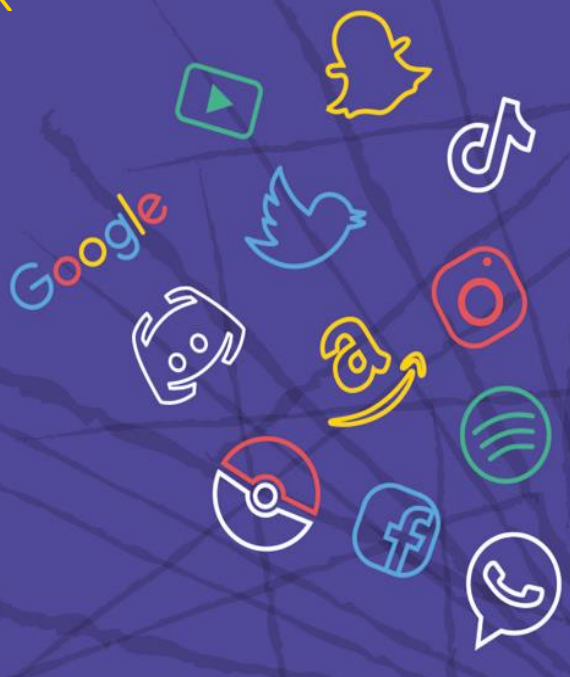
Children's data and privacy online

Growing up in a digital age

Mariya Stoilova, Sonia Livingstone and Rishita Nandagiri

Department of Media and Communications
London School of Economics and Political Science

#ChildPrivacyOnline www.myprivacy.uk



Contents

Preferred citation:
Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. Research findings. London: London School of Economics and Political Science.

Acknowledgements:
We are grateful to the Information Commissioner's Office (ICO) for funding this project and to our expert advisory group for their input and guidance.

For more about the project, see:
http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

Key points

- Children are encountering continual technological innovation which brings new and complex risks and opportunities
- In an age of datafication, privacy is being reconfigured, with data protection regulation increasingly important in protecting privacy
- Existing research demonstrates that children develop their privacy-related awareness and desire for privacy as they grow older, especially in relation to institutional and commercial contexts for privacy
- Children care about their privacy online, and they want to be able to decide what information is shared and with whom
- Children engage in a wide range of strategies to keep their devices, online profiles and personal information safe from unwanted interference
- Children tend to think of privacy online in terms of e-safety, struggling to grasp the relation between privacy and data – hence only e-safety risks seem truly real
- It matters that children first learn about interpersonal privacy - extending interpersonal assumptions to institutional and commercial contexts leads to misunderstandings
- Children focus on data they know they give, much more than data that is taken or inferred – and they think all of it is 'none of their business'
- Terminology misleads – they must give 'consent'; businesses want their personal data; what's deleted isn't gone; private means friends can't see but others can
- Children's media literacy – especially their critical knowledge of the data ecology - plays an important part in how they can understand, manage and safeguard their privacy
- Understanding grows with experience, but there's no 'magic' age of capacity
- Parents are confused and concerned, and like teachers, they want higher-level solutions; they can't deal with online data and privacy alone
- This report ends with key recommendations based on the research. We have developed an online toolkit for children at www.myprivacy.uk

Growing up in the digital age

Children are encountering continual technological innovation which brings new risks and opportunities, and which is becoming ever more complex

In the digital age, technologies are increasingly important as a means through which children can exercise their rights and meet basic needs – they provide much needed access to education, socialising, participation, wellbeing and entertainment. But as technologies become more sophisticated, networked and commercially viable, children's privacy is threatened by new forms of data collection and surveillance enacted by businesses, parents and the state (including schools, health and welfare systems and law enforcement).

The complexity of the current digital ecology makes it particularly hard, for children and adults alike to anticipate the long-term consequences of growing up in the digital age. This makes today's children the 'canary in the coalmine' of our datafied society.

Children are often pioneers of the new, ready to learn and experiment ahead of parents and other adults

Children are often pioneers in exploring and experimenting with new digital technologies and services. Curious and inventive, they seize new opportunities, thinking on their feet about possible consequences and shortcomings. Increasingly independent users of digital technologies and starting at a much younger age, children experience newly emerging risks often before adults know about their existence or are able to put mitigating strategies in place. In the contemporary digital environment, children's actions are particularly consequential as technologies transform their lives into data which can be recorded, tracked, aggregated, analysed and monetised – and which is durable, searchable and virtually undeletable.

In an age of datafication, privacy is being reconfigured

Privacy is often conceived as individual control over information that is knowingly given or shared with others (Westin, 1967). As technologies mediating communication and information of all kinds become more sophisticated, globally networked and commercially valuable, privacy is becoming less about 'the personal'. Situated in a complex evolving data ecology which includes multiple types of data whose processing goes beyond questions of individual control (van der Hof, 2016) or even awareness, privacy is also becoming less about 'the private'.

Privacy is relational: it is sustained (and contested or threatened) through interactions among people and/or organisations – increasingly, across networked digital contexts. Privacy depends on how people understand those contexts – the values and norms that are established for them (in terms of visibility, surveillance, consent or redress) and boundaries they attribute to them. Privacy is, therefore, 'neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information' (NIssenbaum, 2010:3). In the absence of a meaningful relationship with the businesses or institutions that process their personal data, and insofar as they lack a critical understanding of the

wider contexts within which those businesses or institutions operate, it is likely that children will struggle to understand how their privacy is being reconfigured in the digital age. Pressing questions include how much we can teach children about their privacy (for instance, as part of media literacy education), and how much change is required from the businesses and institutions which process their data, if children's right to privacy is to be protected.

Managing privacy via data protection regulation

Children's specific needs and rights have been too little recognised or provided for by the digital environment and the regulatory, state and commercial organisations that underpin it (Livingstone et al, 2015). There are growing calls for intervention, including for privacy-by-design (along with safety- and ethics-by-design) to be embedded in the digital environment (Kidron et al, 2018).

- **Achieving a holistic approach to children's 'best interests' depends on managing the balance between protection and participation online:** children's issues are mainly considered in the context of child protection (cyberbullying, abuse and sexual exploitation), while other child rights (e.g., to privacy and freedom of expression) are often overlooked. It is important to consider privacy in its own right as well as a mediator of other rights in seeking a balance between child protection and participation online.

- **Challenges of age verification impede efforts to respect children's 'evolving capacity':** the challenges of age verification, including establishing who is a child and how old they are makes for an ecology that can easily slip into universal (often, adult) treatment of all its users. Provision and regulation too often fails to respect children's 'evolving capacity,' lumping children into over-broad categories (under-13s, under-18s) that do not support their development – hence public controversy over the so-called 'digital age of consent.'

- **Institutional and commercial data protection regimes may enable or infringe privacy when systems work as intended, also infringing it when breaches occur:** it is easy to identify data protection breaches as infringements of privacy, but important privacy questions may also arise from the effective functioning of institutional and commercial data protection regimes. Digitally 'heavy' systems with limited opt-out options, no granular control to facilitate different levels of consent or unclear long-term outcomes can easily infringe children's privacy rights.

- **Regulation of children's data and privacy online must draw on multidisciplinary research and expertise** about (i) children's experiences, (ii) childhood and child development, (iii) effectiveness of law and regulation and (iv) technological innovation, design and markets: while the commercial use of children's data is at the forefront of current privacy debates, the empirical evidence lags behind, and there are many gaps, particularly in relation to institutional and commercial privacy. A cross-sectional approach that considers all areas is necessary to ensure comprehensive and efficient regulation that addresses the challenges faced by all stakeholders.

Since children are little consulted about data and privacy online, we ask:

- How do children understand, value and negotiate their privacy online?
- What capabilities or vulnerabilities shape children's navigation of the digital environment?
- What evidence gaps regarding children's data and privacy online impede the development of policy and practice?
- What are the implications of children's understanding and practices for the realisation of their rights by relevant stakeholders?

The digital data ecology

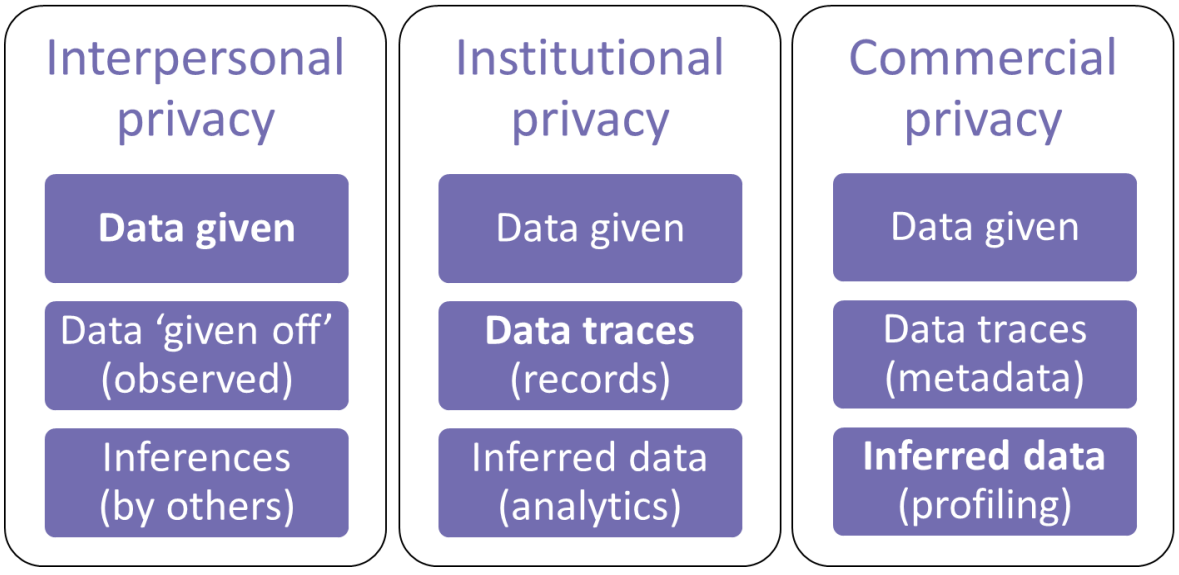
Privacy is both a means and an end, valued in itself and vital for autonomy, identity, security, participation and wellbeing. To capture the complexity of children's privacy and data online, we theorised the digital data ecology by recognising three contexts for privacy:

- **Interpersonal** – how a 'data self' is created, accessed and multiplied via social connections
- **Institutional** – how public agencies such as government, educational and health institutions gather and handle data about a person
- **Commercial** – how personal data is harvested and used for business and marketing purposes

Distinguishing between interpersonal, institutional and commercial contexts helps resolve the so-called privacy paradox – namely, that young people say they care about their privacy yet in practice they share personal information on public platforms. To conceptualise what children know and expect of digital data, we adapted a typology of data types from privacy lawyer Simone van her Hof (2016):

- **Data given** – the data contributed by individuals (about themselves or about others), usually knowingly, although not necessarily intentionally, during their participation online
- **Data traces** – the data left, mostly unknowingly, by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata
- **Inferred data** – the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources

The different privacy contexts prioritise different types of data and so also afford different kinds of infringement, since only 'data given' is actively contributed by individuals.



Our approach

The child-centred approach prioritised children's voices and experiences to inform evidence-based policy development. The project involved:

- A systematic evidence mapping of existing knowledge on children's data and privacy online, identify research gaps and outline areas of potential policy and practice development.
- Focus group research with 150 children of secondary school age, their parents and educators, from selected schools in England, Scotland and Wales.
- Child juries for evaluating online privacy resources and reviewing recommendations for policy and practice.
- Creating an online toolkit to support and promote children's digital privacy skills and awareness.

Systematic evidence mapping

Using systematic evidence mapping, we reviewed the existing knowledge on children's data and privacy online, identified research gaps and outlined areas of potential policy and practice development.

