CHAPTER 7

Smartphone privacy

Finnish young people's perceptions of privacy regarding data collected when using their mobile devices

LIISA A. MÄKINEN & JOHANNA JUNNILA
DEPARTMENT OF GEOGRAPHY AND GEOLOGY, UNIVERSITY OF TURKU, FINLAND

ABSTRACT
In this chapter, we explore Finnish teenagers' experiences and understandings of privacy concerning the data stored in and flowing through their smartphones. Building mostly on qualitative interview data collected in Finland, we investigate what kind of factors are meaningful for young people when thinking about privacy on mobile devices, and how the level and nature of privacy required depends on the audience. Our results reveal that banking information, passwords, fingerprints, and locations were considered the most private information on smartphones. A myriad of personal factors affected how certain information was deemed more private than other kinds, hinting that much of this judgement lies in the context. Privacy matters to young people, but it seems to hold more meaning in social contexts and often remains overlooked in institutional settings, where the potential risks of privacy losses may seem unclear, abstract, or even irrelevant.

KEYWORDS: privacy attitudes, smartphones, applications, tracking, teenagers

Mäkinen, L. A., & Junnila, J. (2023). Smartphone privacy: Finnish young people's perceptions of privacy regarding data collected when using their mobile devices. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 145–166). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-7

Introduction

Young people spend much of their waking hours on their smartphones and online. In Finland, 99 per cent of people aged 16 to 24 use the Internet on a daily or almost daily basis, and 98 per cent use it on their smartphone (Statistics Finland, 2021). During the 2000s, the mobile phone became "woven into the fabric" of young people's lives as a source of entertainment, a creator of social stimuli, and an aid to escapism (Grant & O'Donohoe, 2007: 232). Contemporary smartphones are used for communication, social media activities, creating and consuming media, playing, reading, navigating, shopping, studying, monitoring health, and seeking information. They allow children and young people to communicate privately with their friends, explore different identities, and learn social skills independently. As such, smartphones can be "tool[s] for autonomy and freedom" (Vickery, 2015: 284), but they are simultaneously collecting vast amounts of data regarding these personal communications, daily activities, and social contacts. Indeed, while smartphones may bring young people certain freedoms in communication and mobility, they can also be used by parents to monitor and supervise their children's behaviour (Barron, 2014; Oostveen, 2014; Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021).

How children and young people use their mobile phones has been the focus of much sociological research over the last few years. Topics have included parental surveillance practices (Barron, 2014; Devitt & Roker, 2009; Fotel & Thomsen, 2003; Oostveen, 2014; Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021; Williams & Williams, 2005; Wisniewski et al., 2022); texting and sexting[1] (Grant & O'Donohoe, 2007; Hasinoff & Shepherd, 2014); and targeted advertising (Chen & Wen, 2022) (for other examples of highly cited articles relating to young people and mobile phones, see Yan, 2018). Research on this topic is complicated by the fact that the phenomenon is often analysed not as a separate subject, but as part of a bigger whole. This bigger concept of a media ecology, with smartphones often at its centre, describes how traditional and digital forms of media are now often combined for a variety of purposes (Ito et al., 2008; Vickery, 2015; Wisniewski et al., 2022). Consequently, much of the research on how young people communicate online is also relevant to the present study.

It is nevertheless surprising that only a few researchers have focused on privacy in the context of mobile phones and young people; these studies have focused either on how they communicate on their smartphones, or more recently, on location-tracking technology. For example, Ian Grant and Stephanie O'Donohoe (2007: 236) analysed perceptions of texting in their research on young people's motivations for using a mobile phone, arguing that young people see their smartphones as a "private form of communication". Similarly, but in a more specific context, Amy Adele Hasinoff and Tamara Shepherd (2014) found some widely accepted and shared norms for

privacy in sexting. Meanwhile, in 2015, Jacqueline Ryan Vickery based her ethnographic research on the social privacy challenges facing young people from low-income and non-dominant social backgrounds, concluding that they negotiate and manage their privacy by developing various deliberate strategies to resist social convergence and adult- and peer-surveillance. While context-specific, these studies show certain commonalities and indicate how mobile-device privacy is important even in challenging circumstances. More recently, privacy has become a relevant frame in research examining family use of location-tracking apps on mobile phones, in terms of how location tracking is perceived, used, negotiated, and resisted by parents and young people alike (Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021).

While these studies provide important insights into young people's perceptions of privacy in the mobile context, none take into consideration the vast scope of data that such devices store and share. As well as storing details of one's location and private communications, mobile devices (and the apps on them) store contacts, photos, videos, recordings, passwords, banking information, social media interactions, information on the surroundings of the device, and biometric data – all of which is directly traceable to the user. Each smartphone has a unique ID distinguishing it from others which cannot customarily be disabled by the user. This ID can be used, for example, by a manufacturer or service provider to collect data on the calls and messages made, and this also counts for the installed apps. Before installing an app, the user is usually required to give their permission for it to access certain information on the smartphone. This information will concern use of the app, but may also include contacts, call logs, schedules, location data, or Internet data, which can then be sold by the app provider to third parties. As data is collected by multiple actors and stored in various locations, it is often difficult or impossible to ascertain exactly where one's data is stored, who has access to it, and to whom it might be sold in the future (Aditya et al., 2014; Furini et al., 2020, Ketelaar & van Balen, 2018; Martin & Shilton, 2016; Sipior et al., 2014).

Thus, privacy is particularly pertinent in the smartphone context due to the many layers of data collection and the number of actors involved. In this chapter, we analyse qualitative data gathered from young people in Finland about how they define privacy and its limits in the mobile context. Our work was guided by two main research questions: 1) what information do young people consider to be most private or personally sensitive to them on their smartphones; and 2) who are the people they want to share that information with, or hide it from? The rest of this chapter is structured as follows: first, a brief introduction to existing privacy research, especially regarding young people's views on it; then, a presentation of our data and methods, followed by a detailed analysis of the two research questions; then, our results in the context of existing research; and finally, our conclusions.

