries, though not exclusively nor uniformly," and higher levels of concerns around commercial actors' use of personal information (Third & Moody, 2021).

Within WEIRD contexts too, children's perceptions about online privacy have been found to vary. For example, a Europe-wide study found variations in children's self-reported experiences of "data misuses," such as "using personal information in a way children do not like," across Europe (Smahel et al., 2020).

Research Questions

We recognize that having a deeper understanding about how children and young people recognize and problematise the implications associated with datafication is crucial for informing effective legislative and regulative agendas. Furthermore, these agendas need to be sensitive to domestic context where regulation may be implemented in practice, as well as the global context that unites many of the experiences of online privacy in principle. This research aims to address these challenges by exploring:

- How young people define privacy;
- To what extent young people problematise their online privacy, with a particular focus on datafication and commercial relationship, and;
- What changes young people want to see to improve their online privacy.

This article makes a critical contribution to our understanding of these issues by taking a comparative perspective and focuses on identifying the importance of social and political context for us to consider datafication in shaping young people's perspectives about online privacy and privacy protections.

Methods

This research used mixed methods to unpack young people's perceptions of online privacy and adopted both design-based (Crippen & Brown, 2018) and action-research (McNiff, 2017) techniques. Young people's perspectives on privacy and privacy protections were investigated in four real-world settings, Antigua & Barbuda, Australia, Ghana, and Slovenia, using focus groups and surveys, and participants (aged 10–18 years) then engaged with change-making policy discussions as part of the research process.

Sites were selected to allow for insightful comparative analysis and to maximize potential policy relevance in the action phase. Countries where relevant policy dialogues were active or emerging were long-listed, including, for example, countries anticipating a review of children's privacy or related regulations (such as Australia, Slovenia via the EU, various US States, Canada, etc.) or emerging conversation among civil society and/or policy-makers about potential reforms (such as Antigua & Barbuda, Ghana, South Africa, Turkey, etc.). The long list was narrowed down to maintain geographic diversity; including countries from the global North and the global South, both hemispheres, different continents, and both WEIRD and non-WEIRD countries (Figure 1). This study

received ethical approval from the Reset.Tech internal ethics review process on January 10, 2022.

A series of deliberative focus groups with young people aged 10–18 years and a survey of additional young people aged 10–18 years was held at each site. These were adapted to meet the needs of each context, including methods that might maximize relevance to domestic policy-makers (such as requiring large-scale research to inform policy development at an EU level, versus more facilitated focus groups helpful to the civil service in Antigua & Barbuda), and to accommodate different local restrictions (such as location availability, school days vs. holidays, availability of survey partners, etc.).

Embracing this variability was a principled decision. Learning from design-based research principles, this research aimed to focus on the requirements of each domestic context and the participants themselves (Crippen & Brown, 2018). This research did not attempt to replicate the same research methods across four sites, rather we set out instead to answer the same research questions in an adaptive and responsive way in four sites. The focus was less on generating "generalisations" but to instead focus on the "particular" (Bertelsen et al., 2018). This variability complicates methods and analysis, and this is addressed below. However, embracing variability allowed us to create meaningful engagement with young people in different circumstances, produce domestically relevant research, and maintain our ability to consistently address core research questions.

In total, in:

- **Antigua & Barbuda**: a hybrid focus group was held with 42 young people aged 13–15 years in St John's, over 2 days in Saint John's (and online from Codrington). This was supplemented by survey data of 55 additional young people aged 13–18 years across the twin-islands;
- **Australia**: a day-long focus group was held with 12 young people in Sydney, followed up with 2-hour-long online meetings. This was supplemented by 5-hour-long depth interviews from young people from other cities and regions too far from Sydney to enable attendance and a survey of 506 children aged 16 and 17 years from across Australia undertaken by a commercial polling company;
- **Ghana**: a day-long focus group was held with 21 young people aged 13–17 years in Accra. This was supplemented by a survey of 101 additional young people shared through schools across the country;
- **Slovenia**: In excess of 200 hour-long focus groups were held, with more than 15,000 young people aged 11–17 years attending. This happened in conjunction with the release of a popular Slovenian language teen-movie Gaja's World 2, which helped attract significant numbers. This was supplemented by a survey of 948 young people aged 14–18 years, led by the University of Ljubljana.

Describing the detailed session plans of each activity used in the focus groups is not possible within the space allowed, especially given the variation, so we have published them online for researchers to access. As an overview, each focus group followed four sequential phases (see Figure 2 also):

1. Exploring and discussing young people's data footprint. Following an ice-breaker and warm up activity, each group collectively brainstormed the types of personal data they believed were collected about young people by existing online platforms. Participants were then encouraged to unpack who they believed these data were accessible to. Information about what data participants believed was being collected, and which actors accessed it was then used as a prompt to open up discussions about the levels of comfort or discomfort participants felt around online privacy.
2. Deliberations about the acceptability of these data flows, and discussions about whether young people felt these data processes and processors were trustworthy. Following this exploration session, each group developed a definition of privacy that related to their online experiences. Using this definition as a prompt, groups then discussed whether they felt they were private online or not, and if they trusted those involved in the data flow.
3. Developing a list of guiding principles for protecting young people's privacy. As a whole group, participants discussed what they wanted to happen about their online privacy, addressing any gaps or issues identified in Phase 2. This broad discussion moved on to a process of attempting to state their specific desires in the form of 'dos and don'ts.' Groups were provided with a set of 10 or so 'dos and don'ts' prompt cards to start this process. Building on the principles of co-design (e.g., Bevan Jones et al., 2020), these prompt cards included suggestions that young people had made in the surveys and/or in other research sites. The groups then worked to flesh out their own extensive lists of 'dos and don'ts' (see examples in Figure 3). This first long list of 'dos and don'ts' was refined into a collated list of principles by the young people (or in Slovenia, the researchers).
4. A small action-research phase, where young participants were supported to share their thoughts and privacy principles with relevant decision-makers. Young people brainstormed who they might want to share their guiding principles with. These discussions were also deliberative and informed by the facilitators' suggestions around policy possibilities in each location (i.e., if there was a regulatory review coming up, or who might be "responsible" for what change). Due to the pace of the Slovenian workshops, young people were simply offered the opportunity to connect

