

Children's data and privacy online: challenges and solutions

#ChildPrivacyOnline

Department of Media and Communications
London School of Economics and Political Science (LSE)
24 June 2019

Meeting report

Author: Gianfranco Polizzi, on behalf of the Children's Data and
Privacy Online project



Overview

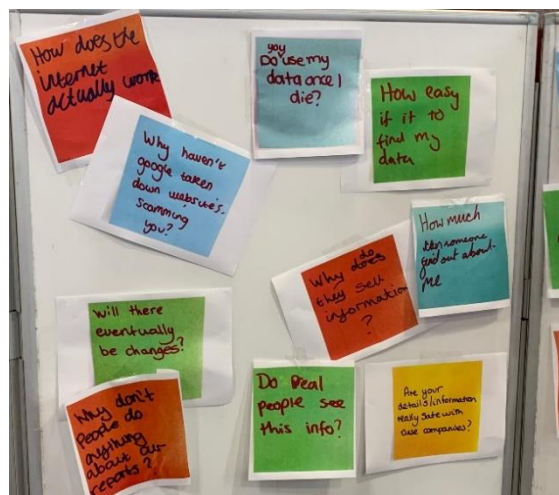
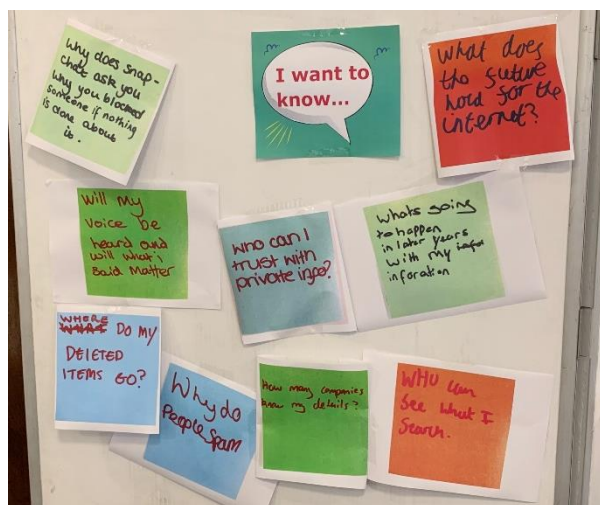
The project [*Children's data and privacy online: growing up in a digital age*](#) led by Prof [Sonia Livingstone](#) recently launched its findings and an online privacy toolkit for children, parents and teachers. The event gathered a range of different stakeholders, from academics to representatives from tech companies, the media industry and civil society and focused firstly on what the existing evidence tells us about children's data and privacy online and what gaps matter, and secondly on the way forward, sharing the responsibilities among stakeholders, and who should do what and how. This report summarises the presentations and discussions.

As Livingstone pointed out in her opening speech, the event is timely and follows the [Information Commissioner's Office](#) (ICO) consultation with relevant stakeholders and the development of a draft age-appropriate design code. The code aims to ensure that online services are designed in ways that safeguard children and their personal data.

Contents

Morning poster presentation: What do children want to know?	3
Children's data and privacy online: growing up in a digital age (<i>Sonia Livingstone, Rishita Nandagiri and Mariya Stoilova, LSE</i>)	3
Breakout session 1: Children's data and privacy online – what the evidence tells us & what gaps matter	7
Age appropriate design: A code of practice for online services (<i>Elanor McCombe, Information Commissioner's Office</i>)	9
Lunch poster presentation: What do children want to change?	13
A new deal between children and the tech sector? (<i>Jay Harman, 5Rights</i>)	13
Breakout session 2: the way forward for children's data and privacy online: sharing the responsibilities among stakeholders – who should do what and how	15
Panel discussion: "Challenges and solutions for children's data and privacy online" <i>Victoria Betton (NHS), Jen Persson (Defenddigitalme), Liz Moorse (Association for Citizenship Teaching), Vicki Shotbolt (Parent Zone) and Sally Greig Lockwood (BBC)</i>	16
Final remarks (<i>Sonia Livingstone, LSE</i>)	18
Appendix 1: Seminar agenda	20
Appendix 2: List of attendees	21
Appendix 3: Project outputs	23

Morning poster presentation: What do children want to know?