Briefly on privacy

Although extensive research on privacy dates back at least a century, controversy still surrounds its precise definition. Focusing on the aspect of information control, one definition is that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967: 5). Understood this way, privacy focuses on the individual, and is a means for reinforcing individuality (Bennett, 2011). Another classic definition of privacy focuses on its social value, arguing that privacy is "an interpersonal boundary control process" (Altman, 1976: 27). The boundary is one between "closedness and openness" and, rather than being fixed, is negotiated through social practices (Steeves & Regan, 2014: 303). In this respect, privacy acts as a means for creating and maintaining social relationships, determining the nexus, or balancing point, between the need to withhold personal information (in some contexts) and the need to divulge it (in others). As such, privacy is often perceived as a trade-off in which the benefits of sharing are weighed against any possible negative repercussions – this is often referred to as privacy calculus (Baruh & Popescu, 2017; Marwick & Hargittai, 2018; Steeves & Regan, 2014; Vickery, 2015).

The context of where information sharing takes place is perhaps the most important factor in analysing issues of privacy. To this end, Helen Nissenbaum (2004, 2010) has suggested a framework for determining the contextual integrity of privacy. She argued that in any context or sphere, there are two types of informational norms which apply: "norms of appropriateness", which deem what is appropriate to reveal; and "norms of flow or distribution", which deem who this information should be shared with (Nissenbaum, 2004). Privacy is thus greatly affected by the kinds of social norms applied. This also manifests itself in the way some forms of surveillance might go unproblematised in certain contexts but provoke criticism in others. Nissenbaum's contextuality framework is thus a useful tool for analysing young people's privacy attitudes and strategies, as they communicate with a multitude of different audiences on a variety of platforms, many of which are online. These are complex to analyse, however, as online environments consist of different, overlapping contexts, some of which may be combined with offline relationships to varying extents, depending on the platform. These overlapping contexts and the ways in which performances flow between them also complicate online privacy (Steeves & Regan, 2014). Meanwhile, smartphones complicate the situation further; in addition to information flowing between various online environments, data and metadata are also often collected without the user's knowledge and sent to locations unknown to them. Smartphones are used in contexts where risks are perceived and accepted differently, depending on the social norms and what is known or presumed about the flow of data.

In addition to this contextual value, Valerie Steeves and Priscilla Regan (2014) argued that privacy has performative, dialectical, and relational value for young people too. Performative value comes from the need to have a private or safe space to explore identities. Dialectical value comes from the need to find balance between public and private needs through constant negotiation. And relational value emphasises the need for reciprocity in any social relationship when sharing information. If it is only shared unilaterally, the relationship is instrumental and can only ever be, at most, consent-based. Consent is founded on the idea that organisations notify users about their information policy, and users make informed decisions based on that; this is seen to protect privacy. This approach, however, has only a narrow understanding of what the lived realities of privacy are, and there have been many critiques of the privacy self-management paradigm, especially in the face of expanding algorithmic surveillance and the use of Big Data (e.g., Baruh & Popescu, 2017; Lehtiniemi & Kortesniemi, 2017; Steeves & Regan, 2014; Solove, 2013).

Steeves and Regan's (2014) typology of the various social values of privacy demonstrates concrete ways in which young people negotiate their privacy online, and it also offers tools for contextualising how young people experience privacy. Youth researchers generally agree that young people *do* care about their privacy, and while privacy may be contextual and networked, it has not lost its meaning for teenagers in the social media era (boyd, 2014; boyd & Hargittai, 2010; Cocq et al., 2020; Livingstone, 2008; Marwick & boyd, 2014; Marwick & Hargittai, 2018; Steeves & Regan, 2014; Stoilova et al., 2020; Vickery, 2015; Wisniewski et al., 2022). Although privacy management may indeed be difficult, young people have several ways to micromanage their online practices on a day-to-day basis. Without wanting to hide "anything 'bad'", they still want to "control the context in which information is disclosed and shared, as well as to control access to their digital identities, spaces, and devices" (Vickery, 2015: 281–282; see also Cocq et al., 2020; Marwick & Hargittai, 2018; Wisniewski et al., 2022).

In recent decades, research has duly recognised the magnitude and complexity of surveillance for everyone – not just young people. However, a more precise analysis of particular age groups – and their personal or individual experiences of being monitored in different surroundings and contexts – is still needed. Research on the relationship of children and teenagers to privacy increased in the 2010s, but the focus has so far generally been on interpersonal contexts rather than organisational and commercial contexts, where data is not so much actively given out as automatically harvested (Stoilova et al., 2020).

We recognise that in analysing how surveillance is felt and perceived on an individual level, many surveillance scholars have argued that privacy is an inadequate concept (Ball, 2009; Bennett, 2008; Gilliom, 2001). Nevertheless, in the context of this research, it offers a valid conceptual tool for analysing different levels of data collection, various data items, and the complex per-

ceptions that young people have towards these issues. While recognising the challenges of investigating surveillance in the context of privacy, we also see that privacy remains an important "way to frame the contemporary problem, as a regime of governance and as a set of practices" (Bennett, 2011: 486).

To summarise, online environments (including smartphones) are complex surroundings from a privacy perspective. They enable young people to create, develop, and test their identities, but at the same time, they are subjected to vast amounts of visible and invisible monitoring from their peers, commercial actors, and government organisations (Regan & Steeves, 2010; Steeves & Regan, 2014). As smartphones are primarily used for online activities, their use should also be analysed as a complex web of displaying information for some while hiding it from others, and for managing not just audiences, but also one's own actions. Simultaneously, it is important to bear in mind that young people and (adult) society may well have different understandings of "the social contexts in which teens disclose information, perform identity, and communicate with one another" (Vickery, 2015: 282; see also Herring, 2008). To get a better idea, then, of precisely how information is shared between people, organisations, and these various social contexts, we must ask young people themselves.

Data and methodology

The data for this research was collected in Finland between March 2020 and December 2021 as part of a larger research project examining the subjective experiences of surveillance. The participants were recruited through schools, municipalities, and nongovernmental organisations in two large Finnish cities. Altogether, 37 people aged 12 to 19 participated in this research: 24 of them were girls, 10 boys, and 3 identified as other or did not reveal their gender. The data collection used a mixed-methods approach combining concept mapping, Q-sorting, and in-depth interviews; not all participants took part in all three data collection methods. This chapter uses all the data collected from all 37 participants but pays closest attention to the qualitative interviews conducted with 14 of the participants. The overall data collection process, its methodological framework, and the size of each dataset are described below.