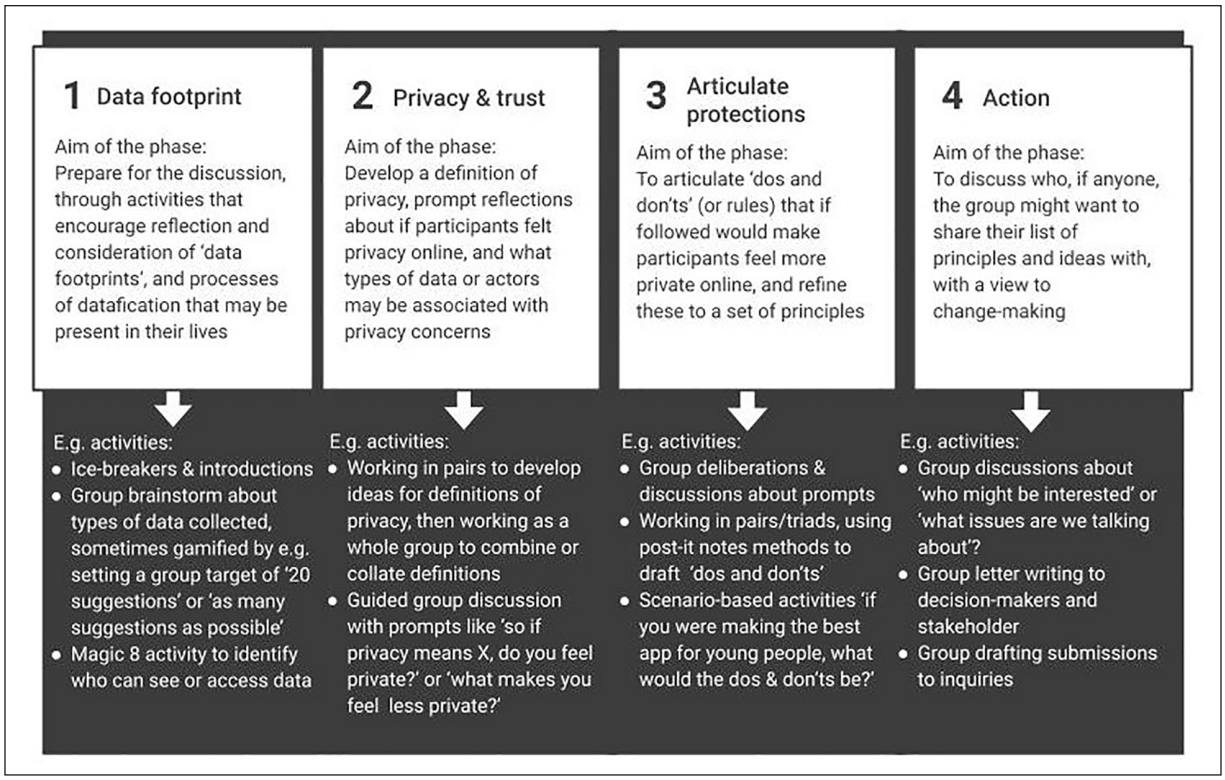

Figure 2. A diagrammatic representation of the research phases.

with decision-makers via an upcoming consultation if they wanted. Young people were supported to undertake the actions they deliberated and decided on, leading to:

5. Antigua & Barbuda: participants gave a list of suggestions to teachers about things they believe young people should be taught about privacy and called for the publication of a "magazine" about the issue for decision-makers (which researchers then published and distributed);
6. Australia: participants wrote a submission to a government inquiry and gave oral evidence to a government department about Australia's privacy law review;
7. Ghana: participants wrote a letter to multiple stakeholders they identified, sharing their guiding principles;
8. Slovenia: participants' privacy principles were sent to relevant regulators and ministers and will be sent to the EU regulators inquiry when it opens.

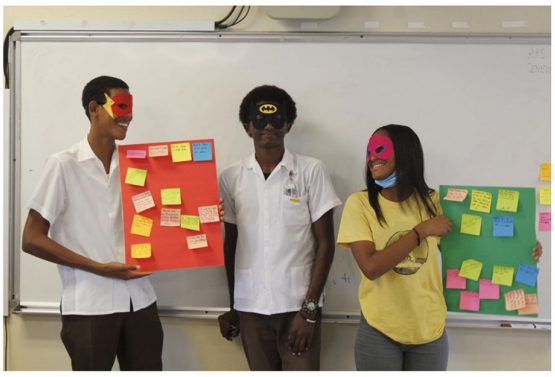

Figure 3. A small group of young people presenting their list of 'dos and don'ts' to the whole group. (Photo credits to Antigua and Barbuda Ministry of Education Broadcast Unit).

Our qualitative analysis involved exploring the "artefacts" created by each group, including their definitions of privacy, their lists of dos and don'ts, and their privacy principles. We focused on analyzing these artifacts first because they provided consistency across the groups and represent a sort of "experiential statement" for the whole-of-group experience. For example, in one site, 15 different definitions of privacy were drafted by small groups (pairs or triads), but through discussion and deliberation, the whole group agreed on a single definition. This analysis focused on this agreed-upon definition. These artifacts were coded using a close reading method. Close reading involves sustained and careful reading to interpret the meaning of a text and generate any dialogic insights (Ruiz De Castilla, 2017). This approach allowed us

to group concepts and uncover themes in these artifacts. These themes, uncovered from a close reading of the artifacts, are supplemented in this article by quotes from focus group transcripts and field notes from researchers.

Privacy as a Protective, Contextual, and Enabling Right

Participants held nuanced views about what online privacy meant to them, but four key ingredients emerged from their definitions and descriptions of privacy. First and most centrally, privacy involved the ability to conceal personal information. Young people spoke about wanting to "protect and conceal our information" (Antigua & Barbuda) or the ability to "protect and conceal our personal information" (Australia). This concept of concealing information and data was always the first idea to emerge among the four groups, aligning with Westin (1968)'s traditional conceptualization of privacy as "control over" information.