Children's data and privacy online: growing up in a digital age (Sonia Livingstone, Rishita Nandagiri and Mariya Stoilova, LSE)

Download: [findings report](#), [presentation](#)

Access the online privacy toolkit: www.myprivacy.uk

Key points:

- We live in an age with continual technological innovation that presents both opportunities and challenges. Children are often the pioneers – the “canaries in the coal mine in the digital age”.
- Their research draws on Nissenbaum's definition of privacy. Privacy is not about secrecy nor control. It refers to the “right to appropriate flow of personal information”. We exercise privacy in particular contexts, and privacy is relational. In other words, privacy matters in terms of social relationships and conditions, which involve a full range of actors, among whom institutions.
- As everything in our life has become datafied, there are new challenges (e.g., the challenges of age verification, data breaches). Academics need to ask what “working well” means in our complex data ecology. To answer this question is challenging because it requires expertise that draws on multiple fields (e.g., legal, technological, childhood studies).
- As children are little consulted about data and privacy, Livingstone, Stoilova and Nandagiri's ICO-funded research is underpinned by the following research questions: (1) How do children understand their privacy online? (2) What capabilities or vulnerabilities shape how they navigate the digital environment? (3) What evidence gaps impede the development of policy and practice? (4) What are the implications of children's understanding and practices?

- Theoretical framework: the study maps the digital environment in terms of three privacy contexts and types of data:
 - Interpersonal privacy: data given, data given off (observed), inferences (by others)
 - Institutional privacy: data given, data traces (records) and inferred data (analytics)
 - Commercial privacy: data given, data traces (metadata) and inferred data (profiling)
- The study includes a systematic mapping of the available evidence focused on empirical studies with children. This found that most studies tend to be with older teenagers and on interpersonal privacy. There is very little research on how children understand institutional privacy and commercial privacy.
- Methodology: the study employed a child-centred qualitative methodology, conducting focus group discussions with children aged 11-16 from different parts of the UK. The focus groups were interactive and participatory. The team also spoke with teachers and parents. The focus groups started by asking children to write on post-its all the apps, platforms and devices they used during the last week. Then the team used cards with different terms to see what children know, asking about “facial recognition”, “algorithms”, etc. This was followed by another activity to capture what kinds of data children share online and with whom. It is through these exercises that often the children realised how their practices feed into online advertising and corporate data collection practices. More on the methodology is available [here](#).
- Findings:
 - (1) How children engage online: the apps they use are mostly apps that adults use, they are not child-specific but common apps such as Spotify.
 - (2) What children (do not) know, and how they think, about data and privacy:
 - Children care about their privacy, contrary to what we often think.
 - “Private”, to them, means that friends cannot see what they post, but others (like companies) can. So, their idea of “private” is not really private.
 - The relation between privacy and data is not obvious to many children.
 - They feel puzzled as to why companies collect so much of their data.



- Even by the age of 16, only a few can map what happens beyond the screen, when it comes to our digital ecology.
 - They do not know what happens to their data once it is deleted.
 - Once they realise how their data is collected and used, they often shift to an outrage mode.
 - Children think “consent” should be something that they should be able to give. Instead, they feel that they do not have a choice.
- (3) How children construct their understanding of privacy and data, and how their understanding shapes their engagement:
- Children get their ideas about privacy from their personal circumstances (interpersonal privacy).
 - Trying to understand institutional and commercial privacy from understanding interpersonal privacy causes a lot of confusion. Children assume that companies would act as friends. Or they transfer their personal reactions by projecting them to the companies.
 - Children feel offended that companies keep so much data. They also think that nobody cares about what they share online, overlooking that their data is valuable to companies.
 - Children engage in privacy tactics as they would in interpersonal contexts when engaging with friends, using, for example, different names and expecting this to confuse their online profiling.

(4) From empowered to powerless children:

- Children feel confident that they are the pioneers of the digital world. They also use a very moral language to refer to what is offensive or appropriate about how their data is used.
- Once they feel outraged after realising what internet corporations do with their data, they feel powerless and describe the future in dystopian, Black Mirror-like, terms and emphasise that Mark Zuckerberg is always watching you.

(5) What children want:

- They want a lot of changes when it comes to the online services and platforms they use.
- They also want child-friendly Terms & Conditions, their accounts to be private by default, to be able to delete online content when they want.

(6) As for the teachers and parents who were interviewed:

- They have a sense that there is something at stake.
- Parents are full of questions and need support. They have questions, for instance, about how schools and companies are handling data. And they try to understand their own responsibilities.
- They do not know what happens with their children's data.
- Teachers, by contrast, are more pragmatic. They are interested in what works for teaching. They focus on safeguarding and are very trusting and hopeful that the school has everything under control.