The data collection in its entirety was built on a 51-item list entitled "What my phone knows about me".[2] The list included items such as basic information (e.g., name, age, occupation); contact information (mobile phone number, e-mail, home and work addresses); online communications and social activities (e.g., the content of messages sent and received, a list of the words used in messages); metadata (e.g., where and when messages were sent and received, where each photo was taken, how often each app was used); location data (e.g., current location of the smartphone, information about regularly visited locations and usual routes); biometrics; content stored on the smartphone

(such as documents, photos, and recordings made on it, downloaded to it, or uploaded from it); items relating to what the smartphone can "see" or "hear" with its microphone or camera; details about purchases made on the smartphone; banking and credit card information; and passwords.

Data collection began with a concept-mapping exercise, where participants were asked to rate each item listed on a 1–5 scale according to how sensitive or private they considered it. Participants were also asked to rate each item based on how comfortable they would feel revealing that information to three separate groups: people close to them, people they knew in their community, and people or organisations they did not know. Concept mapping, as a participatory qualitative research method, was originally developed by William M. K. Trochim (1985) as a means of using quantitative data to provide "structure and objectivity to qualitative data" (Burke et al. 2006: 1393). An online version of this method was used via the GroupWisdom™ site, with 30 participants.

Next, we conducted semi-structured qualitative interviews with 14 participants (11 girls, 2 boys, 1 other), who were all aged between 15 and 19. We conducted four interviews of which two were in person (with one researcher participating face-to-face and one remotely) and two, due to the Covid-19 pandemic, fully remote via Zoom. One interviewee was met one-on-one, while the rest participated in focus group interviews. The interviews each lasted 60–95 minutes (average 80), with a combined length of 5 hours and 20 minutes. The discussions were then transcribed, resulting in 111 pages of data. The interviews began with a Q-sorting exercise. Like concept mapping, Q-sorting is a three-step method – participants firstly rank a set of items on a fixed rating scale, and then the rankings undergo quantitative and qualitative analysis (for more on methodological issues, see, e.g., Rost, 2021). In this Q-sorting task, participants ranked the same 51-item list used in the concept-mapping exercise. They began by choosing three items that described topics they considered to be the most sensitive or private, and then three that were the least. After that, they chose four of each, then six, and finally, eight. An online platform called Miro (www.miro.org) was used for the task when it was done remotely, and small cards were used in the face-to-face meetings. This resulted in 13 Q-sorting tables being returned, which, along with the concept-mapping tasks, could then be discussed in the interviews. Additionally, the interviews focused on three broad themes: 1) privacy in general (e.g., what it is, how it is defined, its value, reasons for privacy, and the consequences of privacy invasions); 2) privacy as a contextual process (who they want privacy from); and 3) privacy in the specific context of one's mobile phone (e.g., whether the participants think about surveillance and data collection when using their smartphones or manage their privacy settings somehow).

The interviews were analysed using data-driven, qualitative content analysis focusing on the specific research questions and building on replies received from

the Q-sorting task. Content analysis is a common and flexible method of analysis for many different types of qualitative data. It can be used on its own or in combination with, for example, discursive or thematic analysis, and allows the data to be quantified to some extent, even if no actual statistical correlations are sought (Prior, 2020). The interviews were analysed using NVivo-software, and the quotes in this article were translated by the authors after the analysis. Pseudonyms have been used throughout for all the participants.

The quantitative methods – particularly the Q-sorting task – offer a backdrop for the descriptions of how young people perceive private information. However, the focus of this chapter is on the qualitative interviews and achieving a deeper understanding through their in-depth analysis. While the number of participants is small – meaning the results are not generalisable to those of a similar age in Finland (let alone globally) – they do shed light on the kinds of views and experiences young people have about smartphone privacy in the 2020s. The study was also reviewed and approved by the Ethics Committee of the University of Turku. In the next two sections of the chapter, we first examine which items our participants considered most private to them and their thoughts on why, then we analyse the different audiences envisioned by them – in particular, those they wanted to hide information from. Following these two analysis sections, our results are then discussed in a wider context and some conclusions drawn.

Young people's perspectives on privacy concerning specific data items stored on their smartphones

Of all the information stored on their smartphones and apps, respondents considered credit card and banking information to be the most private. In the Q-sorting task, credit card and banking information was chosen by 12 of the 13 as one of the three items most private or sensitive to them personally, and in the concept mapping it was given a rating of five (extremely sensitive or private) by all respondents (N = 30). Credit card and banking information were thus considered very private, as they concerned money and were thought of as information belonging to no one else. As one of the interviewees, Iris (aged 19) said: "Then there's my banking information. I'd prefer not to have it as public information, because it's my money and it doesn't concern anyone else". In addition to concerns of losing their money, the respondents also worried that someone could gain access to other private information using this data: "With banking information", Oliver (aged 15) observed, "you can gain access to someone's health records, which can be sensitive, or someone might think they are".

The passwords on a mobile phone were the next most often mentioned: seven participants chose them as one of the three most private pieces of information (with an average rating of 4.50 from the concept mapping re-

spondents). The issue of passwords also revealed some ways in which young people aimed to manage and protect their privacy: "I put strong passwords on my phone so that nobody can get information from it", noted Alva (aged 17), and "I also save all my passwords on paper. I write them down so that I don't have them anywhere digital".

The fact that credit card and banking information and passwords were chosen as the most private or sensitive data by so many respondents shows a somewhat technically oriented and formal approach to privacy and a very tangible understanding of the kinds of risk associated with access to finances or other sensitive information protected by this data.

The third choice varied more, but fingerprints were among the most frequent (three mentions and an average rating of 3.87). In terms of content, fingerprints are closely attached to the two former items, because like passwords, and to some extent banking information, they can be interpreted as a means of accessing other information: gateways to something *more* valuable. Rosa (aged 16), for example, stated that "with [my] fingerprints, you can get into my phone […] and my phone has all the information you've listed here".