- **Search**: We consulted experts, and searched 19 databases selected to cover the social sciences, legal studies, computer science studies, government publications, legal documents and grey literature (policy reports, conference papers, advocacy tools and case studies).
- **Selection**: The inclusion criteria captured studies from any country published in English language since 2007. The database searches were conducted using three groups of search terms: (i) child terms, (ii) digital technology terms and (iii) privacy terms. Search testing was conducted to ensure validity, optimal coverage and efficiency.
- **Screening**: The search produced 9,119 source. After removal of duplicates, and a careful screening of the abstracts based on an assessment of quality, appropriateness and relevance, 105 articles were identified for coding and analysis.

The existing research demonstrates that children develop their privacy-related awareness and desire for privacy as they grow older. Their literacy and ability to manage different privacy boundaries also becomes more complex with age, and they gain a wider range of technical skills and knowledge enabling them to navigate better privacy parameters on digital platforms. Based on the evidence review we mapped the development of children's understanding of privacy by age (see the following table).

The evidence mapping identified substantial gaps in existing knowledge in relation to all dimensions of privacy online, but particularly with reference to institutional and commercial uses of data. More research is needed to improve our understating of how children's developmental needs affect their privacy awareness, exposure to risks and related media literacy. In spite of the existing gaps, the child development evidence related to privacy undoubtedly points to the need for a tailored approach which acknowledges developments and individual differences among children.

Most research concerns interpersonal dimensions of privacy and data given. Much less is known about data given off and data traces, while institutional and commercial privacy are rarely at the forefront of discussions, and inferred data is hardly ever considered.

More about the evidence review is available at Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) *Children's Data and Privacy Online: Growing Up in a Digital Age. An Evidence Review*. London: London School of Economics and Political Science.

Children's understanding of privacy by age

	Interpersonal privacy	Institutional and commercial privacy
5- to 7-year-olds	• A developing sense of ownership, fairness and independence • Learning about rules but may not follow them, and don't get consequences • Use digital devices confidently, for a narrow range of activities • Getting the idea of secrets, know how to hide, but tend to regard tracking/monitoring by a trusted adult as helpful	• Limited evidence exists on understanding of the digital world • Low risk awareness (focus on device damage or personal upset) • Few strategies (can close the app, call on a parent for help) • Broadly trusting
8- to 11-year-olds	• Starting to understand risks of sharing but generally trusting • Privacy management means rules not internalised self-regulation of behaviour • Still see monitoring by a parent or other trusted adult positively, to ensure their safety • Privacy risks linked to 'stranger danger' and interpersonal harms • Struggle to identify risks or distinguish what applies offline/online •	• Still little research available • Gaps in ability to decide about trustworthiness or identify adverts • Gaps in understanding privacy Terms and Conditions • Interactive learning shown to improve awareness and transfer to practice
12- to 17-year-olds	• Online as 'personal space' for expression, socialising, learning • Concerned about parental monitoring yet broad trust in parental and school restrictions • Aware of/attend to privacy risks, but mainly seen as interpersonal • Weigh up risks and opportunities, but decisions influenced by desire for immediate benefits	• Privacy tactics focus on online identity management not data flows (seeing data as static and fragmented) • Aware of 'data traces' (e.g., ads) and device tracking (e.g., location) but less personally concerned or aware of future consequences • Willing to reflect and learn but do so retrospectively • Media literacy education is most effective if adolescents can use their knowledge to make meaningful decisions in practice

Child-centred methods

We developed a qualitative research methodology which allows children's voices and experiences to be expressed in a way that is meaningful to them.

This included real-life scenarios and exemplar digital experiences to facilitate the discussions and to ensure that children focused on the opportunities, risks and practical dilemmas posed by the online environment.

We also aimed to enable children to act as agents in shaping their digital rights, civic participation and need for support.

The primary research involved:

- A series of workshop methods developed, piloted, revised and conducted in schools in London, Essex, the Midlands, Wales and Scotland.
- 28 mixed-gender focus groups, lasting 173 minutes on average, with 135 children aged 11-12 (Year 7), 13-14 (Year 9) and 15-16 (Year 11).
- Two focus groups and seven interviews with teachers, one focus group with parents and 15 child–parent paired interviews.
- Three child jury panels with a mix of 18 children in Years 8 and 10.

Methods to encourage children to talk about their data and privacy online

The focus groups started with unprompted perceptions of privacy and children's practices. We asked about apps and websites used during the last week, the process of selecting these apps (checking age restrictions, reading Terms and Conditions, getting advice about new apps from others), using privacy settings and negotiating independent use with parents.

It was quickly clear that children engage primarily with apps and services for the general public more than with child-specific apps.

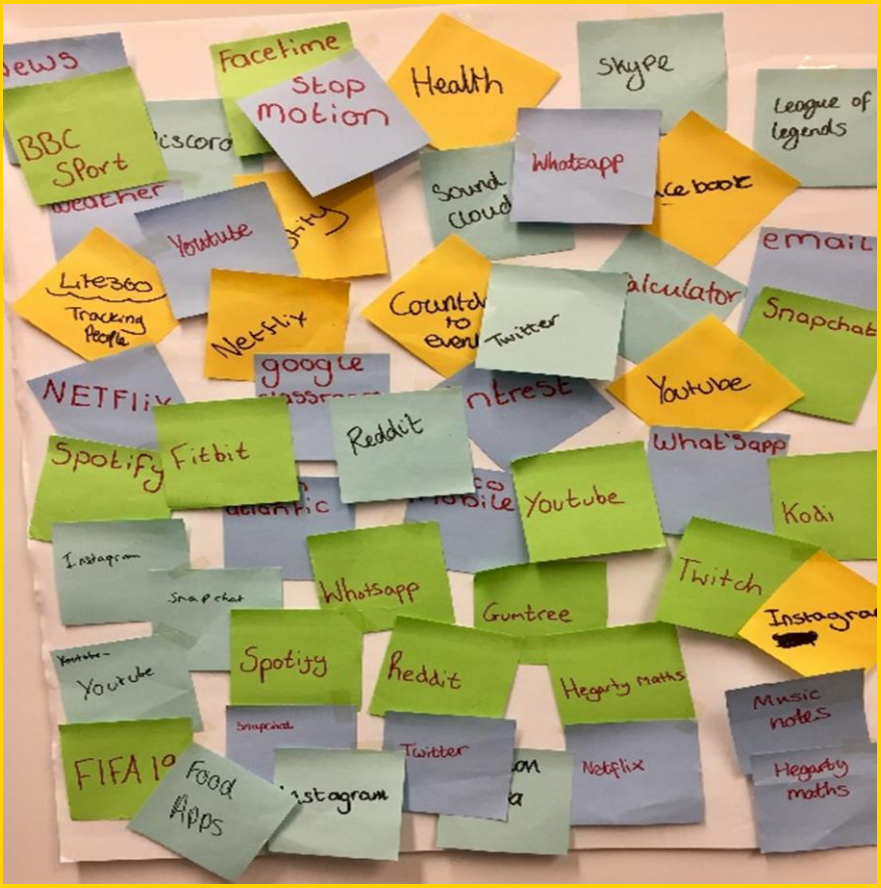
Secondary school seems to mark a 'rite of passage' when children get their first smartphone or a better one, which allows them to do more with it and to be more independent. They start to engage in a wider range of activities online and want to explore what the internet has to offer, often by trial and error. Children often describe the beginning of secondary school as the period when 'everyone downloads everything' and having access to apps, especially before your peers, brings a certain social status.

> *When you're in Year 7, you've got loads of apps and as you grow older, it gets smaller and smaller. (boy, Year 11, Essex)*

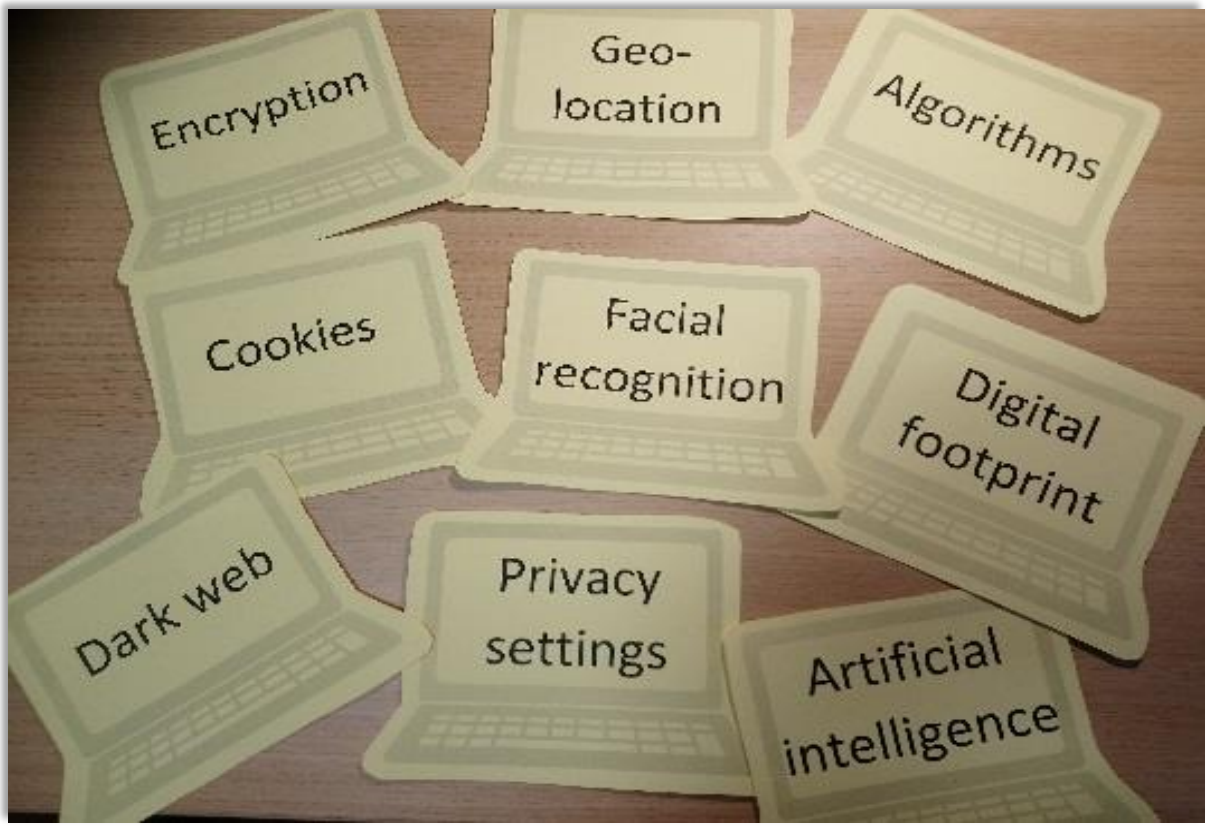
> *I was like oh my God, I'm so cool. I've got Instagram and I'm not even 13 yet. And then literally everyone's got it, no one actually cares. (boy, Year 9, Essex)*

Thus from Year 7, children were highly experimental, using a wide range of apps covering all areas of their everyday life and activities (leisure, commercial, learning, etc.). These are mostly apps and services for the general public and not child-based (e.g., they use YouTube rather than YouTube Kids). The youngest group engages with the largest number of platforms. App use is very dynamic, playful and based on trial and error. Children get 'drawn in' (by curiosity, need to socialise with friends and trends) but also might quickly lose interest and move on to something else.

What apps do you use (focus group activity)



We also explored children's familiarity with relevant terminology (e.g., cookies, privacy settings, algorithms, facial recognition), then discussing more complex questions such as types of data they share and with whom.