The nature of the personal information that young people spoke of wanting to conceal was diverse and highlighted an awareness of datafication as an issue. It included traditional identity markers such as name and date of birth, as well as categorical descriptors such as religion, gender, or your hometown, but also included types of data associated with commercial actors and online surveillance (e.g., metadata). Data about all the things "you have posted online," photographs posted online, and especially geolocation data were noted as types of data that were personal. Geolocation data in particular were problematised across all sites. As one young Australian put it, "I understand that there is an economic side to it, but morally, you don't need to know a 17-year-old's location." Other digital datasets were thought to be particularly deserving of privacy too, including all the "naughty things you have done" and details about the people "you don't like," noted in Ghana as particularly sensitive.

Second, privacy protects personal information from "others" who might want to interfere. Privacy was described as a protective factor that kept information and personal business away from potentially interfering "others." The Antiguan and Barbudan group described privacy as "helping to create boundaries to protect us from interference in our lives" or as safeguarding information "that you don't want others to get," for example. The nature of the "others," from whom personal information needed to be protected, was equally diverse. In Slovenia and Antigua & Barbuda, hackers were frequently discussed as a malicious "other" deserving of particular attention, while they were present but less of a focus in Australia and Ghana. Focus groups spoke about protecting data from states or state institutions like schools or education boards but also wanting interpersonal privacy from family and friends. Notably, commercial companies were also frequently discussed, with young people expressing a desire for privacy from individual companies like Google and Facebook to broader commercial concepts like "online game companies" or "social media" in general. The third-sector too was not immune, as one young person outlined, "(it's) not just advertisers, but any companies. Even not-for-profits will get up in your face sometimes."

Young people spoke about different "others" as warranting different levels of protection, particularly with different types of personal information. For example, in Ghana, as a quick activity to help unpack the concept of privacy, we ran a "straw poll" asking the young people who they thought should see the different types of personal information they identified in Phase 1 of the methods (brainstorming about data footprints). When it came to data about "all the things you have done online," 33% of the group said that they would be okay for best friends to see that, 44% for online friends to see that, and only 22% said their parents or carers should see that. But they wanted complete protection from online companies; nobody wanted them to see that information. When it came to a specific piece of content they posted online, 22% thought it was okay for their best friends to see it, 67% for online friends to see it, but nobody wanted their parents, carers, or online companies to see it.

While this may seem somewhat confusing, especially to older generations that do not differentiate between online and analogue friends, or to online companies trying not to "see" content posted on their own platforms, it is loaded with comprehensible intent. Young people wanted differential protections from others and saw online companies as among the least trustworthy actors when it came to their privacy. This is much more in line with Nissenbaum (2004)'s contextual definition of privacy, which describes privacy as the appropriate flow of information as assessed by each individual based on their preferences and perceptions. Who the data is flowing to is important for young people when it comes to their preferences and perceptions.

Third, privacy was seen as an enabling factor that creates a sense of security, safety, and wellbeing. It was described in Antigua & Barbuda as "set(ing) boundaries making your life personal and more comfortable" or as "mak(ing) you feel a sense of safety and comfortability knowing your info is safe with you." In Ghana, young people described feelings of being "worried" or "upset" because of privacy invasions. In Australia, young people described feeling "unsafe" about some common data practices, such as broadcasting live location details on social media platforms. One young person described it as "really bad, like, actually so bad. Like, I think that's crazy" when we talked about broadcasting maps of where young people are. Privacy—when realized—helps to enable young people's sense of security, safety, and wellbeing, and when violated, it creates a sense of ill-ease and concern.

Finally, privacy was described as a right or expectation in its own right. While privacy also helped secure young people's wellbeing, it was also valued as a right or a legitimate expectation young people hold regardless. In Australia, privacy was described as "a right to protect and conceal"; in

Ghana, young people felt they had "the right to keep certain information to themselves away from others"; and in Antigua & Barbuda, young people felt "no one should be allowed to look at (private information)." Curiously, while the idea that privacy was a right or legitimate expectation was uncontested in each country, the expectations about what the realization of this right looked like differed widely. We discuss the implications of this through a lens of datafication below.

The Normalization or Problematization of Datafication

Datafication is a risk to young people's online privacy as they defined it in this research. Widespread datafication left young people unable to conceal personal information (e.g., geolocation data and what they posted online, as mentioned by young people from Ghana and Australia for example) from "others" who they wanted to conceal it from (e.g., commercial companies, as mentioned in Antigua & Barbuda and Australia for example). It was a frequent and arbitrary interference with young people's expectations to be and feel private online. However, this does not necessarily mean that datafication would automatically be problematised or indeed normalized. Normalization refers to the process of general acceptance of certain social behavior which becomes a social norm (Petzold and Peter, 2015); the pervasive practice of collecting and processing personal data, particularly among young people, is normalized and becomes societal norm, whereas problematization pertains to the critical examination and questioning of the impact and implications of datafication on young people's online privacy. Problematization, unlike normalization, suggests "transformative engagement" (Stengers, 2021), and therefore, conscious awareness and questioning of the ethical and social dimensions of datafication.

The literature suggests that the extent to which young people problematise/normalize datafication depends on (at least) three culturally located experiences: the level of datafication of young people, young people's awareness of datafication, and young people's trust in datafication.

First, it is worth recognizing that problematisation or normalization of datafication depends on the extent to which young people's lives are indeed datafied. While datafication is rife, there are still many young people in communities or parts of the world with limited connectivity where datafication might not be such a significant feature of their lives (including in WEIRD countries, like outback Australia, and non-WEIRD countries, like parts of east Antigua). However, this research was not intended to investigate the perspectives of unconnected young people. The ice-break activity—asking young people to introduce themselves and their favorite app for example—doubled as a check to ensure that all participants were indeed connected.

For connected young people, who this research focussed on, understanding the extent to which datafication is problematized or normalized requires unpacking two socially located experiences. Young people's awareness of datafication is crucial; where young people are unaware that they are datafied (such as when they are unaware that apps track their location data), the very invisibility of the practice makes it difficult to problematize and allows the practice to operate as an unspoken social norm. Where there is awareness of datafication, trust—the second socially located practice—comes into play. Datafication only becomes normalized under conditions of trust (van Dijck, 2014). Without trust in those actors involved in datafication, the practice would be strongly rejected. Both trust and awareness are explored below.

Awareness of Datafication

Awareness of datafication was mixed in these research sites, with a split between WEIRD and non-WEIRD research sites. In Australia and Slovenia, young participants appeared to be largely aware of the practice of datafication, that is, all the young people we spoke to were aware that datafication happened, although with different levels of understanding about the scale of the practice, that is, some thought that very little data were collected while others understood the potential scale of the practice.