In addition to fingerprints, the item list included two other biometric details: "what my face looks like" and "what my voice sounds like". Face and voice, however, were not seen as being nearly as sensitive forms of information as fingerprints. Indeed, most participants ranked them as "not at all sensitive or private" to them. The interviews revealed that the potential uses of biometric recognition were unclear to many respondents:

> And then, of course, my fingerprints, because I don't want to be framed for a crime [laughs] […]. It sounds far-fetched, but couldn't they actually do it? I mean, like, murder someone and put my fingerprints there, and then it's my fault? (Kris, aged 16)

> Julia: But this is also a bit double-edged, "what my voice sounds like"; what if someone takes my voice and does something with it?
> Sara: But what would they do with your voice?
> Julia: I don't know.
> Kris: […] I mean, nowadays you can do anything.
> (Sara & Julia, aged 15; Kris, aged 16)

> Rosa: Is my face private?
> Sara: No, I can see your face [laughs].
> Kris: It's a little private because you have, for instance, Face ID.
> Sara: Yeah, but…
> Zelda: Even if you had a picture of Rosa, you couldn't get into her phone.
> Kris: Couldn't I?
> Everyone else: No!

Rosa: You'd need… like a 3D […]?
Sara: But where would you get a 3D image of Rosa […]?
Kris: I wouldn't, but someone could.
(Kris, Rosa, & Zelda, aged 16; Sara & Julia, aged 15)

The above quotes show how the respondents ponder what might be done with their voice or an image of their face, but because they do not know, they end up not choosing these as being some of their most private information. We witnessed similar confusion around other items on the list, such as "the phone's unique device ID number" – in almost all interviews, the participants asked what it actually meant.

The last item on many respondents' list of three was either something relating to location (altogether eight mentions for five different items) or something relating to personal content stored on the smartphone (a total of seven mentions for three different items). Participants thought the idea of someone they did not know being able to track their location to be "scary", "disturbing", "annoying", or "plain creepy". For example, Rosa (aged 16) explained that "it's a little disturbing if someone knows precisely what time you go to school and which way you go there and so on". Similarly, Mia (aged 16) explained that she chose "my direction and speed of movement" as one of the most sensitive pieces of information, arguing that "if someone knows that, then they also know my location, and it's quite a serious security risk". Location data was also seen as necessary to protect for personal reasons, such as going to the doctor's office, or not wanting to reveal who one is spending time with.

When moving on to the next four most private or sensitive items, information concerning location was chosen more regularly, cited altogether 18 times (across seven different items), with the single most often mentioned of these being home address (eight times). This seems particularly interesting, as in Finland, people's home address is quite easy to get from public registers: Anyone can find out where anyone else lives with a single SMS or a call, unless the person in question has specifically denied access to that information. Home address was linked to security issues and feeling safe in one's own home. Sara (aged 15), for example, talked of her home needing to be "like your own place where you'd want to be safe, and you wouldn't like if everyone knew where you lived and could come there".

One item particularly worthy of mention here, because it provoked quite different responses – exemplifying how perceptions of privacy can vary wildly – was gender. Most respondents were completely indifferent to it, considering it one of the most public pieces of information. For example, when Kris (aged 16) was asked about the items they felt least sensitive about on the list, they replied, "my name, age, and gender, they are things I could tell anyone the moment I meet them". However, our dataset included some respondents who had non-binary thoughts about their gender or did not want to reveal

it. For some of these participants, gender was therefore a more sensitive issue and private information. The difference between Kris's response above and Nova's response below is striking in this respect, highlighting just how contextual privacy is – not only in terms of who is telling what to whom, and in which particular situation, but also because the same issues may have completely different meanings for different people:

> Well, my gender is like… I wouldn't say, somehow, I wouldn't say that I'm a woman, but I wouldn't go as far as to say non-binary. So, because of that, it's a really sensitive subject for me, and I would like to keep it secret. [...] I don't know, I feel like everyone is labelling [each other], and I can't really talk about these things very publicly. [...] So because of that it's a bit more of a private issue. (Nova, aged 18)

Young people's considerations of privacy in terms of which specific audiences can access their data

There were some variations in how young people viewed the data stored on their mobile phone, and who they felt comfortable about being able to access it. In other words, we were asking them what they thought about privacy in terms of sharing data with specific audiences. Participants also gave their own unprompted examples of such audiences, their own definitions of what privacy means, what makes something private, and how privacy can be violated. Specific audiences cited by the participants included unknown people, acquaintances, ethnoreligious communities, friends, relatives, family members, and just themselves. Some references were made to partners, authorities, or organisations – but they were surprisingly few. Below, we consider these different audiences one by one, proceeding from wider or unknown audiences towards people closer to the participants, and then to institutions. We conclude by connecting these audiences to participants' notions of the differences between online and offline environments.

Thinking about an unspecified "someone" or "everyone" provided the general baseline for participants – the "gut feeling" of privacy, per item. Alva (aged 17), for example, said "I'd like to have privacy from anyone whose name I don't know – that's like a good basis for me. Usually, if I know someone's name, I know that person at least to some extent". Groups of unfamiliar people with slightly different nuances were also mentioned by participants: people whose names they did not recognise, or they did not know but their friends did, and foreign people (insofar as it came as a privacy violation from someone abroad). There were also certain information participants did not want to share with anyone else, either because it was extremely intimate or just for the joy of being able to do something without anyone asking questions:

> As a rule, you may just want to feel that you can keep some things to yourself. That you don't have to worry that some things about you will get spread about without you having any control over it. So, in that way, [I want privacy] from everyone. (Iida, aged 17)

A connection with someone of some kind usually made sharing information feel more natural. Indeed, some participants referred to privacy in terms of trust. They wanted people close to them to respect their privacy, explaining that this meant they could trust that their personal matters were safe with these people. In this respect, private information was seen as something that is not fully exclusive yet expected to stay within only a small circle. However, other participants felt more at ease revealing something to complete strangers – for example, issues that were personal to them but that they knew someone already in their lives would not understand or appreciate. Relationship status was one such issue: For some, it felt more comfortable to share this with complete strangers, as then it was less likely to reach people closer to them whom it might upset.