(7) Recommendations:

- We need to find better ways to talk about different kinds of privacy
- We need child-rights-respecting policies
- We need to make sure that children can be taught better in school by placing more emphasis on digital literacy.

(8) Toolkit (available at www.myprivacy.uk):

- This was designed to improve 11-16-year-olds' understanding of their data and privacy online.
- It includes guidance and resources for parents and educators.
- It is an interactive toolkit that focuses on questions and activities around what data is, why we should care, what we mean by personal information online.

- It also has watch and play activities, and it has an international reach.

Points from the discussion

- What kind of schools did the team approach: diversity was aimed for in terms of location and socio-economic status. Socio-economic status was crucial in shaping what children know, and how they talk about, their data and privacy.
- Where does “institutional privacy” fit in their research: while a lot of children’s, parents’ and teacher’s concerns are about commercial privacy, there are a number of ways in which distinguishing between the three types of privacy is key. In terms of trust, there is a need for institutions to be trustworthy. If schools treated children’s data appropriately, they would set a good example. While there is a question of how and to what extent it may be possible to regulate global corporations, we can be more successful at regulating our public institutions.
- Thirteen is generally accepted by children as the appropriate age to use online platforms. There is support for stronger age verification enforcement.
- The idea of an age-appropriate design code is that it is primarily for children, but also adults would benefit from it, who do not necessarily know much more about data and privacy. If something works for children, it is likely to work for adults too.
- When we do not understand something, we need to have trusted sources where we can gather information. This is what prompted the team to develop an online toolkit.

Breakout session 1: Children’s data and privacy online – what the evidence tells us & what gaps matter

The attendees were asked to discuss in groups what evidence exists about children’s data and privacy, what gaps and questions need to be addressed and why they matter for different sectors. They were then asked to reconvene and share what they had discussed.

Questions that need to be addressed:

(1) Understanding and redesigning the digital environment

- How does data flow?
- How is trust on the internet found, lost and used?
- Is age verification advisable, considering that it requires users to share more data? Relatedly, what do we benefit and lose with age verification?
- How do we involve different stakeholders?

(2) Children

- How do children navigate contradictory messages and what is the state of their participation as citizens?
- When it comes to surveillance and safeguarding, what really needs to be protected?
- How can we effectively explain consent to children? How do we make sure that they give informed consent?
- What are the shifts in the general social norms that underpin how children engage online? What is acceptable or not to share?

(3) Education

- How are data and social media taught in school?
- What differences exist among teachers in terms of digital literacy and how confidently they use the internet?
- How do we navigate an increasingly complex educational matrix where the issues to tackle are being amplified by technology? How do we address knowledge and power asymmetries between tech corporations and lay publics?
- Do we need more interaction between children and schools' data protection officers?

Points from the discussion

- There is a disconnect between what parents and children know about their data.
- Children and parents often use terms interchangeably, so it is really hard to understand what they know.
- It is hard to find the right balance between protecting children, excepting them to participate in the digital environment and regulation.
- We need to make the legal language accessible and explain to children how their data is managed in ways that can be clearly understood.
- Cross-European research is needed.

Age appropriate design: A code of practice for online services (Elanor McCombe, Information Commissioner's Office)

Elanor McCombe is a Project Manager at the ICO, working on the development of [the Age-Appropriate Design Code](#). Her presentation covered the following points:

(1) Why the code is needed, and which companies will be affected:



- A code of practice for online services is needed because children are at the forefront in terms of using the internet. So, we want to make sure the internet is a safe place for them to explore. The code is not meant to not to put children off using the internet but to keep them safe.
 - Multiple online service providers are going to be affected by the code, with whom ICO is currently consulting.
 - The code affects all internet services that are likely to be accessed by children, including, for instance, apps, websites, connected toys, smart speakers, online games.
- (2) Links with the current legislation and how the code is being developed:
- If you are an online service provider and follow the code, you are compliant with the General Data Protection Regulation (GDPR). The code is rooted in the GDPR and the UK's Data Protection Act 2018, which is aligned with the GDPR. It also draws on the United Nations Convention on the Rights of the Child (UNCRC).