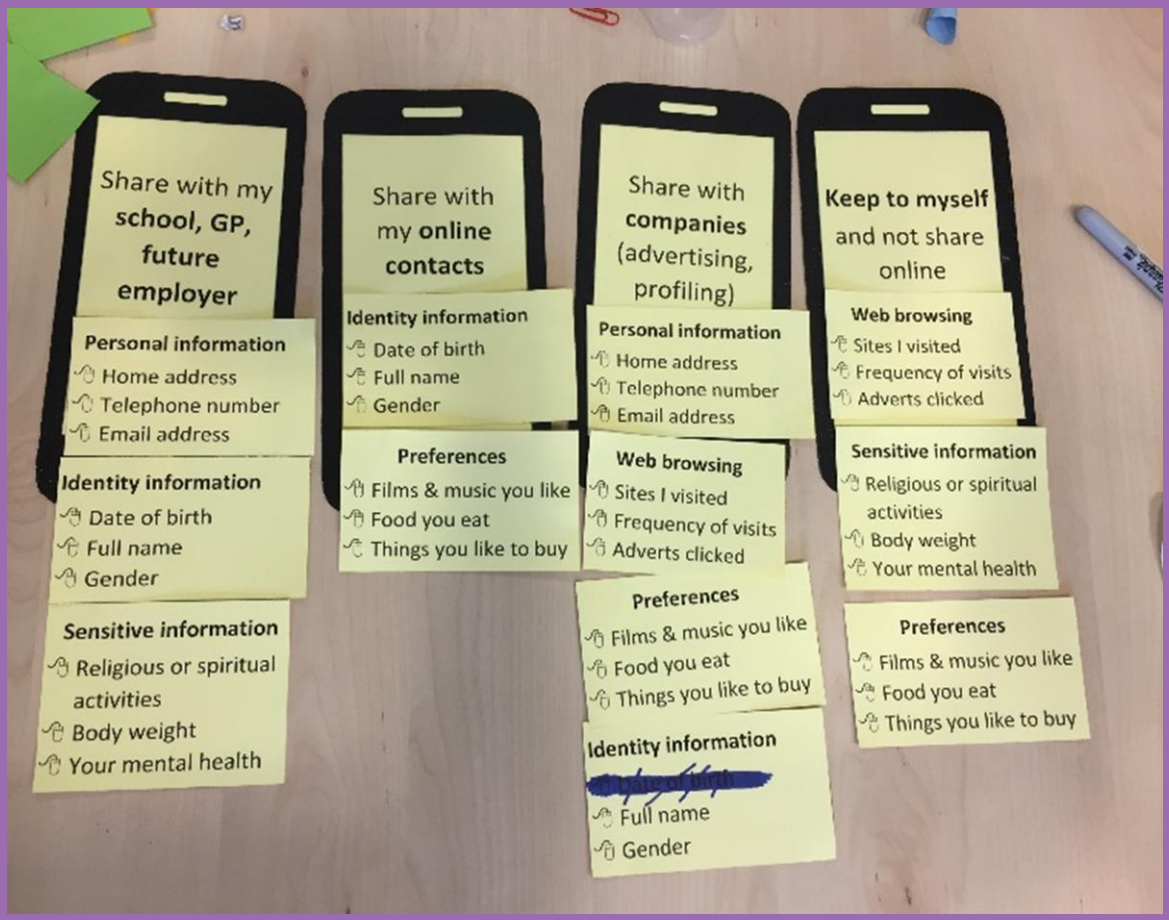


We designed an activity where children were given four options for sharing their data – share with online contacts (interpersonal privacy); share with my school, GP, future employer (institutional privacy); share with companies (commercial privacy); and keep to myself (a desire not to share something).

After discussion with the UnBias project, we identified 13 types of data that might be shared digitally and reduced these to the nine most relevant categories: personal information, biometric data, preferences, internet searches, location, social networks, school records, health, and confidential information. We asked children who they share this data with, referring both to active and passive sharing, and allowing them to choose as many sharing options as they thought relevant. This allowed the gradual building of the landscape of children's online privacy behaviour, enabling discussion of less thought-of areas such as data harvesting and profiling.

For more on the methodology and the challenges, see Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) *Talking to Children about Data and Privacy Online: Research Methodology*. London: London School of Economics and Political Science.

Talking to children about the data they share



We created a visual and interactive activity enabling children to engage with the different dimensions of privacy and think about the data they share. Children were given four sharing options – share with online contacts (interpersonal privacy); share with my school, GP, or future employer (institutional privacy); share with companies (commercial privacy); and keep to myself (a desire not to share something).

They were asked to reflect on their practices of sharing different types of data (personal information, internet searches, preferences, location, social network data, biometric and health data, confidential data).

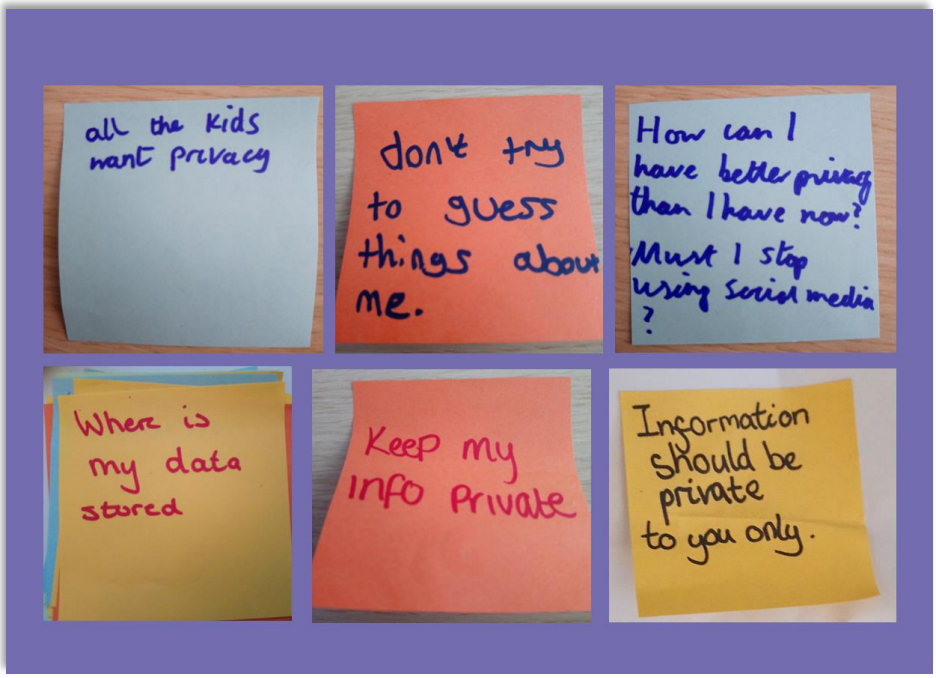
Findings: children's privacy values and practices

✓ Children care about their privacy online

Children care about their privacy online. They are clear too that not all personal information should be online. Even if a child has a public social media profile, they still think about privacy and might protect it by making careful decisions about what they post.

Children often understand 'privacy' as being able to keep their online activities to themselves without others finding out. In cases when they want to share, they want to be able to decide what information is shared and with whom. As a generation that has grown up with digital technologies and in the spotlight of social media, children acknowledge that their interests and practices change over time, many admitting feeling uncomfortable having their 'pervious selves' recorded and retrievable online.

> *I do care… Pretty much all kids will say they want their privacy. (boy, Year 9, Midlands)*
>
> *You don't really need to share every detail of your life online. (girl, Year 7, Midlands)*
>
> *Your information is specifically yours. Like your full name, mental health, that's to do with you. So you should be able to choose who knows and who doesn't. (boy, Year 9, Scotland)*



Children insist that growing up online is a learning process and they want to have the freedom to experiment and learn by trial and error without being judged too harshly for the mistakes they might make along the way. Making mistakes while learning how to behave online is part of growing up – a necessary stage that everyone needs to go through. Therefore, children want the content they create online to have an 'expiration date', and some even expect online platforms will cease to exist in the future and their digital footprint will perish with them. Children also acknowledge that becoming independent might require gaining rights gradually, while remaining under parental control for some aspects (such as payment-related features).

> *You have to slowly figure out the basic guidelines, what you should do, what you shouldn't do because you don't want people to judge you for it. […] It's quite hard and you have to figure out… (girl, Year 9, Wales)*

> *So you have to get used to people commenting, you have to get used to what you post and who will see it … you have to almost, yes, learn how to use it. (boy, Year 9, Wales)*

Children often disagree about the suitable minimum age for apps and many do not know or check the age verifications before they start using an app. Age-appropriate labelling is mostly seen as rough guidance, with many children stating that what matters more is how you use the app – for example, whether your account is private or not. Adult rating (18+) sends a stronger message that the content is likely to be unsuitable for children. Opinions also differ regarding what age is appropriate to start making independent decisions about app use, but there is overall agreement that it is acceptable for younger children (in primary school) to be supervised by adults. Still, when children disagree with age-appropriateness, they admit trying to find a way to bypass it (e.g., by entering a different age).

> *I feel like things are aged wrong. (girl, Year 7, Scotland)*

> *I used to ask my parents if I was allowed to use the service. Now I just click 'yes'. (boy, Year 7, London)*

> *I don't really need to worry about ages because they [my parents] don't really care what I'm downloading. (girl, Year 7, Scotland)*

✓ Privacy-protecting tactics are common

Children engage in a wide range of strategies to keep their devices, online profiles and personal information safe from unwanted interference. Some of the strategies are based on withholding information and deciding not to share content considered to be inappropriate. Other strategies are more proactive, such as selecting among the multiple communication channels and accounts based on the privacy they offer, changing settings as a way of managing audiences and boundaries or content modification (providing fake information, changing textual descriptions, removing tags, altering images, deleting or blocking people).

> *I check on Snapchat, if I'm on ghost mode or not… And on maps, I sometimes check that people can't see if I'm at home. (girl, Year 11, Essex)*

I don't like sharing a lot of things like online, unless I actually have to for some reason, then I'll do that. (girl, Year 7, Scotland)

My contacts are only people who I have met. (girl, Year 7, Essex)

Well, I have two accounts. One's my personal account, where it's on private. I have another account where it's, like, open. But I don't reveal anything about myself. I just … do drawings and post them. (girl, Year 7, Essex)

If I'm trying out a site but I think it's dodgy, then I put a random name in. (boy, Year 11, Essex)

✓ Children tend to think of privacy online in terms of e-safety

The e-safety framing of privacy is so familiar that it obscures other privacy considerations. Indeed, at first children thought we were asking about e-safety although they have heard of Cambridge Analytica and data breaches, so they know there's more to it. Indeed, we had to explain carefully that we were asking about other issues beyond e-safety.