Interestingly, it was the acquaintances that participants knew partly but not closely that some wanted privacy from the most – people with whom they did not have any really meaningful relationship or mutual trust, yet from whom they also lacked comfortable anonymity:

> The people you don't know that well but who you meet occasionally, like acquaintances, are maybe the worst. I mean, you know you'll meet them again sometime, but you don't really know them. If they were just someone you'll never meet again, it would not feel so difficult. (Maria, aged 16)

This might partly explain the popularity of anonymous apps, such as Jodel, which many of the participants used. According to them, its anonymity provided a suitable place to ask "stupid questions" that they might otherwise have never dared ask. However, it was also a location where bullying and trolling were rather common, and it became apparent that Jodel was a place of only partial anonymity, as it blended online and offline life, since many schools had their own channels on the app.

In terms of family, relationships with parents were closer for some participants than for others, but most required some modicum of privacy:

> [You do want some privacy] also from your family, especially at this age, you need your own space and so on. Your family doesn't have to know everything that's going on in your life. I also feel it's good to keep some things just to yourself […]. You don't have to always share everything. (Sara, aged 15)

In some cases, this desire for privacy also made some participants approach their parents about it and consider decreasing the number of digital traces they left behind. With some amusement, Zelda (aged 16) explained how she

found out her father could track her whereabouts during the school day by monitoring her purchases: "I was just surprised [that my father could see where and when I'd been using my bank card]. Then I was just like 'okay, in certain situations, I'm just going to have to use cash'". Indeed, most of the participants had their own smartphone already as younger children, so they were used to parental controls, mobile-enabled tracking, and negotiating with parents about smartphone use. However, as they had become teenagers, parental attempts to control their activities had decreased or changed in form – parents were usually more concerned about the length of time spent on screens rather than what they were doing on them:

> For ages I had one of those screen time apps, where you could see what apps I use, for how long, and how long I'm allowed to use them [...]. Now I'm about to turn 18, so they don't follow it that much anymore. (Camilla, aged 17)

> One thing that really annoyed me was they wanted to know my location all the time. [...] I feel old enough now to take care of my own whereabouts, and I always tell them where I am, but they still wanted to know it. [...] But then we talked about it and decided that they don't have to track it. (Rosa, aged 16)

Location tracking was not a simple issue, however. While participants generally wanted some privacy about their location, they also felt that sharing it with family or other people they trusted was sometimes a useful safety measure, actively sought from parents, or in some cases even close friends, when this feature might also serve social purposes – such as planning gatherings:

> My parents have never wanted to track my location or anything. When I was younger, I probably wouldn't have wanted to let them know, but just recently, when I said "hey, I've put [my location] on now so you can see where I am if someone tries to kidnap me", my parents were a bit like "why should we know where you are?" And I was like "well... because I want it!" (Kris, aged 16)

> Iida: I don't have anything like that [location tracking] with my parents, but I do have with my friends. [...] If one of us goes missing or something happens, we know where they are. [...] It was our mutual decision, so that if someone needs help or their phone dies, you can know exactly where they are. [...]
>
> Interviewer: So, it's ok to check and see where your friend is right now?
>
> Iida: [Yes.] We also use it, for example, if we are going to meet, to check when the others are leaving [home]. None of us is usually late or too early because everyone knows where everyone else is. (Iida, aged 17)

When asked to think about different forms of institutional surveillance, most participants expressed trust in the Finnish authorities and thought that their data was safe with them, referring to how authorities are obliged by law and employment contracts to respect confidentiality. For example, Leo (aged 15), explained how this type of organisational surveillance is "not that big a problem, if they use the data responsibly, so the police are not giving it out". Trusting the authorities with personal information meant one could expect "proper privacy" – as one participant put it:

> In that way, it's easy to disclose [information] to them because they're... bound by professional confidentiality. I trust that my data stays safe, because it's [written] in their employment contract, after all. When they got the employment contract, they signed it and agreed to it, so then I trust it too. (Iris, aged 19)

However, some participants had quite a different opinion: Some referred to leaks and other mishandlings of personal data that have happened and diminished their trust in organisations and authorities. "To be honest", admitted Nova (aged 18), for example, "I don't trust [authorities or organisations]. I've seen so much news about e-mails getting leaked, that to my mind, it's very alarming. I mean, you just can't tell... anyone could do it, so no, I don't trust [them] that much". Some participants were therefore strongly against organisations and commercial entities gathering and selling their data for profit, sometimes comparing different companies by the reputation they had in managing their customers' data. Others did not find it quite as problematic, focusing on the benefits of customised advertising, or else they saw data collection as something that all companies must do. Most participants, however, had no strong opinions one way or the other.

The discussion about different audiences tended to focus on possible privacy violations: Participants considered both the nature of shared information and possible consequences of privacy breaches when deciding whom to trust with their information. However, in social contexts, privacy violations were not seen in black-and-white terms; they were considered less severe if they happened by accident or stemmed from good intentions, such as caring about someone's well-being. As for institutional surveillance, participants also referred to the trade-offs needed to operate in the smartphone culture of today, where participation without giving away personal information is increasingly difficult. Some participants also thought that since their personal data was only the tiniest fraction of a much bigger mass of data, it was largely irrelevant. Regardless of the exact audience, however, many participants felt it was disturbing that people could make decisions based on knowing things about them; especially when it was information they did not realise was being collected in the first place, could not access themselves, or that came from many sources. "It's a bit scary", observed Kris (aged 16). "If you look

at this... 'a list of the words I use in text messages and e-mails', not even I have any idea what they could be".