In Ghana and Antigua & Barbuda, while many young people were deeply aware of the datafication of their lives and the scale of it, some were not. A description of a quick, pre-lunch activity in Antigua & Barbuda highlights this perfectly. Trying to fill in a 10-minute gap after a discussion about "data footprints," before lunch arrived, we ran a quick quiz & movement activity to activate the "hungry teen energy." Giving each young person a post-it note, we asked them to guess how many data points they thought online companies held about each young person and to get up and try and stick them on a whiteboard in order of lowest to highest guess. The breadth of guesses gave us an unexpected glimpse into the participant's awareness of datafication. Ten young people made guesses on the very low end, around 50 or 100 data points, while eight young people added ginormous estimates of 400 million or 10 billion to the board, and other guesses were scattered in between. We did not discuss what a "datapoint" was to understand what young people meant by 50 or 10 billion, but it is not the numbers themselves that matter here. Two guesses stood out to the research team. Even after the activities around data footprints, with small group discussions among peers and many young people checking which app was collecting what for an entire morning, two young people guessed zero. A descriptive field note taken after the session highlights this:

> I watched one young woman who had written "0" on her post-it note walk up to the board in the maelstrom of activity, ready to stick her guess up. She stopped three steps in front of the board, and watched her peers sticking up guesses that said thousands, millions or billions. She looked down at her post-it note again, then up at the board, watching the post-it note guesses spread

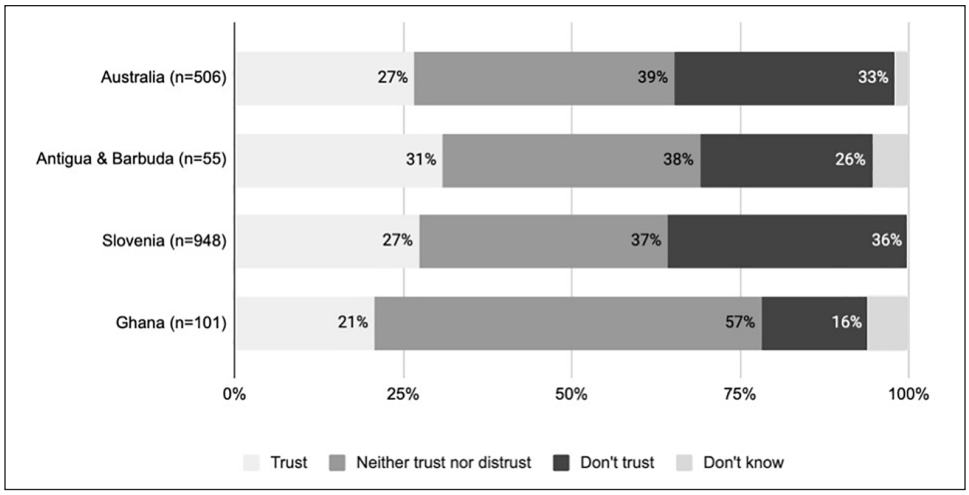

Figure 4. The percentage of young people who reported trusting or distrusting that their data were handled carefully by digital products and services.

> further and further to the right hand side (where the high numbers were being stuck up). She looked at her own post-it note again and froze. I could see her trying to work out why her peers thought that anyone held any data about young people, she was just completely unable to reconcile this with her guess of "0."

This young person was not disconnected from the digital world and had spoken about multiple online services and apps they used regularly, from free games to Google products. It appears that for some young people, the datafication of their lives truly was invisible to them. This could suggest it was an unobserved norm for them. But this was not true for all young people in Antigua & Barbuda, and many young people were deeply aware. We asked one young Antiguan if he was aware of the practice, for example, and he said "a couple of years ago, I read the (Terms of Service) for the first time. Yeah, you can't go back after that." To most young people, datafication was not invisible, and they were aware to various extents that it was happening.

Trust in Those Who Datafy

Awareness of datafication does not mean that the practice is accepted and normalized, nor challenged and problematised. van Dijck (2014) describes the importance of trust in those who collect and use data as a prerequisite for the normalization of datafication. van Dijck (2014) posits that for the questionable ideological grounds for datafication to become normalized, people must implicitly trust in the agents that collect, analyze, and share their data.

In the surveys and polls, we asked young people very broadly if they "trusted" that digital products and services, like apps and websites, handled their personal data carefully (Figure 4). What we found appeared to be broadly speaking equal levels of trust and distrust, and a lot of young people who felt ambivalent. The four-country average for those who trusted that their data was handled carefully was 26%, compared to 27% who distrusted and 43% who neither trusted nor distrusted.

We asked some young Australians to help us understand what this might mean, and their descriptions suggested a strong relationship between normalization and trust as van Dijck (2014) described. But this was not necessarily trust in the "dictionary" sense of the word. Young people spoke about trusting that companies were handling their data carefully because they had to. Trust did not seem to be unquestionably given, nor earned, but offered as a sort of "deal with the devil." One young woman said "if I was given that question [in the survey] I'd say 'Sweet Jesus, like no, I don't think I trust them with my privacy.' But at the same time, you know, I'm on every social media that there is, so . . .." Another young man outlined "because you rely on it. So it's not even about whether or not you can, you don't really have the choice to trust it or not. You just have to use it because everyone else is on it. It isn't about whether or not you believe in your privacy."

Trust as a function of necessity appeared in almost all our research sites. One young Antiguan surveyed explained that they had trust "because they are things I use on daily," and one Ghanaian youngster said they trusted their data were being used carefully on platforms "because it is what we use in our everyday life" but added that "I also do not trust it because it is easy for hackers to access your personal information." Normalizing the questionable way the digital world exploits data requires trust (van Dijck, 2014), but for some young people, this appears to have been a forced normalization. They appear to be actively deciding to trust those involved in data processing simply because they have to.

This idea of "having to trust" those involved in data processing resulted in a lot of discussions around trust as a personal balancing act, where young people felt they were personally

balancing their right to privacy with their right to access the digital world. One young man in Australia described this as

> basically a trade off. And the whole world is full of different perspectives and views, just like the internet. So if we have a look at the two, it's big. Your privacy for something else, or that fun for just a few, like a little bit of information. But I think what makes most people willing to share that information is they think, "Oh, who would be interested in me, like, I'm just one drop out of the ocean. You know, there's millions of other people who do the same thing." So they're pretty trusting.

