

“It sets boundaries making your life personal and more comfortable”: Understanding young people’s privacy needs and concerns

Rys Farthing
Centre for the Digital Child
Deakin University
Melbourne, Australia
rys.farthing@deakin.edu.au

Teki Akuetteh
Africa Digital Rights Hub
Accra, Ghana
takuetteh@afriadigitalrightshub.org

Katja Koren Ošljak
Faculty of Social Sciences
University of Ljubljana
Ljubljana, Slovenia
katja.osljak@fdv.uni-lj.si

Genevieve Smith-Nunes
Department of Education
University of Cambridge
Cambridge, UK
ges52@cam.ac.uk

Kadian Comacho
Department of Education
University of West Indies
Saint John’s, Antigua & Barbuda
60043907@uwi.edu

Jun Zhao
Department of Computer Science
University of Oxford
Oxford, UK
jun.zhao@cs.ox.ac.uk

Abstract—Children and young people are prolific digital users, and often engage with the digital world in distinct ways. However, their unique understandings about privacy are rarely considered when designing privacy protections and information security practices. This article develops a youth-centric notion of digital privacy, and guiding principles around privacy developed by young people from Antigua & Barbuda, Australia, Ghana and Slovenia.

Keywords—young people, children, privacy, trustworthy tech

I. INTRODUCTION

Children and young people make up a third of the world’s online users [1], but are often not considered in debates and discussions around privacy and data security [2]. While there is extensive research exploring children and young people’s potentially harmful experiences within the digital context, such as dangerous content, grooming and abuse or risky online behaviors like cyberbullying to excessive ‘screen time’, there has been a far more limited focus on exploring children and young people’s privacy concerns [3]. Previous research has often identified that young people hold unique ideas about privacy [4, 5], identifying privacy as a right which they feel is often challenged or threatened, [6] and that there is a gap in research around young people’s perspectives around commercial contexts, which is rapidly important in the increasing commercially digital environment [7].

Understanding children and young people’s privacy concerns regarding commercial digital products (be online platforms or personal digital gadgets), and what they want done about them, is an important task. Children and young people are unique users of the digital world, and there are at least three reasons young people’s privacy concerns may be distinct from adults. Firstly, the ways that young people are datafied and the nature of their data footprint is distinct from adults. Today’s young people are the first to be datafied—to have their lives turned into extracted data points — from even before birth [8]. They carry a whole lifetime worth of data (and privacy concerns), shared with a fluid mix of State and commercial

companies that young people may be unaware of. Many of these data holders may not be committed to young people’s best interests, which leads to our second distinction: this data can be used young people in ways to shape their lives and life chances in ways that current adults have not experience [9]. For example, when high school leaving exams were cancelled because of COVID in the UK, young people’s postcode data—a marker of socio-economic status—was used to downgrade university entrance scores of young people from lower-income neighbourhoods [10]. This was reversed after a public backlash in this instance, but the algorithmic governance of future generations from before birth remains possible if not inevitable. Lastly, the scale and pervasiveness of this datafication has gone hand in hand with the normalization of surveillance and datafication [11], which may mean that young people, having grown up entirely in a different age of dataism, may have different perspectives about privacy and data security that are worthy of consideration.

If technologists and policy makers aim to develop solutions that serve all members of the community, understanding how children and young people think about privacy, and what they think should happen with their personal data, is therefore critical. Ensuring effective privacy protections and information security protocols that meet the unique needs and expectations of young people is important for their flourishing and safety, but also to realize a more inclusive democracy for all of us.

A. Aims and contributions of this research

This paper aims to fill some of this gap, by providing an analysis of privacy, especially privacy in a commercial digital context, from young people’s perspectives around the world. It also makes a critical contribution to relevant knowledge by developing a set of guiding policy principles about privacy from young people’s perspectives, that may be important to both technologists and policy makers working on privacy protections and information security.

II. METHODS

Using mix-methods we engaged young people aged 10-18 years old in four locations; Accra in Ghana, multiple places across Slovenia, Saint John's in Antigua & Barbuda and Sydney in Australia. These sites were chosen to (1) allow some international comparisons between young people's perspectives emerging from Western, Educated, Industrial, Rich, Democratic (WEIRD) contexts and non-WEIRD contexts, and (2) engage with emerging policy and technological debates about privacy and trustworthy tech that were happening in each location. Impact was prioritized in this research, and the aim was to generate insightful, youth-led discussions capable of catalyzing change in each location.

Below we discuss the common and divergent features of each site, to help understanding the nature of the data captured.