Participants referred to situations where they actively managed their different audiences by making decisions about privacy or sharing based on trust, previous experiences, or other factors. Technical measures were considered important too, especially when travelling abroad, as one could not be so sure of the situation as at home:

> I protect my device when using a public network. If someone breaks into that public network, at least my data won't be stolen. There are some skilful hackers and such [...]. Maybe not that many in Finland, but if I go abroad, I protect myself. (Iris, aged 19)

However, other people were not just seen as potential audiences for leaked private information, they were also seen as individuals who themselves have their own expectations of privacy. For many participants, other people's privacy was very important, and some were even in positions of trust themselves (e.g., at school or in politics). This meant they handled information regarding others and needed to take care, especially with contact information and messages. "Messages and calls, well, they are not exactly private as such", remarked Nova (aged 18), for example, "but [...] some people might come to me with things they don't want other people to know about. That's why I am careful, too".

All the participants considered the norms and issues governing privacy online and offline to be quite different. Managing information online felt significantly more difficult, to the point that offline information seemed far less of a problem to manage that any information spreading online. For example, Oliver (aged 15) explained:

> In "real life", if you don't tell anyone anything sensitive about yourself, then in principle it can't spread, whereas online, someone can just dig up all the information [you might not have filtered] from your profile, without you being able to do anything.

Other differences which made information management online more difficult than offline was the speed with which information could spread, how such audiences could be much wider and unknown, and that screenshots could be taken of private conversations as damaging "proof".

> You're much more vulnerable [online] to privacy violations, since you are more in control of what you tell others [offline]. For instance, if you tell a friend something, that friend can't share that so easily. But if you send a message, it stays there, and it's much easier to share. (Sara, aged 15)

However, it was also noted how it is possible to decide whether you show your face or name online, while in public, these are more difficult to keep

private. The Covid-19 pandemic has brought some interesting nuances to this distinction, though, now that using a face mask in public has become quite commonplace and many traditional face-to-face events and concrete environments, such as schools, have at least temporarily moved to being done remotely online.

In conclusion, participants recognised various kinds of audiences and degrees of privacy which distinguished these audiences. In general, they felt more comfortable sharing information with people closest to them, but sometimes anonymity encouraged openness and was also considered a safe place to share personal issues. Lastly, most of the participants trusted their data with national authorities, but opinions were divided when it came to private organisations using and selling it.

Discussion

Through analysing young people's perspectives on smartphone privacy, we found that participants most often referred to items of a more technical and formal nature (i.e., banking information, passwords, and fingerprints), which, if leaked, would have the most directly tangible effects (e.g., financial losses). These data items were generally felt to be easier to control compared to, for example, the continuous and hidden accumulation of message or location data. While the need for privacy can be seen as a desire to protect "both tangible and intangible properties" (Furini et al., 2020: 1055), tangible information is more likely to be easier to recognise and protect. It is also worth noting that, although some data items are considered sensitive regardless of the context in which they are shared, there are also certain contexts which are consistently more sensitive than others. Banking, for instance, is one such context where privacy has always been found to be important (see, e.g., Martin & Shilton, 2016). Choosing to engage in any kind of financial transaction online, particularly via a mobile device such as a smartphone, is thus often preceded by careful consideration of the trustworthiness of the site (Marwick & Hargittai, 2018). This technical data with tangible effects can also be understood as a kind of liminal form of information because it also acts as a gate through which other information or vulnerable online spaces can be accessed. In Finland, online banking details are used as secure login data for online sites and services in many areas (e.g., social security, welfare, healthcare, taxes, electricity, and insurance), so losing that data could lead to a lot more than just financial losses.

Overall, our data revealed that the concrete risks of privacy breaches, such as physical safety, were of most concern to participants, with the consequence that online risks were often overlooked, unless they, too, had physical consequences – particularly in cases where location data was compromised. These results perhaps reflect what is taught in schools about privacy online, where

the focus of e-safety is on the concrete threats of hoaxes and predators. This would also explain the often quite shallow understanding many young people displayed of the extent of institutional surveillance and data collected about them – and its potential consequences. Young people have rarely had any experience of privacy violations committed by an institution that might affect data sharing (Marwick & Hargittai, 2018; Stoilova et al., 2020).

While our participants' focus was on real-life risks, their expectations for privacy differed in online and offline contexts, and they decided what information they wanted to share, how, and to whom, depending on whether the context was online or offline. We argued above that privacy can be seen as "an interpersonal boundary control process" (Altman, 1976: 27), where the boundary between what is shared, where it is shared, and how it is shared, is constantly negotiated. The context where this negotiation takes place affects and is affected by individual privacy expectations. Examining privacy as a contextual process might seem inevitably difficult, as contexts are negotiated and fluid. However, previous research has proven that people's privacy concerns are *predictably* contextual and that it is possible to measure "nuanced, contextual concerns" and decipher which data types are sensitive in which contexts (Martin & Shilton, 2016: 211). Indeed, while the participants in our study had varied notions of audiences and the privacy of certain data items, there were some ideas shared by all.

We must bear in mind, however, that the context for sharing information via a smartphone is somewhat nebulous, as it will inevitably be leaked to more audiences than just the intended. The actions of smartphone users leave unintentional traces, which often makes it harder to manage privacy as one might like (see also Hasinoff & Shepherd, 2014; Steeves & Regan, 2014; Stoilova et al., 2020). Because of this difficulty, young people will control what they can – for example, access to the more technical, clearly defined data – or focus on the visible and intended audiences and disregard those which remain unseen (i.e., system-level data collection).

It has been argued that the audience matters as much as the information itself; that defining privacy should not be "tied to the disclosure of certain types of information, rather a definition centred on having control over who knows what about you" (Livingstone, 2008: 404; see also Livingstone, 2006). However, while this argument is pertinent to various social groups, it overlooks much of the institutional context of surveillance – as the young people in our study also seemed to do. Issues of privacy in social situations were dwelt on more than institutional types of surveillance. While the typical risks of system-level data collection were recognised – data exploitation, data loss, and data overreach (e.g., Aditya et al., 2014) – they were more an afterthought, barely affecting how information is shared between social groups.

In conclusion, we would argue that, rather than young people being unaware of the potential privacy risks they are taking, they are making a con-

scious choice – knowing full well it is one they cannot avoid. They understand and recognise (some) of the potential risks, but choose to not dwell on them, as doing so might prevent them from continuing to use their device (see also Marwick & Hargittai, 2018). So, if an individual really wants to address privacy issues in smartphone culture, it might mean not participating in it at all.