The commerce involved in this trade-off was a significant consideration when it came to trusting or distrusting digital actors. Young people in each research site described the monetisation of their data as the opposite of their privacy. For example, one young Ghanaian spoke about their ambivalence in trusting that their data were handled carefully by explaining "I trust them because they keep my data safe, and I mostly have control over it. But, I don't trust them because of the way they gather my data and somethings sell it to companies like Google or Facebook to push ads to me." An Australian who did not trust that their data was handled carefully explained that this was "because big companies only care about money and will do anything to get more money, including disrespecting privacy," and a young Antiguan & Barbudan said they distrusted digital services with their personal data because "I believe that they will sell my account." Wherever commercialisation of data was described, it appeared to be a cause of distrust. While the commercialisation–distrust nexus was universal across all four research sites, the frequency with which it was mentioned varied. It was frequently discussed in Australia but rarely in Antigua & Barbuda for example.

As interesting as these variations and nuances are, there is a more obvious conclusion that warrants stating explicitly. Only a minority of young people unquestionably trust that their data are handled carefully, ranging from 21% in Ghana, 27% in Australia and Slovenia, to 31% in Antigua & Barbuda.

Trust is a multifaceted and complex concept intricately linked with various contextual factors, such as the actors involved, the tasks being performed, and the cultural or digital literacy background of the stakeholders (Sztompka, 1999). Our findings underscore the intricate nature of trust development among young people, highlighting the significant roles played by familiarity, knowledge about actors, and past experiences in shaping trust dynamics (Hameleers and van der Meer, 2023). It is crucial to acknowledge that young individuals may sometimes feel compelled to "express" or "normalize" trust, even when they harbor reservations about digital products, driven by a perceived lack of viable alternatives (Bryce and Fraser, 2014; Ghaiumy Anaraky et al., 2021). Prior research has consistently shown the pivotal role of transparency as a key factor influencing user trust development (Kizilcec, 2016; Schmidt et al., 2020). While our young participants exhibited a heightened awareness of datafication practices, it is essential to recognize that they are not consistently provided with transparent information about how these technologies operate Wang et al. (2023). This lack of transparency, coupled with a lack of support for empowerment, poses significant challenges to their informed decision-making and raises concerns about the actual capability of trust development by young people in the digital landscape.

Privacy Principles

Each group developed a list of "dos and don'ts" about what young people thought should and should not happen with their data. These lists were created with deliberation, and participants were informed of survey data, as well as principles that young people in other research sites had created. In Antigua & Barbuda, Australia, and Ghana, young people themselves analyzed, collated, and prioritized their list of "dos and don'ts" into a final set of "privacy principles," but in Slovenia, the analysis and collation was done by researchers because of the compressed session time. Groups came up with between 9 and 14 distinct principles, sometimes with subcategories or multiple principles that could be meaningfully combined. (This is another example that variation may create difficulties in sensemaking. But even if the variable length of their lists makes comparison difficult, the order of their priorities provides crucial indications of their importance to the young people.)

The final lists of principles varied across each site but bore many commonalities. Our analysis suggests that there were 15 key concepts across all the groups, with only three that were entirely unique to one site (all three in Slovenia, which followed a compressed method). These include:

- Requirements around transparency and meaningful consent around data collection and use. For example, renaming cookies as "data grabbers" so young people are not "pushed or tricked" into handing over data, or that "apps must not process or 'eavesdrop' on the content of messages exchanged through them."
- Providing young users with more control of their data. Suggestions were sometimes broad, like "let us be more controllable of our data," which should be specific, like "young people should have the right to request it be deleted."
- Requirements for stronger data security. Young people wanted to "make security stronger for young people's data" for example.
- Requirements for data minimization or collecting less data, such as requirements to "only collect the information about young people that they actually really need to run their app." This especially applied to location data, with suggestions to prevent products "Collect as much location data about young people as they want."
- Requiring data to be processed only where it is in young people's best interests, which was described

as a meta-principle framing the other concepts. For example, suggestions that young people's data are "only collected and used in ways that advance their best interests, but this needs specifics about what it means. Young people need to decide what young people's best interests are."

- Requirements to prevent excessive data sharing or selling. Popular principles include "for data to not be resold" or "not be sold or traded to other companies."
- Restricting or ending targeted advertising to young people. Suggestions ranged from blanket calls to "stop advertising" to more targeted calls for "don't have advertising turned on by default for young people."
- Requirements around data retention and obligations to delete data when it is not needed. Suggestions ranged from requirements for data only to "be kept for as long as is it needed only" to requirements that "when we log out, all our data is deleted."
- Requiring companies to provide adequate help and support. For example, it was suggested that "companies that collect and use young people's data should be accountable to them. If something goes wrong, it should be the company's responsibility to provide help and support and fix it."
- Requirements for stronger content moderation or mitigation of algorithmic recommendation of harmful content. These ranged from calls for content controls, such as "banning the posting of videos that encourage children to take up dangerous challenges," to calls for controls on how harmful content is shared, such as not "encourag(ing) harmful content in 'for you' feeds."
- Improving the use of data for good, or using it in ways to benefit young people. This ranged from simple calls for things like "free games" to the more transactional "If you take my data, at least make the app better" or a request "to use my data to do things that would benefit me, and let me know."
- Requirements to provide better education for young people. There were calls for young people to be "supported and educated about privacy, their rights and risks," or for the "safe use of the internet (to become) a school subject."
- Restrictions or limitations for young people, such as time limits or age limits to own devices and so on. These ranged from soft requests like "For there to be a day without phones," to stronger suggestions "for under 16s to not use the internet" (Slovenia only).
- Requirements for parental supervision, or additional parental supervision when using the digital world (Slovenia only).
- Others. The scale of the Slovenian workshops generated some suggestions that fit no other categories,