A. Common research methods

This research began from an understanding that the perspectives of young people are valuable but under recognized. Given this, we use participatory methods, allowing young people to shape the research agenda. We also engaged mixed-method, using many youth-friendly activities, like hypothetical and 'real' scenarios, which have successfully been used in research around young people and privacy [4, 5].

Qualitatively, a series of deliberative workshops were held, with activities designed to culminate in the creation of a set of principles that participants felt should govern the use of their private information. These workshops included four key activities as follows.

- 1) Workshopping and discussing their data footprint, including what sorts and how much personal data about young people was collected in their current digital environment. Activities included brainstorming, drawing data heat maps, small group discussions and often "immediate technical investigations" such as logging into an app and seeing if it was tracking their location.
- 2) Discussions and deliberations about how this data was currently processed, including debates around if these processes and processors were trustworthy. This often involved 'role playing' and hypothetical scenarios, such as pretending you were the CEO of a new tech start up. After this, the groups moved on to explore.
- 3) What it would take to make these processes and processors trustworthy, including developing an extensive list of 'dos and don'ts' with their data. These deliberations were informed by suggestions young people had made in quantitative research, and/or in other research sites, and undertaken using post-it note brainstorming and small group discussions. These 'dos and don'ts' were then further refined into a list of principles.
- 4) The final process involved discussions, decisions and actions to connect young research participants with decision-makers in the space, either policymakers or technologists, shifting into the action-research space.

This was supplemented by quantitative polling and surveys.

B. Antigua & Barbuda

Hybrid workshops were held with 42 young people aged 13-15 in St John's, over 2 days. Young people were recruited from schools across Antigua to attend in person, and a school group from Barbuda attended online. An additional 55 young people took part in a survey circulated throughout schools, aged 13-18.

C. Australia

Hybrid workshops and interviews were held with 12 young people from New South Wales, held across a full day with follow-up online meetings. Participants were 15-17 years old, and recruited from a youth work setting, 506 16- and 17-year-olds were polled by a commercial polling company.

D. Ghana

Workshops with 21 13-17-year-olds were held in Accra. Participants were recruited from nine different localities and schools, reflecting different socioeconomic situations. The Ghanaian survey of young people was not completed by the time of this article.

E. Slovenia

Shorter one-hour in-person workshops were held across Slovenia, with in excess of 15,000 young people mostly aged between 11 and 15 attending, with some a bit older or younger. These workshops happened in conjunction with the release of a popular Slovenian language teen-movie *Gaja's World 2*. The pace and scale of these workshops followed a compressed method, without role-playing and with decisions around actions being researcher led rather than youth led. This was supplemented by a survey of 948 young people aged 14-18, led by the University of Ljubljana.

III. PRIVACY AND YOUNG PEOPLE

Many common themes emerged across all the research sites, and these are discussed below.

A. What privacy means to young people

The definitions of privacy highlighted four key aspects and considerations underpinning the idea of privacy for the young people at the workshops. For these young people, privacy:

- Involved being able to conceal personal information (e.g., *'to protect and conceal our information'*). Personal information included identifying data about yourself, including and especially contact details, location details and details as well as information about *'naughty things you've done'*.
- Was a protective factor from 'others' who may want to interfere (e.g., *'helps to create boundaries to protect us from interference in our lives'*). Discussions suggested that 'others' who information may need to be concealed from included States, hackers, friends, parents and companies. Who your data needed to be protected from mattered, including preventing interference from commercial 'others'.
- Created a sense or feeling of safety, security and healthy boundaries (e.g., *'privacy may make you feel a sense of*

safety and comfortability knowing your info is safe with you')

- Was considered as a legitimate expectation or as a right (e.g., it was described as *'a right to protect and or conceal our personal information'*)

These definitions align with Westin's [12] conceptualization of privacy as 'control over' information. But Nissenbaum's [13] alternative contextual definition of privacy—or privacy as the appropriate information flow of information as assessed by each individual based on their preferences and perceptions—slowly emerged.

As discussions around trust and what young people wanted progressed, the understanding that privacy was contextual surfaced. As discussed below, this was particularly visible when young people talked about wanting better things, or to receive more benefits, as a result of the flow of their data. These discussions highlighted that some flows of information were deemed more desirable than others, depending on context. Critically, they also highlighted that commercial considerations were part of the criteria young people were using in deciding which flows they felt were (or not) appropriate.

B. Do young people trust technology with their privacy

Despite being described as 'right' and a positive concept, the workshops uncovered deep misgivings held by some of the young people about their experiences of privacy in the digital world. As one young man put it *'the only way I make myself feel private is by just outright lying to myself and telling myself that the information that I get stolen online won't affect me that much'*.