Yan (2018) has argued that the modern mobile phone has two core features: personalisation (as it aims to satisfy the individual user's needs) and multifunctionality (integrating features from other technologies and adding new ones). After examining how contemporary youths use their smartphones, two more core features become prominent: the phone's proximity to the user (as it is usually kept "within arm's reach") and its perpetual activity (as the phone is nearly always on and in almost constant use). These four features have strong links to questions of surveillance and privacy and resonate with our research findings.

As smartphones aim to satisfy all kinds of individual needs – be they physical, social, cognitive, or emotional (Yan, 2018) – it becomes useful for phone manufacturers and service and app providers to predict those needs. Thus, it is necessary to collect all kinds of data to create individual (consumer) profiles, which can then be used for the direct marketing of new services and apps. The aim of surveillance, then, is to sort people into categories for which services can be provided, turning surveillance into a form of social (and economic) sorting (Lyon, 2003). The fact that the smartphone fulfils one's specific needs makes any trade-offs in whether to use it or not trickier – it is difficult to reject a technology when it can bring so much personalised pleasure.

The multifunctionality of the smartphone means that the collection and storage of information may concern all kinds of daily activities – not just those connected with media use, but also other kinds of functions, from digital money (smart wallets, mobile paying) to measuring bodily activities (biosensors, self-monitoring apps) (Yan, 2018). Connecting many activities to phone usage that previously were quite separate increases both the volume and range of data collection and allows data to be combined and stored in an unprecedented manner. Thus, we would agree that "privacy threats from mobile devices are fundamentally different and inherently more dangerous than in prior systems" (Aditya et al., 2014: 7).

Furthermore, the phone's proximity to its user (see also Vickery, 2015) adds a deeper layer to this data collection, as the phone can not only collect biometric and location data on its user, but also "listen to" and "watch" them. Thus, in addition to location, activities, and encounters, the phone can collect and store "an audio-visual record" of its user's everyday life (Aditya et al., 2014: 7). While this can be, and often is, sold to the consumer through the discourse of ease and convenience, the fact of the matter is that there can be unexpected harm related to this kind of technological embeddedness in everyday life (see, e.g., Burdon & Cohen, 2021).

When it comes to keeping the phone on all or nearly all the time, one would think that young people would be able to negotiate the boundaries of their privacy, particularly in the context of parental supervision, by arguing that they had no battery power, and hence their phone was off (see also Barron, 2014). However, to actually turn one's phone off would mean disconnecting from everything. As the phone is personal, multifunctional, always with its owner, and always on, time spent fully offline is becoming rarer and rarer. Even though life online and offline might still be considered by many – including our participants – as separate contexts, they are often present simultaneously or can leak into one another. In this respect, the smartphone operates as a liminal device combining what is online and offline at the threshold between them.

Conclusion

The majority of young people (and not just the young) use their smartphones every day and all day. Contemporary smartphones are personalised, multifunctional, and perpetually close at hand. The amount of personal data collected by them and stored in them, and the ways in which they enable and contribute to the blending of online and offline realities – especially in young people's lives – suggest that issues of privacy are more important than ever. In this chapter, we aimed to investigate how young people understood privacy in terms of the data collected via their smartphones. By examining Finnish teenagers' experiences and thoughts on the matter, we found that there are details generally considered private (such as banking information, passwords, and fingerprints), but privacy priorities depend on the context, intended audience, and personal preferences. While our data showed there was some agreement about the sensitivity of certain data items, it also proved that there were individual differences in these perceptions.

Although privacy clearly matters to young people, they contextualise potential audiences of their data in a layered manner, and social contexts seem to be more important than organisational, commercial, or institutional settings. Thus, institutional surveillance and data collection often go unnoticed or are purposefully ignored, even though they are continuously happening at the system level. This might be because these risks seem unclear or abstract, but we would argue that they are consciously ignored to enable continued smartphone use.

Acknowledgements

The data examined in this chapter was collected as part of a larger project entitled "Living within, navigating and appropriating everyday surveillance: Case studies on subjective experiences of surveillance and privacy", funded by the Academy of Finland (SA 316013, 2018–2023). This particular study was planned in collaboration with the Canadian research project eQuality (funded by the Social Sciences and Humanities Research Council of Canada, 2015–2022).

References

Aditya, P., Bhattacharjee, B., Druschel, P., Erdelyi, V., & Lentz, M. (2014). Brave new world: Privacy risks for mobile users. *Proceedings of ACM MobiCom Workshop on Security and Privacy in Mobile Environments*, *USA,* 7–12. http://doi.org/10.1145/2646584.2646585

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behaviour*, *8*(1), 7–29.

Ball, K. (2009). Exposure. Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639–657. https://doi.org/10.1080/13691180802270386

Barron, C. M. (2014). "I had no credit to ring you back": Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance & Society*, *12*(3), 401–412. https://doi.org/10.24908/ss.v12i3.4966

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance.* MIT Press.

Bennett, C. J. (2011). In defence of privacy: The concept and the regime. *Surveillance & Society*, *8*(4), 485–496. https://doi.org/10.24908/ss.v8i4.4184

boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press. https://doi.org/10.1007/s10615-014-0512-3

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: who cares? *First Monday*, *15*(8). https://journals.uic.edu/ojs/index.php/fm/article/download/3086/2589

Burdon, M., & Cohen, T. (2021). Modulation harms and the Google home. *Surveillance & Society*, *19*(2), 154–167. https://doi.org/10.24908/ss.v19i2.14299

Burke, J. G., Peak, G. L., O'Campo, P., Gielen, A. C., McDonnell, K. A., & Trochim W. M. K. (2006). An introduction to concept mapping as a participatory public health research method. *Qualitative Health Research*, *15*(10), 1392–1410. https://doi.org/10.1177/1049732305278876

Chen, Y. K., & Wen, C. R. (2022). Taiwanese university students' smartphone use and the privacy paradox. *Comunicar: Media Education Research Journal*, (60), 61–70. https://doi.org/10.3916/C60-2019-06