Cambridge Analytica

Mark Zuckerberg was giving out information to this university to study. But the point of the privacy act, he wasn't allowed to give that information to them. […] When the people that use Facebook signed up agreed to, he broke that trust, pretty much, when he gave that information to the university. (boy, Year 11, Wales)

On Facebook, I think that was the thing where they leaked the information from some of the things. So even if it is a big company, you can't always trust them. (girl, Year 7, London)

Facebook sold the information of their users to a different company who made things to put people off of voting for someone… [That's not okay] because it's probably helped people win things which they shouldn't have won. (boy, Year 7, Essex)

Mark Zuckerberg, he's always watching. (boy, Year 11, Essex)

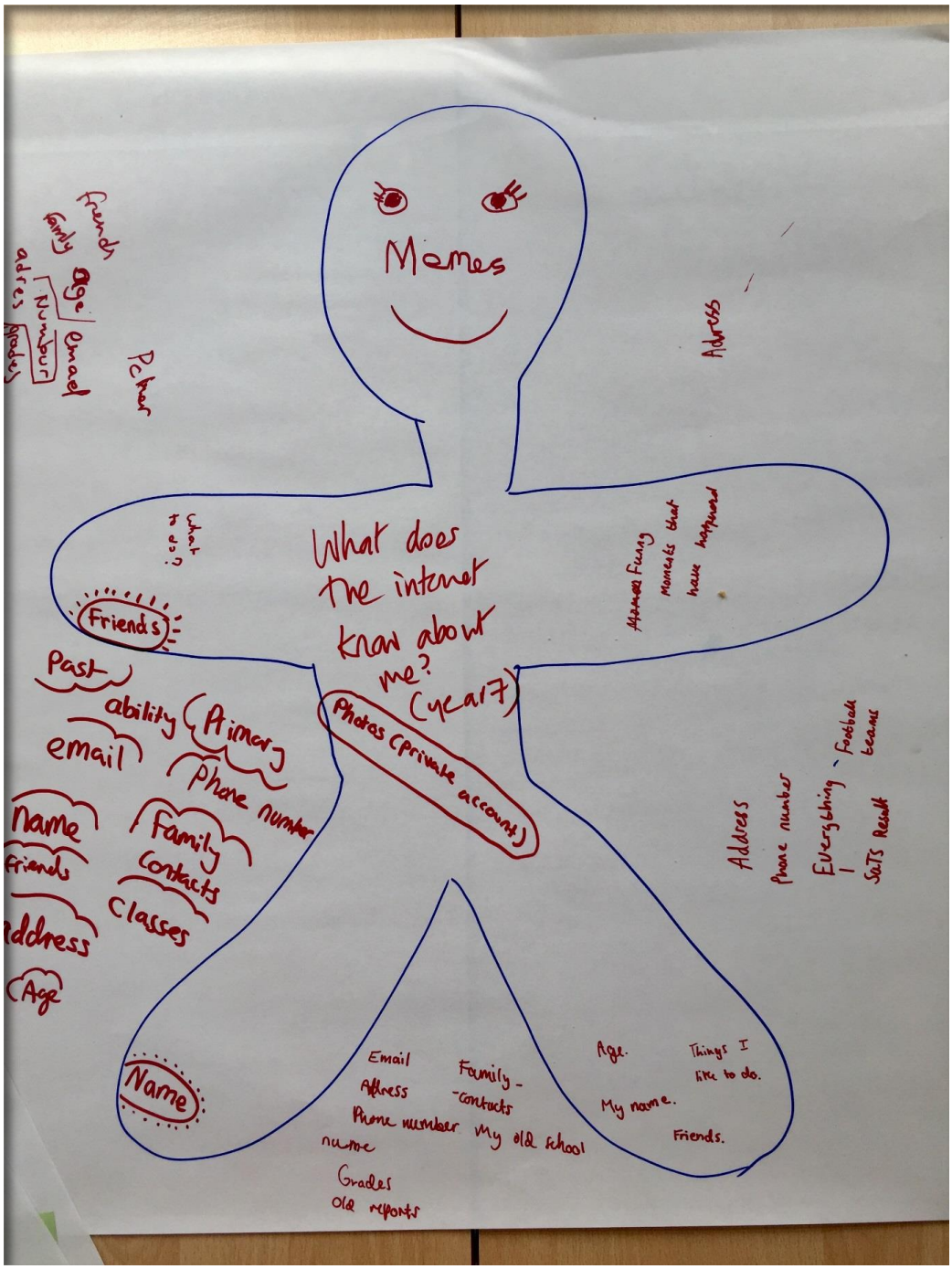
Even so, when talking about privacy online, children spontaneously refer to online safety and raise issues related to being tracked by strangers when sharing personal information that is too detailed, receiving unwanted messages if their accounts are not private, being exposed to phishing, hacking or spam mail, or being bullied if they share embarrassing material. Children have usually discussed these risks at school, and feel that they are well equipped to mitigate them, particularly as they relate to moderating their own behaviour.

People could find out where you go. So, they could try and find you and wait for you there. (boy, Year 7, Essex)

The only thing that worries me is weird folk, like stalkers. (girl, Year 11, Scotland)

Somebody could be, like, pretending to be somebody you know, but aren't actually them. (girl, Year 7, Wales)

Beyond e-safety situations, children often fail to see their online activities as generating data and sharing it beyond their intended circle of social contacts. They often try to guess and work out what these other privacy-related situations might be.



Findings: children's privacy understanding

✓ Children are struggling to grasp the relation between privacy and data

Children sense – or are working out – that everything they do online may be tracked and recorded for whatever purpose. They are mostly able to work out that their online activities are being tracked and recorded. They know that their parents can monitor their location and what they are downloading; they understand that their school is filtering the content they can access on the computers and monitoring their school meals via fingerprint payment systems; and they also notice that advertisements start appearing across platforms as soon as they show some commercial interest in something. However, they struggle to put the puzzle pieces together and to understand how the different pieces might fit together to create a growing digital footprint.

> *There are often ways to access everything, it's there. (boy, Year 11, Scotland)*
>
> *If they can find out stuff about you, then they can find out stuff about your family. (girl, Year 7, Midlands)*
>
> *The fact that you say it's private, doesn't mean it's private. (boy, Year 11, Scotland)*
>
> *So even if it is a big company, you can't always trust them. (girl, Year 7, London)*

✓ It matters that children first learn about interpersonal privacy - extending interpersonal assumptions to institutional and commercial contexts leads to misunderstandings

Children assimilate talk of data to familiar e-safety messages, not grasping the institutional and commercial motives behind today's complex data ecology.

Children understand and consider privacy most often within the realm of interpersonal relations and the active sharing of data (data given). Privacy revolves around managing relationships and information, often trying to navigate monitoring from adults such as family members or teachers. This creates important gaps in children's ability to foresee and traverse institutional and commercial aspects of privacy. It also means that children mainly extend their expectations and actions from the interpersonal dimension into the other two, sometimes creating misconceptions and misplaced anticipations.

> *I don't see what they'd get out of it [selling my data], to be honest. (girl, Year 11, Midlands)*

I'm only one person out of all the hundreds and millions of people who use the website, it's not going affect my life drastically. (boy, Year 7, Midlands)

The only thing that I really care about keeping private is my conversations with other people. That's the only thing. Otherwise I've posted it. I've agreed to Terms and Conditions, it's my fault if they take my data. (girl, Year 9, London)

Children have a much more nuanced understanding of trust within personal relationships, possibly influenced by their greater ability to comprehend and control these relationships. Hence, it is not surprising that they carefully manage the data they willingly give and their immediate audiences, but are much more passive when it comes to managing data traces and profiling. They are also quite trusting of institutions, like their school, to protect their data and to act in their interests.

They're my school, they're going to keep my data safe. (boy, Year 7, Midlands)

In school, blocking those things means that there's less threat to school computers, like, from viruses etc. And it means that emails don't, like, get cluttered up. (boy, Year 9, Wales)

Being monitored may not be understood as a privacy issue: perhaps because children are used to being monitored by adults (parents, teachers), they assume being monitored by companies is similar.

Children talk of 'the people' at Instagram, or a friend's father in the tech industry, assuming that the company will act in the same way as someone they know. Further, children often personify their relationship with the tech industry, pointing out that they trust the companies they know. They assume that large companies would act professionally, have transparent intentions and protect the interests of their customers, also as a way of protecting their own reputation and business interests.

Probably some geek at Amazon [knows what I post online]. (girl, Year 9, Scotland)

If they mess up, it's going to affect their reputation massively. (boy, Year 11, Midlands)

The main ones [companies] I would trust. (boy, Year 11, Wales)

Apple couldn't reveal the DNA of some serial killer because it went against their Terms and Conditions. (boy, Year 11, Essex)

✓ Children focus on data they know they give, much more than data that is taken or inferred

While children understand how their data is recorded on some platforms, cross-device identification, metadata and profiling are hard to grasp. How their data moves online, who uses it and to what ends, and why their data is valuable are some of the most reoccurring questions that children have. They are often unaware that the same company might be behind different platforms they use (e.g., WhatsApp, Instagram and Facebook). Children also try to make sense of how the internet ecology works and create their theories, myths and workarounds. They are also often puzzled by the amount of information they are asked to provide when they register to use product and services, particularly if it seems unrelated to the purpose.

I've never actually known… When I do that Wi-Fi at restaurants and stuff, why it asks for where you live. (girl, Year 11, Essex)

Well we don't actually know where the information is going … they'll say at the bottom that it's all private and stuff, but then it goes somewhere. (boy, Year 11, Midlands)

I'm not sure if they keep it. I want to know if they are deleting my information. (girl, Year 9, London)

Well, it is scary that they know so much about you. But they don't really look into it that much. (boy, Year 11, Essex)

✓ Terminology misleads – children *must* give 'consent'; businesses want their *personal* data; what's *deleted* isn't gone; private means friends can't see but others *can*

Children often take the online environment at face value and can be misled when things are not what they appear to be. When they are asked to provide personal information, for example, when signing up for a service, they are not always able to tell which information is mandatory and which is optional. They can become confused why they are asked for their consent if there is no option to use the service without giving it – even though some are aware of the GDPR, most just automatically press 'agree'.

Children also find it puzzling as to why apps request some of their personal data that seems irrelevant to the activities they are doing – the business model behind using their personal data can is not obvious to them. Children also struggle with the notion of what it means to delete online data. They are aware that things can be saved and distributed further, even if the original content has already been removed (screenshotting social media messages is an example they often refer to), and they also know that they can 'revive' deleted social media profiles. This makes it confusing for them as to what deleting actually means when the information doesn't really go.

As 'private' is mostly understood in interpersonal terms, the fact that information from non-public profiles is in fact shared with the platform itself can also be difficult to understand, particularly as few children know about encryption functionality. Still, they have a general understanding that their activities leave traces online, seen as an unavoidable aspect of online participation, and mostly a background aspect of their online activities that they do not think about. They know they are asked for consent but do not see this as having a real choice, a point also raised by parents and teachers.

You can't get any further without giving your information. Like you don't really get a choice. (boy, Year 9, Scotland)

Lots of websites that you go on, they will ask for your WhatsApp, they ask for your number, your name, your surname, stuff like that. (girl, Year 7, London)

You just scroll straight to the bottom of it and then click 'agree' as if you've read it. (girl, Year 9, Wales)

Generally young people are probably aware that data's collected, but they probably think, well, maybe that's just the nature of the internet. (parent, London)

✓ 'It's none of their business'

Children are highly moral – they talk of what's fair and what's right – and they protest at business practices that use their personal data in unaccountable ways.

Children are generally protective of their information and often reply that they would like to keep to themselves various types of personal data, such as where they go, who they meet and what they search online. Data about what they like and enjoy is usually happily shared with online friends, which confirms the important role of the internet for socialising. They are also not fully aware of the amount of information the internet gathers about them. In the course of the discussion, however, they quickly realise that they are 'volunteering' huge amounts of data and are surprised by how much the internet knows about them. This makes some of them worried, while others respond saying that their data is theirs, and rejecting the data business model. Still, many do not see why datafication matters or are reassured by the information about them being full of mistakes or out of date.

No, it shouldn't be any of their business. (boy, Year 9, Midlands)

I just don't want anyone else to have access to what I'm doing with my computer. It seems weird and wrong. (boy, Year 9, London)

People don't need to know what you look at and companies shouldn't really be poking through your contacts. Because there might be some sensitive information in there which they shouldn't get hold of. (girl, Year 7, Essex)

I think some of the stuff they ask you is irrelevant. (girl, Year 11, Essex)

✓ Because children are offended that 'others' collect their 'private' data, they assume that 'others' would recognise that they should not keep or share their data.