Key concepts underpinning the privacy principles	Antigua & Barbuda - 9 principles	Australia - 11 principles	Ghana - 9 principles	Slovenia - 14 core principles
Transparency and meaningful consent around data collection and use	2	2	1	9
Providing young users with more control of their data	1	7	3	10
Stronger data security	3	4	7	2
Data minimisation or collecting less data	4	3	8	3
Processing in young people's best interests or similar as a meta principle	-	1	2	-
Preventing excessive sharing or selling	7	6	4	1
Restricting or ending targeted advertising to young people	5	11	5	7
Data retention or obligations to delete data when it is not needed	6	5	9	5
Requiring companies to provide adequate help and support	9	8	6	13
Requirements for stronger content moderation/ mitigation of algorithms	-	9	-	6
Improving the use of data for good	8	-	-	11
Requirements to provide better education for young people	-	10	-	14
Restrictions or limitations for young people	-	-	-	4
Requirements for parental supervision	-	-	-	8
Others (combined)	-	-	-	~12

Figure 5. The 15 broad categories of principles listed by young people in each country, in order of priority, where 1 is the most important priority identified by the young people.

from clarion calls like "for children to be in a decision-making role instead of experts and politicians" to specific issues such as "for it to be easier to change the phone number associated with your account" (Slovenia only).

Figure 5 outlines the concepts that young people embedded into their privacy principles, in order of priority. Below, we expand on requirements about behavioral advertising to showcase divergence and "providing users with more control" to highlight convergence.

Privacy and Advertising

It was widely understood in all four sites that behavioral advertising—involving tracking and collecting young people's personal data and online activities, and using this to target them with advertising—is the business behind much of the digital world. It was also a widely held belief that this was not great, with descriptions ranging from being annoying to an outright violation of young people's privacy. Despite this convergence, how advertising was discussed by young people across four sites was particularly insightful and suggests a strong role for political mediation of young people's expectations.

Taking Australia as an example, there was a discernible "chilling effect" where young people limited their principles to what they believed was possible within the current policy climate. In their submission to a Senate inquiry, the young participants opened up with "fundamentally, young people do not want their data used to sell them things." They quickly went on to moderate this statement by calling for advertising to "not be turned on by default for young people. Young people should be able to opt-in and choose to have advertising overall, and also be able to choose if they want their data used to personalise these ads or not." This was not because they felt young people wanted or needed a choice about receiving advertisements, but because, in their words, they wanted to be "realistic" in their discussions with policymakers. They "support(ed) a ban on behavioural advertising, but (are) aware it might be unpopular or difficult to implement."

We unpacked this desire to be "realistic" with the group, as it came up multiple times. During the deliberations around privacy principles, young people expressed genuine concerns that what they really wanted might not be "too much" to ask for. There appeared to be a belief that young people needed to be sources of profit for technology companies to access the digital world. Notes and transcripts from the discussions included multiple comments like "but they won't*t* do that, so don't add it (to the list)," "but that won't make them a profit," "if they don't profit, they won't do it." Or as one young person we interviewed said:

> We can't expect the government to, you know, make (digital products and services) default to "no, you can't share my data." . . . Because like that wouldn't get passed, like no matter what. Because it's just like, it's really unrealistic for them to be able to do that and then make profit at the same time.

Uniquely, these Australian young people had experienced firsthand what can happen when tech companies go head-to-head with governments. In 2021, Facebook responded to the Australian Government's attempts to implement regulation by withdrawing news from its Australian platform, causing "havoc" during bushfire season and the COVID vaccine rollout (Hagey et al., 2022). These young people had also grown up with effective privacy or data-protection regulations; Australia's Privacy Act was passed in 1988, 5 years before the internet was made available to the public and does not protect metadata for example. Growing up in this climate could potentially explain why these young people were inclined to "chill" their expectations, in contract to the principles of young people in Slovenia, Ghana, and Antigua & Barbuda, all of whom called for a more straightforward ban on targeted advertising.

In a welcome but tragic twist, the tempering dose of realism that these young people swallowed was not necessary. Five months after they developed their principles, a review into the Privacy Act—which these young people ultimately gave evidence to—called for a complete prohibition on direct marketing to a child under 18 years of age in Australia, with exceptions only if the personal information used for the direct marketing was collected directly from the child, and the marketing is in the child's best interests. It appears that for these young people, datafication of the digital world was so normalized and unavoidable that they could not even imagine making a plea for what turned out to be thoroughly possible policy reform.

Control of Your Own Data

For young people in each site, having control over their own data was a central expectation and demand that emerged across privacy principles. While control is implicit in almost all the privacy principles young people developed (from data retention to calling for more support where things go wrong), explicit calls for control took many forms. For example, broader calls like "let us be more controllable of our data" were made in Antigua to specific calls like the "option to set permission settings for posts" from Slovenia.

Ghana presented a unique version of this principle, which called for a complete reframing in the relationship between digital platforms and services and young people. In a move that would restore control over data to young people, they asked for companies to consider themselves as mere "caretakers" of young people's data where they use it, rather than as data owners who could collect it, use it, and trade it however they wanted.

In Ghana, the young people were acutely alive to the relationship between data and control and discussed with

researchers how regaining control of their data could be an act of agency. They were aware that data could be used to wielding power over young people, with one young person noting:

> assuming a child's information since they were 8 years' old was online, by 12 years, advertisers and data collectors would have enough information to about the person, to determine likes, dislikes, social affiliations and much more which gives them the ability to determine how best to influence the child towards their desired outcome.

The ability for data to push children to "their desired outcome"—emphasis added—is loaded. "Their" means advertisers and data collectors, or people generally involved in the commercial aspects of the online world. This was not what the young people in Ghana wanted. They wanted control over their own data themselves. In the language of power (Lukes, 2021), they wanted to curtail data's power over them (currently wielded by advertisers and data collectors) and replace it with power to control their own data (putting young people in the driving seat).

To them, this was not as an emancipatory act of freedom rather it was described as an act of fairness. Fairness in the relationship between young people and digital products and services, as they described it, meant young people having power and control over their own information. In a culture—like many others—where young people are often "seen and not heard," control over data was talked about with researchers as an act of fairness for the younger generations.

Conclusions

The young people involved in this research held nuanced and sophisticated understandings of what privacy online should mean for them. They were largely aware of the ways the online world datafied them, and what this meant for their privacy. However, given the prevalence of the practice, datafication did not lead to a straightforward rejection or strong plea for greater privacy. Rather, it appeared to produce difficulties in imagining viable or realistic alternatives when it came to their privacy online. Regardless, at each site, young people were able to articulate a strong set of privacy principles they believed should govern the online world.