Cocq, C., Gelfgren, S., Samuelsson, L., & Enbom, J. (2020). Online surveillance in a Swedish context: Between acceptance and resistance. *Nordicom Review*, *41*(2), 179–193. https://doi.org/10.2478/nor-2020-0022

Devitt, K., & Roker, D. (2009). The role of mobile phones in family communication. *Children and Society*, *23*(3), 189–202. https://doi.org/10.1111/j.1099-0860.2008.00166.x

Fotel, T., & Thomsen, T. U. (2003). The surveillance of children's mobility. *Surveillance & Society*, *1*(4), 535–554. https://doi.org/10.24908/ss.v1i4.3335

Furini, M., Mirri, S., Prandi, C., & Montangero, M. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, *25*, 1055–1061. https://doi.org/10.1007/s11036-020-01529-z

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. University of Chicago Press. https://doi.org/10.2307/3089153

Grant, I., & O'Donohoe, S. (2007). Why young consumers are not open to mobile marketing communication. *International Journal of Advertising*, *26*(2), 223–246. https://doi.org/10.1080/10803548.2007.11073008

Hasinoff, A. A., & Shepherd, T. (2014). Sexting in context: Privacy norms and expectations. *International Journal of Communication*, *8*, 2932–2955. https://ijoc.org/index.php/ijoc/article/view/2264

Herring, S. C. (2008). Questioning the generational divide: Technological exoticism and adult constructions of online youth identity. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 71–92). MIT Press. https://ella.sice.indiana.edu/~herring/macarthur.pdf

Ito, M., Horst, H., Bittanti, M., boyd, d., Herr-Stephenson, B., Lange, P. G., Pascoe, C. J., Robinson, L., Baumer, S., Cody, R., Mahendran, D., Martínez, K., Perkel, D., Sims, C., & Tripp, L. (2008). *Living and learning with new media: Summary of findings from the digital youth project*. The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning. https://library.oapen.org/bitstream/handle/20.500.12657/26078/1004007.pdf

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Lehtiniemi, T., & Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*, *4*(2), 1–11. https://doi.org/10.1177/2053951717721935

Livingstone, S. (2006). Children's privacy online: Experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, phones, and the internet: Domesticating information technology* (pp. 145–167). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195312805.003.0010

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393–411. https://doi.org/10.1177/1461444808089415

Lyon, D. (Ed). (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination*. Routledge. https://doi.org/10.4324/9780203994887

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200–216. https://doi.org/10.1080/01972243.2016.1153012

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Marwick, A., & Hargittai, E. (2018). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and integrity of social life*. Stanford University Press.

Oostveen, A., Vasalou, A., van den Besselaar, P. & Brown, I. (2014). Child location tracking in the US and the UK: Same technology, different social implications. *Surveillance & Society*, *12*(4), 581–593. https://doi.org/10.24908/ss.v12i4.4937

Prior, L. (2020). Content analysis. In P. Leavy (Ed.), *The Oxford handbook of qualitative research* (2nd ed.) (pp. 541–573). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190847388.013.25

Regan, P. M., & Steeves, V. (2010). Kids R us: Online social networking and the potential for empowerment. *Surveillance & Society*, *8*(2), 151–165. https://doi.org/10.24908/ss.v8i2.3483

Rost, F. (2021). Q-sort methodology: Bridging the divide between qualitative and quantitative. An introduction to an innovative method for psychotherapy research. *Counselling and Psychotherapy Research*, *21*(1), 98–106. https://doi.org/10.1002/capr.12367

Sipior, J. C., Ward, B. T., & Volonino, L. (2014). Privacy concerns associated with smartphone use. *Journal of Internet Commerce*, *13*(3–4), 177–193. https://doi.org/10.1080/15332861.2014.947902

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1902.

Statistics Finland. (2021). *Väestön tieto- ja viestintätekniikan käyttö* [*The information and communication technology use of the population*]. https://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_fi.pdf
Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information Communication and Ethics in Society*, *12*(4), 298–313. https://doi.org/10.1108/JICES-01-2014-0004
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. https://doi.org/10.17645/mac.v8i4.3407
Sukk, M., & Siibak, A. (2021). "My mom just wants to know where I am": Estonian pre-teens perspectives on intimate surveillance by parents. *Journal of Children and Media*, *16*(3), 424–440. https://doi.org/10.1080/17482798.2021.2014646
Trochim, W. M. K. (1985). Pattern matching, validity, and conceptualization in program evaluation. *Evaluation Review*, *9*(5), 575–604. https://doi.org/10.1177/0193841X8500900503
Vickery, J. R. (2015). 'I don't have anything to hide, but... ': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294. https://doi.org/10.1080/1369118X.2014.989251
Westin, A. F. (1967). *Privacy and freedom*. Ig Publishing.
Widmer, S., & Albrechtslund, A. (2021). The ambiguities of surveillance as care and control: Struggles in the domestication of location-tracking applications by Danish parents. *Nordicom Review*, *42*(S4), 73–93. https://doi.org/10.2478/nor-2021-0042
Williams, S., & Williams, L. (2005). Space invaders: The negotiation of teenage boundaries through the mobile phone. *The Sociological Review*, *53*(2), 314–331. https://doi.org/10.1111/j.1467-954X.2005.00516.x
Wisniewski, P. J., Vitak, J., & Hartikainen, H. (2022). Privacy in adolescence. In B. P. Knijnenburg, X. Page, P. Wisniewski, H. Richter Lipford, N. Proferes, & J. Romano (Eds.), *Modern socio-technical perspectives on privacy* (pp. 315–336). Springer. https://doi.org/10.1007/978-3-030-82786-1_14
Yan, Z. (2018). Child and adolescent use of mobile phones: An unparalleled complex developmental phenomenon. *Child Development*, *89*(1) *5*–16. https://doi.org/10.1111/cdev.12821

Endnotes

[1] The action or practice of sending sexually explicit photographs or messages via mobile phone.
[2] The list of stimulus items was originally created in the eQuality Project (see the acknowledgements). Items were listed based on a mainstream media search looking for any reports in newspapers, news magazines, and news sites that mentioned what a smartphone knows about its user.