The polling and survey data collected reflects this, and highlighted a significant 'trust gap' when it came to how young people felt their personal information was handled. We asked young people if they trusted that their personal information would be handled carefully, and found that very roughly a third trusted that their personal information was being handled with care, a third did not trust their personal information was handled carefully and the rest were not sure if they distrusted the way their data was handled (see Figure 1).

We asked some young people to help us interpret these findings, and they suggested that the normalization and inevitability of privacy intrusions in their digital worlds may help explain this answer. As one young woman explained *'if I was given that question, 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. And I think a large part of that is... not caring'*. 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"*. The (broadly) even split in responses may be young people's way reconciling the privacy paradox [14] in this survey; as one young Antiguan put it simply *'I trust them because they are things I use on daily'*.

IV. WHAT YOUNG PEOPLE WANT TO IMPROVE THEIR PRIVACY

Privacy intrusions in the digital world may have felt inevitable or normal, but they were not necessarily what the young participants wanted. Young people were able to give us clear ideas about changes they wanted to see, and list specific suggestions as well as guiding principles to improve their sense of privacy in the digital world.

Exploring the list of 'dos and don'ts' created by young people, and their guiding policy principles, ten core asks were frequently repeated across areas (and 3 additional Slovenian asks):

1. Control. The most frequent principle described as important was that young people should have control over their data. There was a sense that young people's information was collected, used and sold in ways that were currently beyond their control, and that young people were entitled to better. Specific suggestions ranged from giving young people *'the right to delete our data'* to *'allowing young people or teenagers to make their own decisions with the available options.'*
2. Transparency and meaningful consent. There was a strong sense that young people were often *'pushed or tricked'* into personal information collection, from opaque privacy policies to smart phones secretly *'eavesdropping'* on conversations. The young people in Australia wanted cookies renamed *'data grabbers'*, and the young people in Slovenia wanted *'translations of apps and programs'* into Slovenian. There was an overarching belief that young people deserved more honest and clear information about how their personal information would be used, especially from commercial platforms.
3. Restricting or ending targeted advertising. There was consensus that the current state of play—where young people's information is used to target them with ads by default—did not meet expectations. Young people in Slovenia, Antigua & Barbuda and Ghana more aggressively called for a ban on advertising, wanting to *'cancel ads'*, saying *'online ads should be banned'* and requesting companies *'stop sending those ads.'* In Australia, the young people instead called for control, that young people should be able to opt-in to advertising, and if they did opt-in to advertising, should also then have the choice about whether their data is used to target ads at them or not. Notably, they called for this rather than a full ban because they wanted *"realistic"* asks; *"fundamentally, young people do not want their data used to sell them things"* they said.
4. Data minimisation. A range of suggestions were discussed that cluster around the concept of *'data minimisation'*, from suggestions to *'avoid asking for data'*, *'avoid accepting cookies'*, *'to not collect data at all'* and suggestions companies *'don't access our location every thirty seconds'*.