As a result, children can be quite trusting of their online environment, especially of the institutions and adults around them, but also of the apps that they use and the companies behind them. While they are aware of commercial models (mostly in relation to exposure to advertising), they are susceptible to marketing messages stating that companies value and protect customers' privacy and collect data to improve the user experience. Children anticipate good intentions and generally trust companies and institutions with their data. When invited to think about why companies collect their data, they tend to focus on how it might benefit them.

Those are usually dodgy companies [who share your data with others], so you can sort of catch them out … their websites usually have a lot of pop-up ads and they just don't look very professional. (girl, Year 11, Midlands)

When you have to put your phone number in … when they send you a code. (girl, Year 11, Essex)

They might use your location to see where in the world people are using it, so that's where your location would be used. (boy, Year 11, Midlands)

[Facial recognition is] easier and people don't see you doing your password out in public. (girl, Year 7, London)

✓ Children have learned that they are unimportant, with random adults showing little interest in them, and so they assume their data is equally unimportant.

Even when children grasp the idea that companies might monitor users for commercial gains, they might fail to recognise why their own data could be useful. Children often see their online activities as trivial and mundane, and argue that they have nothing to hide, so they fail to identify privacy threats.

They take cookies and they track what you're watching, what you do on the internet. To me, I don't really do any sensitive stuff on the internet… Why would somebody want to track me down? That's why I don't really care about cookies and stuff. (boy, Year 7, London)

I don't see why they'd want to [see where I've been]. (girl, Year 7, Midlands)

I don't mind, because I don't have anything to hide. (girl, Year 7, Essex)

I just don't think that what the ordinary everyday person does on the internet is really that interesting to companies and even if they take data, I don't think that anything bad will happen to me. (girl, Year 9, London)

Children expect the tactics, workarounds and deceptions that protect their privacy from friends or parents to also work with companies.

Children often underestimate the extent to which information about them can be aggregated, so they are confident that their data profile is wrong, for example, if they have put a fake name and the wrong age, if they search 'incognito' or switch devices. They are both entertained and irritated when the internet is wrong about them (e.g., when it suggests things they are not interested in) and often hold on to a feeling of an authentic self that is non-digital. At the same time, they do not understand how some activities presented in a fun game form can harvest data about them – many share that they like online quizzes but do not think that they provide personal information when answering the questions.

When you put 'other', it makes it hard for them to realise who you actually are. If you put 'male', you're halving the probability they can find it's you. (boy, Year 11, Essex)

If you didn't use your name, they wouldn't know it was you. If you did use your name, then you're sharing a lot more information. (girl, Year 11, Essex)

I don't put my real age, I don't put any age around my age. (girl, Year 7, London)

Some websites think you are a robot. (boy, Year 7, Wales)

✓ Children are puzzled that anyone would keep irrelevant old data

Children witness the online environment changing, platforms being discontinued and peers moving from one app or device to another in quick succession. This creates an impression that data is temporary, fractured and quickly becomes irrelevant. Instead of considering how their digital footprint grows over time, they are reassured by the assumption that their data will expire or become irrelevant.

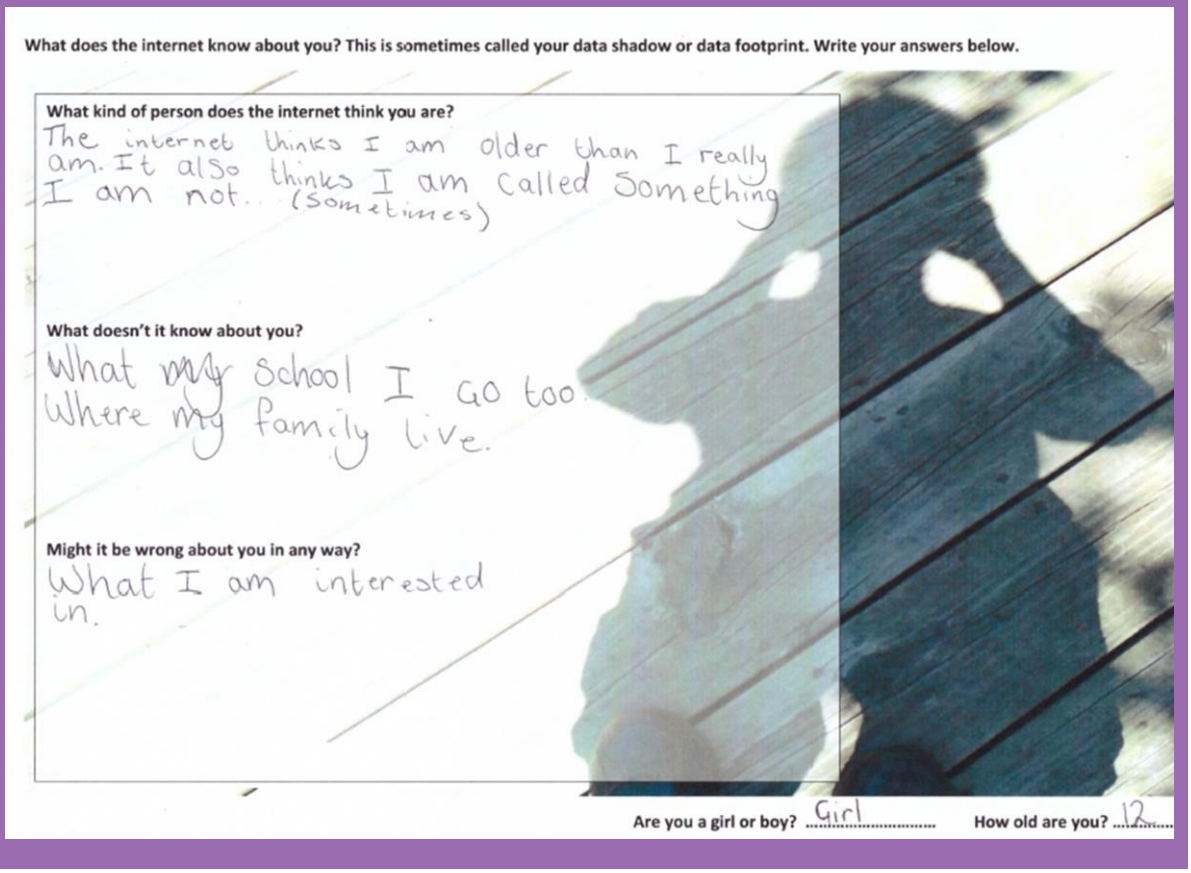
> *There's probably going to be new social apps and stuff, and then people will stop using the old ones. (girl, Year 7, London)*

> *Well, certain things can get, like, dated over time. (boy, Year 9, London)*

> *If it stayed on there for longer than two years, I think it should just come off because there's no point. (girl, Year 11, Essex)*

What does the internet know about you?

Focus group worksheet for children



✓ Key findings for media literacy

Children's media literacy plays an important part in how they can understand, manage and safeguard their privacy. It involves not only the technical skills necessary, but also a broader understanding of how media and information are created, analysed, distributed, applied, used and monetised.

We sought to capture this complexity in the primary research and asked children about their: understanding of key privacy-related terms (e.g., cookies, facial recognition, geo-location, encryption, digital footprint, etc.); knowledge and use of privacy protective strategies; subjective understanding of privacy; online and data-sharing practices and understanding of the ecology (e.g., how data is collected and why, where it goes and how long it is kept); and help-seeking behaviour.

We found that children (not unlike some teachers and parents) have a limited understanding of privacy issues related to datafication, commercialisation and child rights. While they learn from a wide range of sources (parents and older siblings, peers, educators, the news or by searching for information or videos online), their knowledge remains partial, especially in relation to data analytics and profiling, and the overall flow of data and its commercialisation. Children's knowledge is not neatly age-graded, and even some of the older children we spoke with struggled with fairly simple and frequently encountered terms, such as 'cookies'.

> *[Cookies] I've just seen it, I don't really know what it is. (boy, Year 11, Essex)*

> *[Cookies] If it's something you're going to use and then you have to accept it, I think… I don't know what they mean though. (girl, Year 7, Scotland)*

We found that children who are concerned about their privacy and are able to identify the potential risks are more careful with their sharing practices. However, children's privacy awareness varies significantly, and some do not see why they need to have privacy protective strategies – when they weigh up what they might lose or gain, the risk seems low and is surpassed by the benefits they expect.

In addition, children need to have the digital skills to understand and operate the digital environment to be able to protect their privacy effectively. Both underestimating the risks and overestimating one's skills is linked to fewer privacy protective strategies.

> *Unless you have somebody to actually explain to you how dangerous everything is, you wouldn't know… When you're looking through these social media sites, there's nothing to actually say, hang on, wait, this could be dangerous. (girl, Year 9, Wales)*

> *I don't mind if they [companies] know all this […] I think I'm smart enough to know if someone's trying to kidnap me on the internet, or trying to sell stuff to me that might get me in trouble. I think I can pick that out and avoid it. (boy, Year 7, London)*

When asked about their learning experiences, children often refer to their e-safety training, most often part of IT or citizenship. While some of the issues in the curriculum are relevant to privacy (online contacts, sharing information), most often the topics are within the realms of interpersonal privacy and data given, providing a partial picture of the online ecology.

Children also find the current information insufficient and often repetitive, wanting to be taught more relevant material that sparks their curiosity. The suggestions of what they want to learn about range from practical skills of how to handle spam mail to learning about the dark web.

> *They spent, like, two hours doing this workshop with us about being safe online, how we can prevent certain things from happening. Like spam, for example. And then junk mail, you know, phishing, how to prevent it, and why people might do it. (girl, Year 7, London)*

> *We just get bored and don't listen. (girl, Year 9, Essex)*

> *That's basically what they're trying to say is just like, oh yes, don't do this, don't do that, don't do this. When it's like basically the whole point of that thing. (girl, Year 9, Scotland)*

✓ Understanding grows with experience, but there's no 'magic' age of capacity

We met knowledgeable 11-year-olds and confused 16-year-olds – understanding depends on many factors beyond age.

Children have different capacities to understand privacy and different needs that cannot be explained entirely by age. We found that any age group includes children with very different needs and understanding – some 11-year-olds were much more competent than some of their 16-year-old peers. Each child's privacy knowledge and skills evolve gradually and at a different pace and there is no magic age at which a new level of understanding is reached. The need to treat each child as an individual is acknowledged by children, parents and teachers alike.

Children often acknowledge that personal needs, abilities and circumstances should be taken into consideration because children are different and what works for one child might not be suitable for another. Their personal experiences show that the online environment does not show enough flexibility and it is mostly children who need to adapt and to keep up with their peers. Still, they envision the benefits of a more tailored approach and acknowledge that social and technological change leads to generational differences in how children use and experience the internet.

> *There's a lot of, like, variables, but it depends on how you are, if you're mature enough. (boy, Year 11, Wales)*

> *Nowadays, there's, like, Year 5s with Instagram and Snapchat. (girl, Year 11, Wales)*

> *I think they're just too young to be able to know what they're doing as well. (boy, Year 11, Wales)*

Grasping 'where your data goes' is a moving target because technology, regulation and social practices all evolve and innovate.

While children want to keep up with technological developments and trends among their peers, this is not an easy task. New features and devices, app updates and the constant flow of new platforms and services make it hard to follow. On many occasions, they feel that they are playing a 'catch-up'

game and rumours spread as they try to make sense of what the innovations mean. Very few are able to grasp how new regulations, such as the GDPR, affect their rights and experiences even though almost all children recall seeing many more privacy messages than before and having to give consent. Keeping up with app updates and having to change settings over and over is particularly confusing and frustrating for them.

> *Snapchat … didn't say anything about ghost mode. I only found out because my teacher told me. (girl, Year 7, Essex)*

> *If they've changed the privacy settings [with new updates], you might have to change it back. (boy, Year 11, Midlands)*

Even by 16 years old, few children can map the global data ecology beyond the screen or 'behind the scenes'.