Comparatively speaking, these principles showed extensive convergence. Only three principles emerged that were completed unique to one country, and all in Slovenia, including (a) restrictions or limitations for young people, (b) requirements for parental supervision, and (c) a broad category of other disconnected suggestions, which are expected given the sample size. This may reflect the collective experience these young people shared in a "global" online environment. However, even within this convergence, unique socially located differences were apparent.

Understanding young people's perspectives and desires for privacy protections is an increasingly important task. As policy makers around the world activate to protect young people's privacy, young people's voices must be heard, and these can help to inform more effective policy outcomes. This research suggests that young people can and do want to be engaged in these deliberations and highlights the potential for and importance of local deliberations to inform these policy deliberations.

Acknowledgements

We thank all the young people who participated in this research, whose generosity and expertise made this research possible.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Internet Society Foundation.

ORCID iDs

Rys Farthing https://orcid.org/0000-0002-6150-4259
Katja Koren Ošljak https://orcid.org/0009-0003-9168-3475
Jun Zhao https://orcid.org/0000-0001-6935-9028

References

Acker, A., & Bowler, L. (2017). What is your data silhouette? Raising teen awareness of their data traces in social media. In *Proceedings of the 8th international conference on social media & society* (pp. 1–5). Association for Computing Machinery.

Australian Attorney General's Office. (2023). Privacy act review report. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Barassi, V. (2020). *Child data citizen*. MIT Press.

Bernd, J., Gordo, B., Choi, J., Morgan, B., Henderson, N., Egelman, S., Garcia, D. D., & Friedland, G. (2015). Teaching privacy: Multimedia making a difference. *IEEE Multimedia*, *22*(1), 12–19. https://doi.org/10.1109/MMUL.2015.16

Bertelsen, O. W., Bødker, S., Eriksson, E., Hoggan, E., & Vermeulen, J. (2018). Beyond generalization: Research for the very particular. *Interactions*, *26*(1), 34–38. https://doi.org/10.1145/3289425

Bevan Jones, R., Stallard, P., Agha, S. S., Rice, S., Werner-Seidler, A., Stasiak, K., Kahn, J., Simpson, S. A., Alvarez-Jimenez, M., Rice, F., Evan, R., & Merry, S. (2020). Practitioner review: Co-design of digital mental health technologies with children and young people. *Journal of Child Psychology and Psychiatry*, *61*(8), 928–940. https://doi.org/10.1111/jcpp.13258

Bowler, L., Acker, A., Jeng, W., & Chi, Y. (2017). "It lives all around us": Aspects of data literacy in teen's lives. *Proceedings of the Association for Information Science and Technology*, *54*(1), 27–35.

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.

Crippen, K., & Brown, J. (2018). Design-based research. In B. B. Frey (Ed.), *The SAGE encyclopedia of educational research, measurement, and evaluation* (pp. 490–493). SAGE. https://doi.org/10.4135/9781506326139

Data Protection Commission. (2019). Some stuff you just want to keep private. https://www.dataprotection.ie/sites/default/files/uploads/2019-08/Some%20Stuff%20You%20Just%20Want%20to%20Keep%20Private_Consultation%20Report.pdf.AccessedinDecember2023

European Commission. (2022). Better internet for kids+ strategy. https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

Ghaiumy Anaraky, R., Byrne, K. A., Wisniewski, P. J., Page, X., & Knijnenburg, B. (2021). To disclose or not to disclose: Examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1–14). Association for Computing Machinery.

Hagey, K., Cherney, M., & Horwitz, J. (2022, May 5). Facebook deliberately caused havoc in australia to influence new law, whistleblowers say. *The Wall Street Journal*. https://www.wsj.com/articles/facebook-deliberately-caused-havoc-in-australia-to-influence-new-law-whistleblowers-say-11651768302

Hameleers, M., & van der Meer, T. (2023). Striking the balance between fake and real: Under what conditions can media literacy messages that warn about misinformation maintain trust in accurate information? *Behaviour & Information Technology*, 1–3. https://doi.org/10.1080/0144929X.2023.2267700

Harriger, J. A., Evans, J. A., Thompson, J. K., & Tylka, T. L. (2022). The dangers of the rabbit hole: Reflections on social media as a portal into a distorted world of edited bodies and eating disorder risk and the role of algorithms. *Body Image*, *41*, 292–297.

Hartung, P. (2020). *The children's rights-by-design standard for data use by tech companies [UNICEF good governance of children's data project]*. https://tinyurl.com/2s42h5k4 (accessed on 12 September 2022)

Information Commissioner's Office and Revealing Reality. (2019). *Towards a better digital future informing the age appropriate design code*. https://ico.org.uk/media/about-the-fico/consultations/2614763/ico-rr-report-0703.pdf.AccessinApril2024

Irish Council for Civil Liberties. (2023). 5 years: GDPR's crisis point. https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf

Jarke, J., & Breiter, A. (2019). The datafication of education. *Learning, Media and Technology*, *44*(1), 1–6. https://doi.org/10.1080/17439884.2019.1573833

Kennedy, H., Poell, T., & van Dijck, J. (2015). Data and agency. *Big Data and Society*, *2*(2), Article 621569. https://doi.org/10.1177/2053951715621569

Kizilcec, R. F. (2016). How much information? Effects of transparency on trust in an algorithmic interface. In Proceedings of the 2016 CHI conference on human factors in computing systems (pp. 2390–2395). Association for Computing Machinery.

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. *Proceedings of the ACM on Human-Computer Interaction*, *1*, 1–21.

Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online—Growing up in a digital age: An evidence review. https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, *19*(5), 657–670.

Lukes, S. (2021). *Power: A radical view*. Bloomsbury.

Mandell, K., & Farthing, R. (2023). Online privacy, digital trust and young people. *Centre for the Digital Child*. https://www.digitalchild.org.au/blog/online-privacy-digital-trust-and-young-people/

Mascheroni, G. (2018). Researching datafied children as data citizens. *Journal of Children and Media*, *12*(4), 517–523.

Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology*, *68*(6), 798–813. https://doi.org/10.1177/0011392118807534

Mascheroni, G., & Siibak, A. (2021). Datafied childhoods: Data practices and imaginaries in children's lives. Peter Lang.