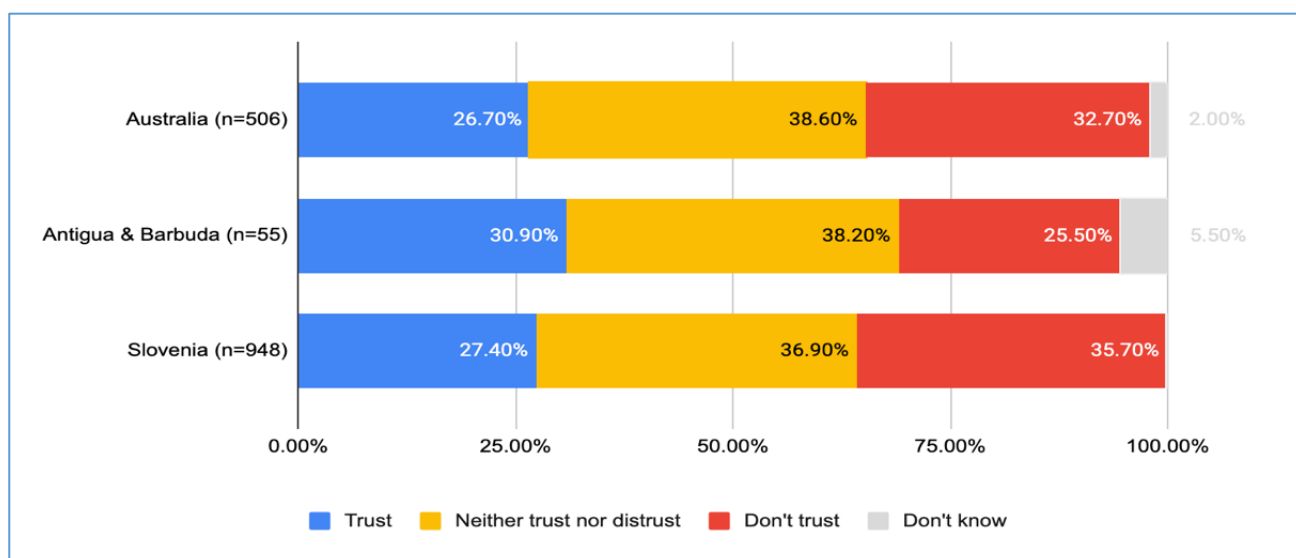


Figure 1. Young people's sense of trust or distrust about whether their personal information was "handled carefully", by location.

5. Data retention. Young people in each site seemed to agree that young people's information should not be kept for too long, with requests to 'delete young people's data when it's not needed' and especially after an app is uninstalled.
6. Excessive sharing and selling. There was a feeling that young people's personal information was shared with too many people, including families, too many apps and sold to too many companies. Young people wanted data to be more 'concealed'. Requests to 'Don't sell our data to others' were others, as were suggestions to limiting 'Family link' (an app that shares your location and other data) up until certain ages or banning it altogether. Information about young people's locations was considered especially sensitive for oversharing, and suggestions to 'limit who can see your location' were frequent.
7. Adequate help and support. In each site, young people felt they should have better access to support if something went wrong, from a 'Help portal in case of personal profile hacks' to calls for services to 'respond quickly to reports and violations of guidelines.'
8. Security. Security came up as a concern in each site, but some more than others. Antigua & Barbuda and Slovenia were very concern about security, while Ghana & Australia were less so. But generally, young people felt their data deserved higher levels of security and protection from hackers than it currently received.
9. A need for more education for young people about their privacy. At each site, young people talked about the need for more education (often younger young people) about privacy. Suggestions ranged from 'talks in schools' to a specialized school subject on the "safe use of the Internet" to more education "about privacy, their rights and risks" in general.
10. *in schools*' to a specialised school subject on the 'safe use of the Internet' to more education 'about privacy, their rights and risks' in general.
11. Doing things for young people's benefit. In Antigua & Barbuda there was a cluster of specific suggestions to ensure that young people benefited from the use of their personal information. 'If you take my data, at least make the app better' and 'protect our data for better uses.' Likewise in Slovenia, there was support to make all games free and to operate without data. The capacity of the digital world to provide good services that young people want to use was not overlooked. This speaks to their idea of data and its flows as part of a contextual relationship in the commercial world; or more precisely, highlights that they want a 'better deal' from this relationship.
12. Limitations and restricted use. Given the vast size of the Slovenian workshops, a number of unique Slovenian suggestions were generated. A moderate focus on the potential capacities of limitations (such as calls for age restrictions, or limiting device use) and reduced use (such as days off and time limits) emerged.
13. Content moderation. Some Slovenian young people suggestions also called for better or safer content moderation, from banning videos that encourage kids to do dangerous challenges, to deleting negative comments.
14. Parental supervision. Some Slovenian young people also called for increased parental supervision or oversight, although it should be noted that others called for privacy from their parents.

We asked young people if they felt that their list of principles aligned with what could be broadly considered

“children’s best interests” as the Convention on the Rights of the Child describes it [15]. The reaction was broadly yes, but with specification. In Antigua and Barbuda, young people gave an unstirred ‘*sure*’ with a shrug of the shoulders because it seemed a bit too common-sense. In Ghana, this was one of the most popular suggestions, and they also included suggestions around ‘*doing no harm*’ with data too. In Australia, they decided that best interests was the first principal, but needed a caveat: that ‘*young people need to decide what young people’s best interests are*’.

V. THE VALUE OF ENGAGING YOUNG PEOPLE

Realizing young people’s best interests requires their participation in decision-making processes. And off all the brilliant suggestions developed by young people, one suggestion stood out: ‘*so that children make decisions instead of experts and politicians.*’ This research actively tried to engage with technologists and decision makers to achieve this.

In Antigua and Barbuda, the principles developed by young people were turned into a ‘magazine’ for decision-makers and a workshop held with teachers to share ideas for curriculum reforms. In Australia, the principles were turned into a submission to an inquiry and participants gave evidence to Senators. In Ghana, young people identified multiple stakeholders, from Ministers to business titans, who they are writing to. In Slovenia, throughout 2023 are being used to inform an exhibition about young people’s privacy with Information Commissioner invited to attend.