Even the oldest children struggle to comprehend the full complexity of internet data flows and some aspects of data commercialisation. Most understand that they are being targeted with advertising and are able to make connections with what they have previously done online (e.g., online searches, likes, purchases), but the functionality of how this happens remains a puzzle for many. Few consider the wider implication from this relating to the algorithmic reshaping of the online environment and how it might bias their online experience.

> *They use it to direct your attention towards stuff that you can be buy. (boy, Year 11, Essex)*

> *If you have an advert, like on an app or something, it usually says download now, and like it's easy to download stuff. (girl, Year 7, Scotland)*

> *Maybe cookies have a positive effect because if you're searching for beans and then you get ads for beans, maybe you can find a better price. (girl, Year 7, London)*

Still, there are broad trends – younger children are more trusting; older ones are becoming cynical.

Findings: children's views of privacy-related harm

✓ Only e-safety risks seem truly real

Since children find it hard to think about privacy risks beyond the interpersonal level and the information they give, they find it hard to think about possible harms other than interpersonal, often covered in e-safety discussions. While they are aware of data breaches and leaks, such risks seem remote from their experience and with unforeseeable consequences. Other risks leading to possible negative outcomes in the future, for example, in relation to education or employment opportunities, are also hard to imagine and relate to. In some cases, children draw on information from the news or the experiences of people around them to learn about possible harms. These are mostly longer-term consequences related to delayed harmful effects from online data.

> *If you try to apply for a job and you put something on the internet and it comes back… [My brother] posted something online about the boss of the company that he applied for. He couldn't actually get the job because he was quite offensive towards him. (boy, Year 9, Essex)*

> *That happened to Jack Maynard, didn't it. He went on, 'I'm a Celebrity', and then they found out stuff he put on Twitter ages ago and then he couldn't be on it anymore. (girl, Year 11, Essex)*

Children struggle to see how they might have a more active role in protecting their privacy online in relation to risk arising from institutional and commercial use of their data, an environment they generally experience as confusing and overwhelming. Finding it hard to predict how they might be harmed, they tend to focus on the more certain and immediate benefits, such as socialising, participation, entertainment, and on managing risks related to the interpersonal.

> *It's all really overwhelming when it comes to things like the internet, and people don't realise how careful they need to be. (girl, Year 9, Wales)*

> *I don't see how that could harm you because how is somebody going to use your dental records against you? Fingerprints as well, nobody else will have the same one so they can't use that against you in a way. My face is my face and nobody else has my face so how would they use that against me? (girl, Year 7, Midlands)*

Experiences of harm are rare and mainly concern embarrassment or reputational damage. Children are mostly worried about negative reactions to something they have posted online, especially things that they did when they were younger, and generally avoid posting sensitive information as a way of preventing harm. Reputational damage can also be caused by lack of sufficient reaction – not getting enough 'likes' can also be a reason to remove online content.

My aunt was commenting on a lot of my posts, and it's sort of getting a bit embarrassing, so my mum spoke to her and she doesn't do it anymore. (girl, Year 9, Wales)

You look back at your memories and you're just like, why did you do that? (boy, Year 11, Essex)

Children often express their discomfort through the idea of things being 'creepy'. Even though children rarely discuss significant harms, they very often express general discomfort with various technological features, advertising techniques and data harvesting, and tracking more generally. Words like 'creepy', 'weird', 'scary' and 'dodgy' are often used to describe their experiences of an ecology that sometimes invades their privacy.

I think that facial recognition is really creepy… It's just so weird. Why are you doing that? (girl, Year 9, London)

Instagram, they ask [to access your contacts] so that you can add people that you might know, but that's still kind of dodgy. (girl, Year 7, Midlands)

On Instagram, if you click on the location of the image […] and you can see exactly where they were when they took this photo. It's really, really creepy. (girl, Year 9, London)

I was trying to find this book and I couldn't find it and then this morning it popped up on Instagram and I found it really strange […] it helped me find it, but it's really weird because it's like an invasion of privacy. (girl, Year 7, Midlands)

✓ Children delight in their agency but are reluctantly aware of their limits

Children's confidence is grounded in trusted social relationships – they are figuring out the digital world with friends, learning from parents, school, the news etc.

Children are actively learning about the online environment, drawing on a wide range of social, educational and online resources. When unsure what to do or faced with difficulties online, they often expect to be able to sort things out on their own, usually by searching for more information online. Peers or siblings are also important sources of support that children turn to when they are not able to resolve the problem on their own. Sometimes they also turn to parents and teachers, even though this tends to be when the situation is more serious or when the particular adult is seen as an expert in the field. Many children expect to know more about technology than the adults while others find that everyone is equally confused and unable to predict what the privacy implications are –resulting in children trying to figure out independently their way around.

I just ask one of my pals because my mom and dad wouldn't know. I just expect them not to know. (girl, Year 7, Scotland)

Like, if I can't find something, or done something wrong … I just ask my brother to help me and then he helps me. (boy, Year 7, Scotland)

[When I need help, I ask] My computer science teachers because they're the most experienced because they've got a degree and stuff. (boy, Year 9, Essex)

[Dad] he's got a software degree, so that's why I go to him, because he, that's his job, that's what he does. (boy, Year 11, Scotland)

No one really knows what's going to happen. No one knows where it's going to go. (girl, Year 11, Essex)

But at a certain point in each focus group, children recognised their powerlessness, and then their talk swiftly became dystopian. Children often switch between the fairly relaxed attitude of 'I have nothing to hide' to a dystopian nightmare with horror stories about abduction, hacking, and scandals around social media misuse or privacy breaches. They struggle to build a comprehensive and balanced view of possible negative outcomes and fall into apocalyptic scenarios when they realise their own powerlessness.

Just a few bits of information can completely give away who you are, where you live, what school you go to… People who do bad things can put that together and completely wreck your life. (boy, Year 9, Wales)

All these people building robots, I just think it's stupid. What if it does a robot uprising? I'm being serious. (girl, Year 11, Essex)

It could come back and hurt you in the future … that could come back and get you sent to prison. Facebook could be your downfall. (boy, Year 11, Essex)

Findings from parents

✓ Parents are confused and concerned

Although children often turn to their parents for guidance about their privacy online, parents feel ill prepared: most trust the school and government, but fewer trust companies.

Parents are equally confused about the digital environment and the dangers it proses to privacy, finding it hard not only to predict the direction of development in the future, but also to know what actions they should take and what advice they should give to their children. Even the more technology-savvy parents are not confident that they know how best to support their children, often finding themselves helpless to prevent risks.

> *What are these big corporations going to do with all that data and how are they going to manipulate me or anyone, or anyone else's life in the future? […] I can't really educate my child on that because we don't know, I don't know where we are on that. I don't know where I am on that myself. (parent, London)*
>
> *We don't know exactly what we're dealing with. We know some of the dangers but I'm sure there's an awful lot out there that we're not aware of. (parent, London)*
>
> *Our kids are the sort of guinea pig generation. […] We don't know what the consequences are going to be. (parent, London)*

In contrast to children, parents are much more sceptical about the business model and criticise companies for disregarding children's interests and rights in the pursuit of commercial benefit. Still, when it comes to institutional privacy, they often trust the education system and expect it to work in children's best interests and to protect their privacy.

> *If a 13-year-old can decipher the legalities and ins and outs of what they're doing. Do you think they will be...? I don't think they'll be savvy or quite understand the terms that all these internet companies use. I think they're just paying lip service. (parent, London)*
>
> *[Student data used by schools] I assume that it's mainly anonymised or pseudo-anonymised, but I don't know. […] My feeling is if it's for a good purpose. I'm not aware that they're using it, you know, that they allow a third party access to it. I'd be quite annoyed if they did. (parent, London)*
>
> *What does the government do with SATS results and all the data that the teachers are collecting? Where does it go, where is it flogged onto? (parent, London)*

There are substantial differences in the support children receive from parents, which creates important inequalities, making some children more vulnerable.

Overall, children want to be able to make their own decisions and not be bound by (parental or school) rules or by app functionality. They see the internet as a place that enables them to do things they

enjoy, and when faced by limitations, they usually protest (where they can use their phone, what apps to use, in-app purchases and device compatibility). Still, they understand that these regulations are often there with a good reason and sometimes for their own protection.

Parental mediation varies significantly. The more active parents provide advice, supervise children's activities (e.g., ask them to check the settings when installing a new app), check their mobile devices and make decisions about what platforms are suitable and how long children should spend online. Some even track their children's whereabouts via location-based apps. Other parents are much less engaged in their children's use of technologies, allowing their children to have more independence and make their own decisions. In many cases these are parents who know less about digital technologies and are less able to provide advice to their children.

> *My mum has loads of them [apps] that find out where I am. […] It's quite annoying but she's being doing it for ages so I'm kind of used to it now. (girl, Year 11, Essex)*

> *My mum always tells me to stop and read it [the Terms and Conditions]. I'm like, no. But she actually forces me to, basically. But she reads it instead of me. (boy, Year 11, Wales)*

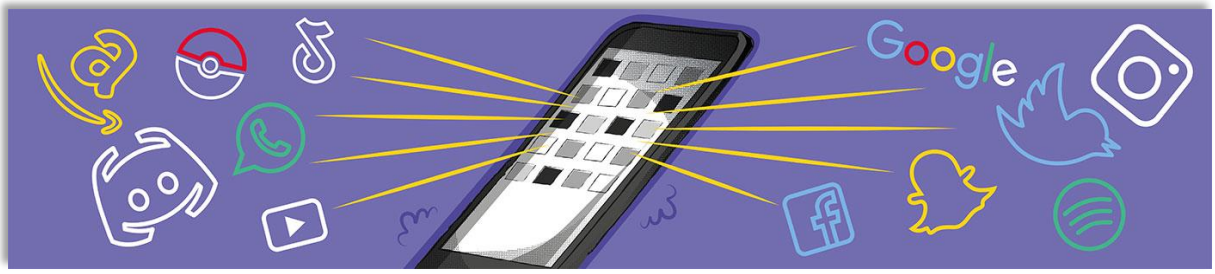
> *My parents still go on my phone. They check my social media but that's pretty much it. (boy, Year 11, Wales)*

The gaps in parental skills and competence are acknowledged by the parents who see this as a potential source of inequality that might make vulnerable children even more disadvantaged.

> *Some of the parents don't have that time or understanding. Sometimes they don't understand certain things about the internet. (parent, London)*

> *I think putting it with parents makes it very hard. Because there are some parents who don't realise the impact of this and other parents who just don't care. […] As soon as you put it in the hands of parents you then create an imbalance. (parent, London)*

Parental mediation does not always depend on the child's age, but overall we found that parents are generally more engaged when children are younger. By the time children reach secondary school, their internet and device use is fairly independent and mostly unsupervised. Both children and parents expect parental supervision to diminish as children grow older, while mediation from older siblings is somewhat more acceptable, even at an older age.



Findings from teachers

✓ Teachers focus mostly on what works in teaching and safeguarding, often trying to keep up with the students

Some teachers acknowledge that children are sometimes more savvy with technology use and they need to catch up with them, not unlike the parents who also do not always think that they have the 'upper hand'. This sometimes means that teachers have to limit their responsibilities for life beyond school, but do try to remain engaged and helpful as much as possible.

> *They [children] are able to use these things better than the people around them because they're so used to it. […] They're more in tune because they've grown up with it. (teacher, London)*

> *We're playing catch up because they're so advanced. (teacher, London)*

More broadly, teachers are as concerned as everyone else: they express fears about children's overconfidence, lack of support seeking and more generally, about the complexity of online privacy.