McNiff, J. (2017). Action research: All you need to know. SAGE.

Nairn, A., & Fine, C. (2008). Who's messing with my mind? The implications of dual-process models for the ethics of advertising to children. *International Journal of Advertising*, *27*(3), 447–470.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, Article 119.

Organisation for Economic Co-operation and Development. (2022). DAC list of ODA recipients. https://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/DAC-List-of-ODA-Recipients-for-reporting-2020-flows.pdf

Pangrazio, L., & Selwyn, N. (2017). 'My data, my bad. . .': Young people's personal data understandings and (counter) practices. In Proceedings of the 8th international conference on social media & society (pp. 1–5). Association for Computing Machinery.

Petzold, K., & Peter, T. (2015). The social norm to study abroad: Determinants and effects. *Higher Education*, *69*:, 885–900.

Ruiz, De, & Castilla, C. (2017). Close reading. In M. Allen (Ed.), *The SAGE encyclopedia of communication research methods* (pp.136–138). SAGE. https://doi.org/10.4135/9781483381411

Schmidt, P., Biessmann, F., & Teubner, T. (2020). Transparency and trust in artificial intelligence systems. *Journal of Decision Systems*, *29*(4), 260–278.

Sefton-Green, J., Dezuanni, M., & Pangrazio, L. (2022). A research agenda to examine the political economy of digital childhood. https://digitalchild.org.au/wp-content/uploads/2024/01/Sefton-Green-Pangrazio-Dezuanni-A-Research-Agenda-into-the-Political-Economy-of-Digital-Childhood-Digital-Child-Working-Paper-2022-06-2.pdf

Sirur, S., Nurse, J. R., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the general data protection regulation (GDPR). *In Proceedings of the 2nd international workshop on multimedia privacy and security (pp*. 88–95). https://doi.org/10.1145/3267357.3267368.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). Eu kids online 2020: Survey results from 19 countries. *EU Kids Online*. https://doi.org/10.21953/lse.47fdeqj01ofo

State of California. (2022). AB-2273: The California Age-Appropriate Design Code Act.

Stengers, I. (2021). Putting problematization to the test of our present. *Theory, Culture & Society*, *38*(2), 71–92.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, *8*(4), 197–207.

Stoilova, M., Nandagiri, R., & Livingstone, S. (2021). Children's understanding of personal data and privacy online: A systematic evidence mapping. *Information, Communication & Society*, *24*(4), 557–575.

Sztompka, P. (1999). *Trust: A sociological theory*. Cambridge University Press.

Third, A., & Moody, L. (2021). *Our rights in the digital world: A report on the children's consultations to inform UNCRC general comment 25*. 5Rights Foundation and Western Sydney University.

Twenge, J. M., Haidt, J., Joiner, T. E., & Campbell, W. K. (2020). Underestimating digital media harm. *Nature Human Behaviour*, *4*(4), 346–348. https://doi.org/10.1038/s41562-020-0839-4

United Nations Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (General Assembly resolution 44/254425). https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

United Nations General Assembly. (1989). Convention on the rights of the child (General Assembly Resolution 44/254425).

United States. (1998). *Children's Online Privacy Protection Act of* 1998,15 U.S.C. 6501–6505).

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208.

Verdoodt, V., Clifford, D., & Lievens, E. (2016). Toying with children's emotions, the new game in town? The legality of advergames in the EU. *Computer Law & Security Review*, *32*(4), 599–614. https://doi.org/10.1016/j.clsr.2016.05.007

Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2022). 'Don't make assumptions about me!': Understanding children's perception of datafication online. *Proceedings of the ACM on Human-Computer Interaction*, *6*, 1–24.

Wang, G., Zhao, J., Van Kleek, M., & Shadbolt, N. (2023, April 11–12). 'Treat me as your friend, not a number in your database': Co-designing with children to cope with datafication online. In *Proceedings of the 2023 CHI conference on human factors in computing systems* (pp. 1–21). Association for Computing Machinery. https://doi.org/10.1145/3544548.3580933

Weiss-Blatt, N. (2021). *The Techlash and tech crisis communication*. Emerald Group.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), Article 166.

Willson, M. (2019). Raising the ideal child? Algorithms, quantification and prediction. *Media, Culture & Society*, *41*(5), 620–636.

Zeichner, O. (2019). The impact of safe internet intervention programs on pupils. *i-manager's: Journal of Educational Technology*, *16*(3), Article 34. https://doi.org/10.26634/jet.16.3.16572

Zhou, Y., Wang, G., Zhao, J., & Li, J. (2023). 'Treat me as your friend, not a number in your database': Co-designing with children to cope with datafication online. https://dl.acm.org/doi/10.1145/3544548.3580933

Zuboff, S. (2015). The age of surveillance capitalism. Profile Books.

Author Biographies

Rys Farthing (PhD, University of Oxford) is a policy expert from Reset.Tech (Australia & US), with a focus on children's rights, especially around technology and disadvantage. She is also a Research Associate at the Information Law & Policy Centre (University of London) and Associate Investigator at the Centre for the Digital Child (Deakin, Australia).

Katja Koren Ošljak (PhD, University of Ljubljana) is a researcher with the Faculty of Social Sciences, University of Ljubljana, and the founder of VSAK Institute, a not-for-profit think tank that promotes young people's digital rights across Slovenia and central Europe. She has a strong focus on critical digital literacy and developing digital curriculum for children.

Teki Akuetteh (LLM, University of Strathclyde) is the Founder and Executive Director at Africa Digital RIghts' Hub (a not-for-profit think tank that promotes digital rights across Africa), a member of the UN Global Pulse Privacy Advisory Group, and a non-resident fellow at the Center for Global Development in Washington DC. She is a privacy and data-protection advocate.

Kadian Camacho is a research associate in the Department of Education, University Of West Indies, Saint John's campus. Kadian informs evidence-based policy and practices, with a focus on the digitization of Antiguan and Barbudan education systems and an interest in the role of privacy within the process.

Genevieve Smith-Nunes (PhD, University of Cambridge) is a lecturer at the University of Roehampton and King's College London. Her research focuses on data ethics through creative computing and biometrics.

Jun Zhao (PhD, University of Manchester) is a senior research fellow from the University of Oxford. Her research focuses on investigating the impact of algorithmic systems on families and young children.