The reaction from decision-makers was enthusiastic, but the young people’s input sat outside the change-making cycle. For example, teachers welcomed knowing what young people wanted to learn, but were not in a position to change their core curriculum. Senators and regulators thanked us for the information, but were not in an active cycle of rule-making to deliver the changes the young people requested.

But this does not mean these engagements have no value, just that we may not be able to fully track the discreet impact of these young people’s contributions. For example, in Antigua & Barbuda, staff at the Department for Education began a scoping note exploring progress against their 2013 ICT in Education policy. Or in Australia, the Senator’s inquiry may feed into an ongoing review of privacy law. Or in Slovenia, the Information Commissioner may engage with the Europe-wide process about children’s data across 2023.

There is an old English adage that suggests the people in positions of power “ignore the youth at their peril”. Ensuring young people’s perspectives are understood and heard is vital to ensuring their right to participate is realized. But it may also be essential to ensuring that data privacy and information security practices are improved in ways that meet whole-of-community expectations. If these decision-makers heed these young people’s feedback, it is possible that positive changes could be made for everyone, including young people.

VI. CONCLUSIONS

Young people have a clear idea of what their privacy is and what it feels like. Privacy is a legitimate expectation or right to

concealing information, from potentially intrusive ‘others’, and creates a feeling of safety and security. Young people did not trust that their privacy was well respected, and noted multiple concerns about the way their personal information flowed in the digital world. These inappropriate practices and undesirable flows were normalized, but not accepted; young people were able to identify ten principles they believed should be enacted to improve their privacy, from more control, transparency to greater support and education. Many of these principles take aim at the commercialization of their personal information.

Involving young people in discussions about privacy and information security is important, if we are aiming to develop solutions that serve all members of the community. The small-scale action-research components outlined in this paper suggest that there is an appetite from decision-makers to engage with young people. Whether or not this engagement is used, in turn, to develop better privacy and information security policies and practices remains to be seen. It rests on the willingness of decision-makers to share their power and integrate their thoughts and perspectives into their work.

ACKNOWLEDGMENTS

With thanks to those who supported the young people’s involvement; the Y in Australia; Child Online Africa & Awo Aidam Amenyah in Ghana; VSAK Institute in Slovenia, and; Department for Education and DadliBots in Antigua & Barbuda.

REFERENCES

- [1] S. Livingstone, J. Carr & J. Byrne 2016 *One in Three: Internet Governance and Children’s Rights Innocenti Discussion Paper 2016-01* UNICEF
- [2] A. Lenhart & K. Owens 2021 *The Unseen Teen: The Challenges of Building Healthy Tech for Young People Data & Society*
- [3] G. Mascheroni & A. Siibak 2021 *Datafied Childhoods: Data Practices and Imaginaries in Children’s Lives* New York: Peter Lang, pp.9
- [4] P. Kumar, S. Naik, U. Devkar, M. Chetty, T. Clegg, & J. Vitak 2017 “No Telling Passcodes Out Because They’re Private”: Understanding Children’s Mental Model of Privacy and Security Online’ *Proceeds of ACM: Human-Computer Interaction*, 1, CSCW, Article 64
- [5] G. Wang, J. Zhao, M. Van Kleek, N. Shadbolt 2022 ‘Don’t make assumptions about me!’: Understanding Children’s Perception of Datafication Online. *Proc. ACM Human Computing Interaction* 6, CSCW2, Article 419
- [6] A. Third & L. Moody 2021 *Our Rights in the Digital World A Report on the Children’s Consultations to inform UNCRC General Comment 25* Sydney: University of Western Sydney
- [7] M. Stoilova, R. Nandagrir & S. Livingstone ‘Children’s understanding of personal data and privacy online—a systematic evidence mapping’ *Information, Communication & Society* 24(4) pp. 557-575
- [8] V. Barassi 2020 *Child | Data | Citizen: How Tech Companies are Profiling Us from Beyond Birth* Boston: The MIT Press

- [9] J. Byrne, E. Day & L. Raftree 2021 *The Case for Better Governance of Children's Data: A Manifesto* UNICEF
- [10] BBC News 2020 "A-Levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco"
<https://www.bbc.co.uk/news/education-53923279>
- [11] J. van Dijck. 2014 'Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology' *Surveillance and Society* 12(2) pp. 197-208
- [12] A. Westin 1967 *Privacy & Freedom* New York, Athenium
- [13] H. Nissenbaum 2004 'Privacy as Contextual Integrity' 79 *Washington Law Review* 119
- [14] N. Gerber, P. Gerber & M. Volkamer 2018 'Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior.' *Computers & security* 77 (2018): 226-261.
- [15] United Nations 1989 *Convention on the Rights of the Child*