> *In terms of companies collecting data on students, though, I just think that for me is a massive grey area. (teacher, Midlands)*

> *Children are savvy enough to not tell you until they've stepped too far. Then you hear about it. So I think that's the actual worry. (teacher, London)*

> *The biggest issue that we've got at the moment is that kids generally on a whole tend to be completely independent when they're online. (teacher, Midlands)*

> *I don't think there's anything you could do or say that will change their mind. Because they know what we're saying is nothing new. (teacher, London)*

In their accounts of digital literacy privacy is generally positioned within e-safety (i.e., in interpersonal terms) with little on the data economy or digital infrastructure.

Teachers acknowledge the numerous challenges they need to address in relation to the digital literacy curriculum – from the format of delivery and embeddedness of technologies in the learning process to more engaging content focusing on opportunities and positive messages.

> *Anything connected to technology, it's almost out of date a week after it's been written. So, what we are trying to do is focus these lessons, and it's almost digital literacy plus. (teacher, Scotland)*

> *They've had that certain level of intervention from the primary schools but it's just generic stuff, it's 'don't give out your date of birth', 'don't give out your address', 'don't give out' and it's much more than that. In terms of their data, in terms of their personal information, I don't think they're wised up. (teacher, Midlands)*

Too often, this story about e-safety gets cast in terms of the really horrible things. (teacher, London)

To embed the use of technology in the learning, the learners need to be allowed to, to some extent, have their technology needs to be accessible all the time, whether it's at break, lunch, in the library or in class. (teacher, Scotland)

Teachers discuss at length their school's practice around GDPR compliance, but also trust that the school system works and is properly regulated. They generally express confidence in the school's procedures of collecting, storing and using students' personal data and discuss at length how the school ensures its GDPR compliance. On many occasions this is supplemented by specific information about the system in place, but in other cases it was more of a general feeling that suitable rules and regulations are in place and a trust that the system works.

We have a protocol of when to delete information and how long to keep it for. We have secret files that only certain people are allowed to open and stuff like that. That's my interpretation. (teacher, London)

We store everything on our own internal hard drives and we have a secondary school where that's all backed up. (teacher, Essex)

The only time it does [to the government] is when we do the Year 11 data […] Because obviously they'll do the tracking of different groups. (teacher, London)

While there is certainty that some practices are in place – such as asking for permission for collecting students' data and taking photographs – and clear procedures for storing and accessing student data, in other cases teachers are unclear what happens to students' data, particularly when it comes to using educational platforms.

I don't know what it collects from them. (teacher, London)

But I would've thought the fact that it's a school-based software, this is all been properly regulated. (teacher, London)

I have to say I'm more interested in the educational side of it and it works for the class. Then as long as it's not collecting their name or email address or anything like that. (teacher, London)

What should be done

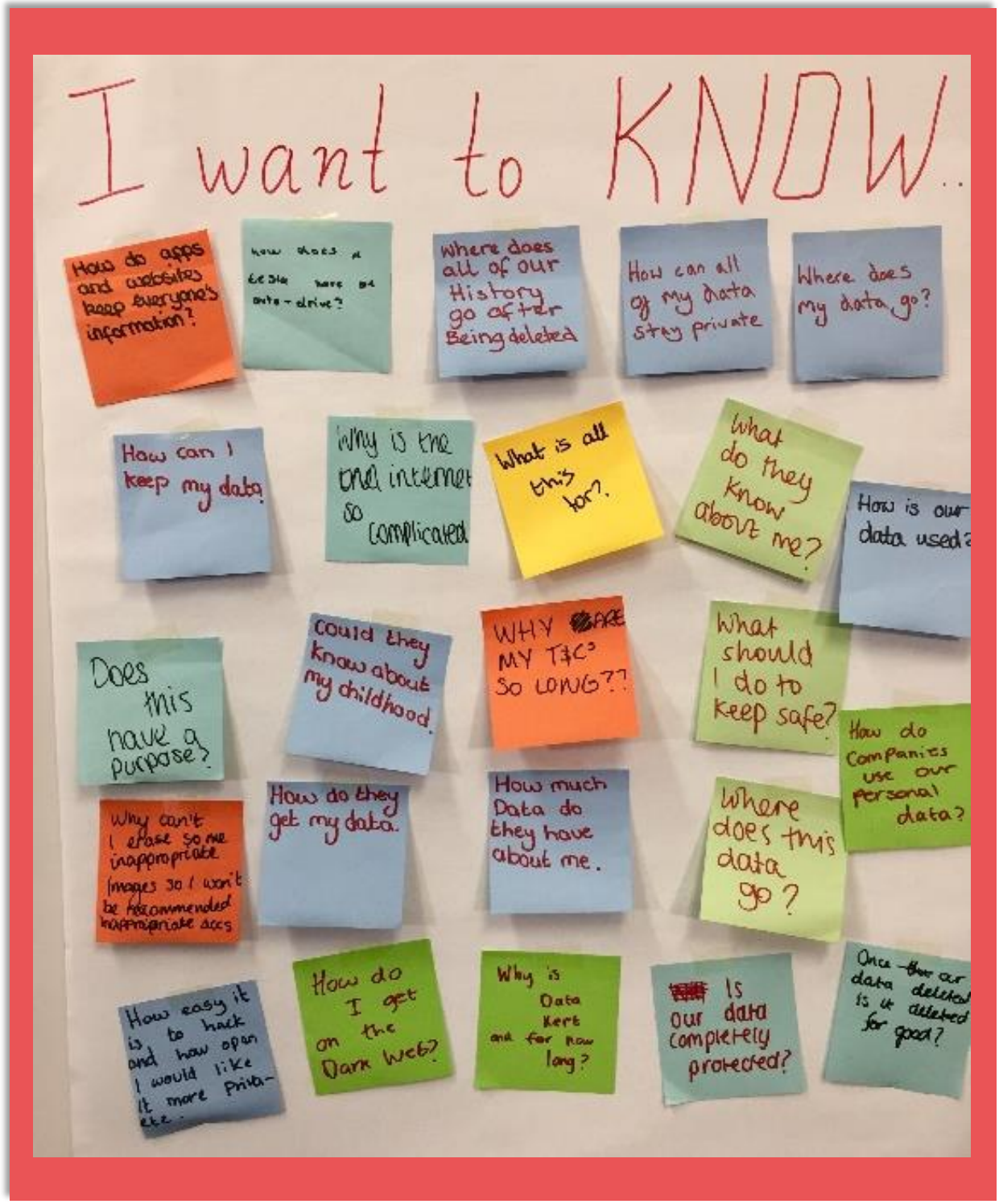
✓ There are lots of things children want to know, and lots of things they want to change

In each focus group we invited children to share what they would like to know about their online data and privacy and, second, to list the things that others (parents, educators, regulators and companies) should do differently to make privacy better.

Overall, children's questions are most often related to how their data flows online, how long it is kept and how it is used. The most popular suggestions for change refer to clearer Terms and Conditions, getting more free content (e.g., less in-app purchases), apps collecting only data that is necessary, not sharing children's data with other companies, prevention of data leaks and being able to delete online information. These are the priorities as children see them, and the main demands that they want to make of regulators and industry.

The team summarised the most popular suggestions and presented them to the child juries, inviting the children to deliberate on the importance of each suggestion and select the ones that should be prioritised. This process demonstrated that the children overall do not think that others (adults) listen to their opinions, suggestions or complaints, and they are keen for their voices to be heard more. They also do not think in terms of their rights online, and experience the digital environment as quite dismissive of their needs and personal preferences.

But they do expect the internet to be mostly fair, and they expect parents, educators, regulators and companies to act responsibly and in children's interests. They want to have an active role in making decisions about their online participation and in protecting their privacy, but also see this as a shared responsibility of all the stakeholders involved. While children can be practical and understand that the commercial model behind the apps they use requires their participation (e.g., that sometimes they have to watch an advert to unlock some content), they also become critical and frustrated when things do not work as they should and nothing is done to fix this (e.g., when they report an incident online and do not hear back).


I want to KNOW..
How do apps and websites keep everyone's information?
Where does all of our History go after Being deleted
How can all of my data stay private
Where does my data go?
How can I keep my data
Why is the UNCL internet so complicated
What is all this for?.
What do they know about me?
How is our data used?
Does this have a purpose?
could they know about my childhood.
WHY ARE MY T&C's SO LONG??
What should I do to keep safe?
How do Companies use our personal data?
Why can't I erase some inappropriate images so I won't be recommended inappropriate accs
How do they get my data.
How much Data do they have about me.
Where does this data go?
How easy it is to hack and how open I would like it more private.
How do I get on the Dark Web?
Why is Data kept and for how long?
Is our data completely protected?
Once our data deleted is it deleted for good?


I want to CHANGE
I want to change that you only have to dismiss pop ups on the apps.
Child friendly T+C's
The fact that there is no way to clear anything completely from the internet
By default accounts should be private
To let people know or specify that once you search something is in the system for good
More education in internet safety
What can I do to prevent private info being leaked?
Concise systems of support
Tighter ways of protecting data so people can't get hacked
I think we should have to give consent for our data to be sold
A way for Data to be Permanently Deleted
Instagram should start your profile off as private
Some social media moderators to be made active more
Make sure permissions etc. are appropriate
Way to access what the internet knows about us.
The Safety of who's watching you
A safe place to use
Can T&Cs be made easier to read?
Check Data is appropriate
Make closing accounts easier
Record not permanently
Encrypting is accurate
There needs to be a way to control the screen time
NO! stalkers Paedophiles
Kid-friendly social media to get used to it
Higher ages limits

Children's views of how their data and privacy online should be addressed: what they want to know, and what they think should be changed

	What children want to know about their data and privacy online	What children think companies should do differently
All ages	• Who has got my personal data, how long do they keep it and what do they do with it? • Why do they collect, share and sell my information? • Where does deleted data go, is it really gone?	• Make deleted apps or information permanently 'gone' • Provide more and better privacy, security and safety options • Make accounts private, turn off geo-location and disable cameras by default • Don't share my data with other sites or services • Better responsiveness to user concerns and complaints • Make Terms and Conditions understandable, short and visual
11- to 12-year-olds	• Why do apps need to know your phone number? • Who controls the websites? • Who can find out about my information? • Why do they set age restrictions so high (e.g., WhatsApp)? • Why don't companies remove scamming sites? • Why is reporting stuff so hard? • Why do they make mistakes about who you are?	• Let under-13s use social media but keep their account private • Make online content more appropriate for our age • Take down hostile content (e.g., fat shaming)
13- to 14-year-olds	• Who can see what I search? • Can people see me through my camera or hear my voice? • What do social media sites do with your information? • What happens when you get hacked? • What happens to your data when you die? • What is the dark web? • What do they do with your face when you use facial recognition?	• Allow paid-for but private apps • Not sell our data • Not show me what I'm not interested in • Make it easier to erase your account
15- to 16-year olds	• Where is data kept, how does it travel across the internet, and what is shared with other companies? • Why do they need to know so much about me (e.g., my gender)? • Is sensitive data shared?	• Leave me alone • Keep biometric data safely • Delete our data after a certain time (e.g., two years) • Only ask for information when relevant • Allow you to opt out of data collection • Better checks on age restrictions • Explain what information they have about you

✓ Parents and teachers ask for higher-level solutions

There is an overall agreement that children cannot, and should not, be expected to navigate a very complex, even for adults, online environment. While learning from mistakes is part of growing up, evidence for children's mistakes is recorded more permanently once it reaches the internet, which is a cause for concern. Both the parents and teachers want children to have a greater freedom and not to be 'followed' by mistakes they made.

> *I don't think children are bothered how it's going to affect at all at this stage in their life … you're a kid. You're meant to make mistakes (teacher, London)*

> *They aren't all going to be responsible, and why should they be? They are kids. They should be allowed to have innocence, which goes with not being utterly responsible. So I think government and companies have to be the responsible ones. You can't necessarily rely on the kids to do that. (parent, London)*

> *They should just be allowed to be kids and not worry about if we made a mistake at school or did something silly, people are going to remember it for a day, a week maybe a couple of weeks. But not once it's there. (teacher, Midlands)*

Parents and teachers see themselves as responsible for educating children about online privacy and supporting them to make the right decisions. At the same time, they often find themselves overwhelmed and unsure how to help children – and seek more support from others. Still, the most prominent demands are for better regulation and more responsible engagement from industry – two stakeholders that need to do much more than what has been achieved at present.

> *We're six hours a day with a student […] You simply cannot influence all these social outcomes through this conduit; there has to be some kind of government regulation on it. (teacher, Essex)*

> *I think they [industry] should definitely take more responsibility for what they're doing. (teacher, Midlands)*

> *They [industry] have got all the brains and software technology, as far as I am aware, to place real constraints on what children could access. They could do it, it's just that they have to accept that they can't make as much money. They could regulate, and there could be a much more powerful regulation from government. They could easily limit what kids could do, in a responsible society, which we don't have. (parent, London)*

> *I think organisations need to do more on children's safety online as well. (parent, London)*

A toolkit for children

Privacy toolkit – freely available at www.myprivacy.uk

- We built a toolkit for children (with guidance and resources for parents and educators).
- The aim is to improve 11- to 16-year-olds' understanding of their data and privacy online.
- The resources had to meet key criteria (free, good quality, no installation or sign up, etc.) and were reviewed by our youth juries (Years 8 and 10).

Online privacy: what's the issue? We share a lot about ourselves online, why does it matter?

Who has my data? Sometimes apps collect information that's unexpected. See what apps collect about you and how.

Who is tracking me? Who gets your data and how do they use it?

What are my rights? As a child, you are entitled to extra protection. See what rights you have.

What can go wrong? Things might sometimes go in unexpected directions. See what might go wrong - now or in the future.

What do children ask for? We spoke to many children across the country. See what questions and suggestions they have.

How to protect my privacy? There are a lot of things you can do to protect your privacy. Find out more.

Where to get help? This is where you can report problems and seek help from trained professionals.

Watch and play Privacy can be fun! Watch some videos and play games.

Recommendations

- **Child rights-respecting policies must promote autonomy, balance protection and participation, and prevent discrimination and other harms:** a healthy balance between children's independence and protection can foster their development, agency and exploration of the physical, social and virtual worlds. Policy and educational measures to ensure children's privacy online and safety should also facilitate their autonomy, proactive risk management and right to participation.

- **Distinguish privacy in interpersonal, institutional and commercial contexts, and ensure policies are context-appropriate and clearly comprehensible:** post-Cambridge Analytica, and post-GDPR, children are becoming aware of the commercial and institutional uses of their data. However, awareness of how children's data is recorded, tracked, aggregated, analysed and monetised is partial and often hard to master, not only by the oldest children, but also by their parents and teachers. It requires developing an understanding of the business models operating in commercial and institutional contexts. This larger understanding – of platform architectures and networked data flows and transactions – is something children are rarely taught about, whatever their age or maturity.

- **Sustained media (data, digital, critical) literacy is vital from an early age – in school curricula and teacher training – but it is not a 'silver bullet' solution:** children start facing privacy decisions and risks as soon as they enter the digital environment, long before their media literacy prepares them to make decisions in their own best interests. They are primarily mindful of data given in interpersonal contexts, and their awareness of the consequences for their privacy depends on their developing understanding – differing by age, maturity and circumstance. Media literacy and privacy-related skills need to be enacted by children, rather than taught as external rules, and need to reflect their actual concerns and experiences. Children need to be able to make more autonomous decisions about effectively protecting themselves online, to gain experience in coping with unexpected or undesired situations, and to learn from mistakes. Yet, media literacy should not be seen as the ultimate solution to all problems. Children cannot and should not be expected to understand and manage the full complexity of the online environment, and some solutions need to happen at the level of regulation and design – a demand that children, parents and teachers insist on.

- **Regulate for privacy-by-design and by-default, and provide child-friendly age-appropriate mechanisms for privacy protection, complaint and remedy:** in the absence of an agentic and meaningful relationship with the businesses or institutions that process their personal data, and in the absence of a sufficient critical understanding of the wider contexts within which those businesses or institutions operate, it is likely that children will continue to think of

data primarily as data given and privacy in interpersonal terms. Children cannot be expected to be solely responsible for handling the complex privacy environment – instead, those relationships and contexts will have to change if children's right to privacy is to be protected. Further work is needed to increase the transparency of data collection, improve privacy control navigation, enable granular control over privacy settings to match the elaborate data-harvesting techniques and create better industry standards around user empowerment. Ease of use, ubiquitous functions and user-friendly features of the privacy setting interface may reinforce children's privacy protection behaviours.

- **Support children by supporting parents, schools and the organisations that work with families and vulnerable children:** adults are often left feeling 'behind' digital developments and struggling to identify the best ways to support children. A comprehensive system supporting children, schools and organisations working with children is a prerequisite for developing privacy awareness and skills, as well as safety mechanisms. Rather than focusing predominantly on parental mediation that can create inequalities and put vulnerable children in a disadvantaged position, a wider approach that engages children's support networks in their full breadth can allow children in different circumstances to receive the support they need.

- **Sustain a robust evidence base that fills key gaps (e.g., include younger children), evaluates the effectiveness of interventions and consults children:** there are still substantial gaps in existing knowledge related to children's developmental needs, particularly for younger and vulnerable children. We need a better understanding of what support and education strategies are most efficient in helping children to take advantage of the existing opportunities, avoid harm and foster resilience and self-efficacy, and what policies and regulations are best equipped to mitigate privacy risks and foster a safe online environment for children. In producing this knowledge, and in designing services, regulation and policy, it is vital that children's own understandings of the digital environment are taken into account. A child-focused approach can give recognition to children's voices and facilitate and support their heterogeneous experiences, competencies and capacities. It can also create opportunities of peer-to-peer support and a more inclusive and tolerant online environment.

Project outputs

Publications

- Livingstone, S., Stoilova, M. and Nandagiri, R. (forthcoming) Data and Privacy Literacy: The role of the school in educating children in a datafied society. In D. Frau-Meigs et al. (eds) *Handbook on Media Education Research*. London: Routledge.

- Stoilova, M., Nandagiri, R. and Livingstone, S. (under review) Children's understanding of personal data and privacy online – A systematic evidence mapping. *Journal of Information, Communication and Society.*

- Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) *Talking to Children about Data and Privacy Online: Research Methodology*. London: London School of Economics and Political Science. [**Report**] [**Supplement**]

- Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) *Children's Data and Privacy Online: Growing Up in a Digital Age. An Evidence Review*. London: London School of Economics and Political Science. **[Evidence Review] [Executive summary] [Supplement]**

- Livingstone, S., Stoilova, M. and Nandagiri, R. (2018) Consultation response to the Information Commissioner's Office Call for evidence on Age Appropriate Design Code.

- Livingstone, S. (2018) Children: A special case for privacy? *Intermedia*, 46 (2), 18-23.

Blog posts

- Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Where does your data go? Developing a research methodology for children's online privacy. *LSE Media Policy* [online]

- Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) Children's personal privacy online – It's neither personal nor private. *LSE Media Policy* [online]

- Nandagiri, R., Livingstone, S. and Stoilova, M. (2018) 11 key readings on children's data and privacy online. *LSE Media Policy* [online]

- Livingstone, S., Stoilova, M. and Nandagiri, R. (2018) Privacy, data protection and the evolving capacity of the child: What the evidence tells us. *LSE Media Policy* [online]

- Yu, J., Livingstone, S. and Stoilova, M. (2018) Regulating children's data and privacy online: The implications of the evidence for age-appropriate design. *LSE Media Policy* [online]

- Livingstone, S., Stoilova, M. and Nandagiri, R. (2018) Conceptualising privacy: what do, and what should, children understand? *www.parenting.digital* [online]

Talks

- Livingstone, S. (2019) Children's personal data and privacy online: It's neither personal nor private. Public lecture for the Psychological Society of Ireland, Dublin.
- Livingstone, S. (2018) Privacy literacy, consent and vulnerable users: Children and the General Data Protection Regulation. Lecture to the Oxford Internet Institute, May.
- Livingstone, S., Stoilova, M. and Nandagiri, R. (2018) Children's conception of privacy online. OECD Expert consultation – 'Protection of children in a connected world.' University of Zurich.
- Livingstone, S. and Stoilova, M. (2018) Children's data and privacy online: Exploring the evidence. Presented at London School of Economics and Political Science, September.

References

Kidron, B., Evans, A. and Afia, J. (2018) *Disrupted childhood. The cost of persuasive design*. London: 5Rights.

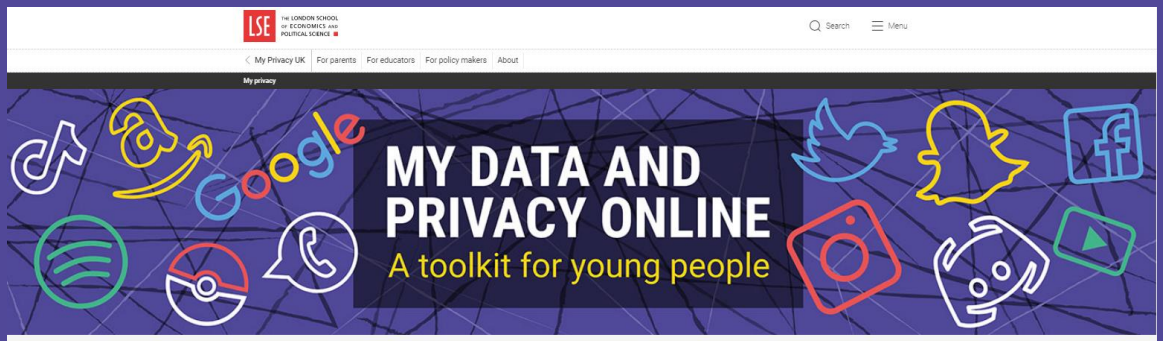
Livingstone, S., Carr, J. and Bryne, J. (2015) One in three: The task for global internet governance in addressing children's rights. *Global Commission on Internet Governance.* London: CIGI and Chatham House.

Nissenbaum, H. (2010) *Privacy in Context. Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

van der Hof, S. (2016) I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal* 34(2), 409-45.

Westin, A.F. (1967) *Privacy and Freedom.* New York: Atheneum.

www.myprivacy.uk



My privacy

"Well we don't actually know where the information is going. You can sign up for an app and tell them your name and your age and stuff and they'll say at the bottom that it's all private and stuff, but then it goes somewhere. There's the question of where does it go."

boy, year 11, Midlands

Imagine that the internet knows everything about you! Does it matter if it does? What can you do to protect your privacy and data online?

We all use the internet a lot in our everyday life. We reveal a lot about ourselves online. And a lot of our data is being recorded and stored online by others (family, school, companies).

Who has access to personal information about us? Why is our data being collected and why? What can go wrong?

This toolkit will help you answer some of these questions. It has been developed in discussion with young people around the country.

Try it out below!

Print or share

ico. Grant Recipient

Online privacy: what's the issue? We share a lot about ourselves online, why does it matter?

Who has my data? Sometimes apps collect information that's unexpected. See what apps collect about you and how.

Who is tracking me? Who gets your data and how do they use it?

What are my rights? As a child, you are entitled to extra protection. See what rights you have.

What can go wrong? Things might sometimes go in unexpected directions. See what might go wrong - now or in the future.

What do children ask for? We spoke to many children across the country. See what questions and suggestions they have.

How to protect my privacy? There are a lot of things you can do to protect your privacy. Find out more.

Where to get help? This is where you can report problems and seek help from trained professionals.

Watch and play Privacy can be fun! Watch some videos and play games.