- It is a ground-breaking code. The UK is the first country to develop it.
 - To develop the code, ICO called for evidence and also commissioned a report from Revealing Reality to find out how children and parents understand privacy. They then developed a draft code and launched a consultation, which closed on 31 May 2019. Over 450 responses were received from individuals, tech multinationals and media organisations. The ICO is currently analysing the responses.
- (3) What is the code about: the draft code contains 16 standards. It aims to protect but also to empower children when it comes to their data. It is intended to maximise internet corporations' transparency, as to how they handle children's data and children's safety. The 16 standards in the code are as follows:
- Anything implemented and designed has to be in the best interest of the child
 - Age appropriate application – the standards of the code should be applied unless companies have robust age-verification mechanisms in place
 - Transparency – personal data should be processed in a transparent manner
 - Use of data that is detrimental to children must be avoided
 - Policies and community standards – Terms & Conditions and features to report, for instance, hate speech need to be prominent and child-friendly
 - Data minimisation, in line with the GDPR – online service providers must collect a minimum amount of data
 - Data sharing – there should be clarity as to where the data goes and whom it is shared with
 - Geolocation settings should be turned off by default and they should turn off automatically after using an app that requires them to be on
 - Parental controls – there should be clarity as to what parental controls are available and when they are on
 - Profiling – there should be clarity as to how children's data are profiled
 - Nudge techniques that encourage children to give out personal information or stay online longer should not be used
 - Connected toys and devices should include effective tools to make them compliant with the code
 - Default settings – privacy settings should be high by default and no incentives should be used to encourage children to lower their settings
 - Online tools should be provided to help children report concerns

- DPIAs (Data Protection Impact Assessments) – online service providers should identify, assess and mitigate the risks they pose to children, in line with the GDPR.
- Governance and accountability – there should be clarity as to what children can do if they are unhappy with how their data has been handled.

(4) ICO’s preliminary findings based on the responses to their consultation:

Top five positives about the code:

- It is principle-based
- It is based on safeguarding the best interests of the child
- It enables children to enjoy the online world while staying safe
- It encourages privacy by default
- It acknowledges different child developmental stages

Top five concerns:

- It will be expensive to implement, and it clashes with the business models of online services
- It will lead de facto to age verification by default, as it gives online service providers the option to choose between high privacy by default or robust age verification process, which is less expensive to implement
- It will lead to a disparity between UK and non-UK businesses
- ICO is overstepping its authority, as parents should be in charge of how their children use the internet
- The time for online service providers to make the necessary changes should be longer

Top five challenges:

- How will the code interact with other codes and standards?
- What is its definition of “child”? (How old? When should a child give consent?)
- What does “online services likely to be accessed by children” mean? Which online services are included?
- What does a “robust age verification process” look like?
- People need more examples to understand how the code works in practice.

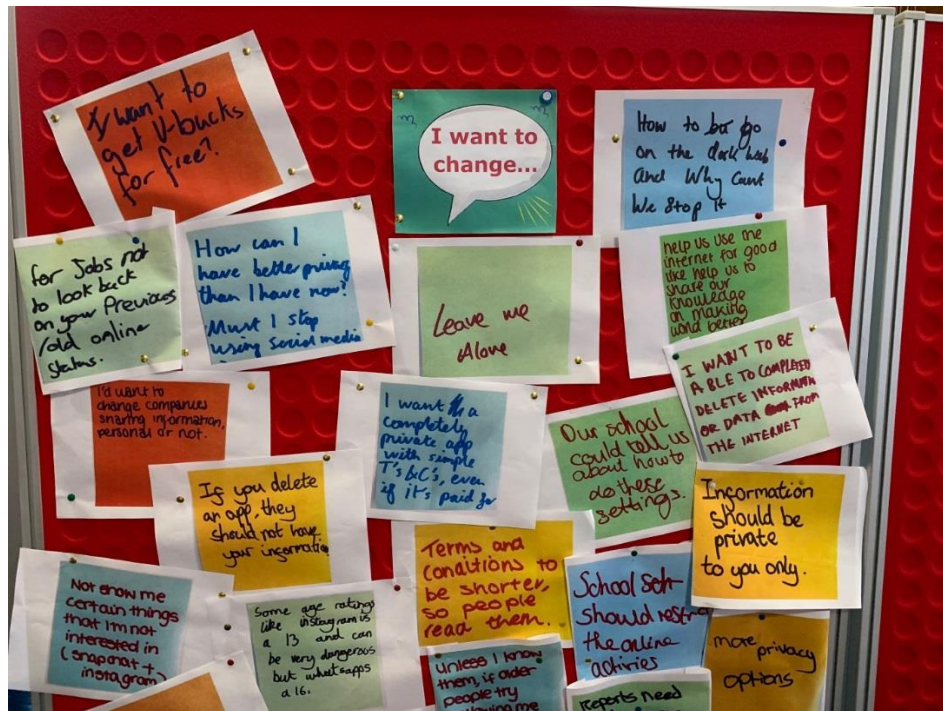
(5) Next steps:

- Once all the responses are analysed, ICO will redraft the code.
- It will publish the consultation responses and ICO responses.
- It will lay the code before Parliament.

Points from the discussion

- How is ICO going to enforce the code?: multiple methods, such as providing codes of conduct certifications and employing enforcement tools, from warning to imposing fines. There will also be a special directorate that deals with special investigations.
- How is help going to be provided to designers for them to understand what is in the best interest of children?: ICO is going to create some data protection examples that people can use. They will also provide briefing documents to their staff so that they can help designers and online services with tricky questions they might have.
- Can the code really deal with the dilemma that to protect their privacy users may need to share more data?: It is ultimately about transparency. Providers would be expected to be transparent about how they use their data while giving them the chance to opt in.
- There is an overlap between ICO's principles underpinning their age-appropriate code and the recently published [White Paper On Online Harms](#).
- ICO is currently discussing with the Department for Digital, Culture, Media and Sport (DCMS) how they could enforce the code outside the UK. A case-by-case approach would need to be taken.
- EU countries have shown interest in the code. And there is also interest from countries outside Europe. At the moment, these countries are waiting to see what happens in the UK with the code.

Lunch poster presentation: What do children want to change?



A new deal between children and the tech sector? (Jay Harman, 5Rights)

Jay Harman works for [5Rights](#), a charity which promotes children's rights in the digital age. His presentation covered the following points:

- 5Rights is interested in how digital design shapes children's experiences online. They believe that there are two things that need to change: a) children need to start being recognised by the online services they use, and b) children should be taken out of the business models of these services.
- The internet was created under principles of egalitarianism and libertarianism. But this means that children are treated like adults, and they can end up exposed, for instance, to inappropriate content, gambling, sexual activities. Online service providers should do a better job at ensuring that no children under the minimum age required to engage online use their services. But there are a lot of children that use social media who are under 13. We need to move meaningfully away from a digital environment where children are not recognised. But we also want to strive for a balance and ensure that protecting children does not mean that they benefit less from the opportunities that come with using the internet. The challenge is to figure out how to achieve such a balance.
- The business models of online service providers are based on keeping children online as long as possible. And they are intrinsically based on harvesting more and more data, making children inevitably subjected to possible harms. 5Right suggests that children should not be part of such business models and their privacy should not be traded as

part of commercial models. It should be recognised that children have rights. The White Paper on online harms does not emphasise that children have the right to be protected at any cost.

- We are faced therefore with a big challenge: to reimagine the digital environment. The question is: how much are we willing to change and demand that online services change? We need a systemic change, which is why 5Rights supports ICO. Their age-appropriate code is based on principles that are sound and desirable. At the same time, we need to be mindful not create too much disruption.

Points from the discussion

- What does it mean that children should benefit from the opportunities that come with using the internet while not paying the costs?: on social networks children should be able to interact and find information without having to surrender too much of their data. Removing children from the business models of online platforms does not mean that they would not be enjoying or using commercial services. It means that such services would not be driven by making money out of targeting children and using their data.
- Are children not already subject to offline advertising about junk food, for instance, which is in itself harmful? How is it different online?: we need to assess who is causing what type of harms and how particular business models are leading to such harms. But the problems we face offline should not discourage us from regulating the digital environment.
- Age verification and age-appropriate options are not impossible to implement successfully. They are safeguarding measures that should not be dismissed a priori. We need to question those companies that say that such measures are too clunky and expensive because it is not true.
- The problem with age-appropriate verification measures is trust. Users may simply be reluctant to give more information away for verification purposes.
- A company that is damaging the environment is not acceptable. Similarly, a company that harms children is not acceptable. But the question is: have we established precisely what harms exist online for children? Or do we need to establish first what rights need to be acknowledged and protected?
- If we know that something undermines children's rights, we should not be expected to do something to protect them only once we have provided evidence.
- We should give internet companies the time and support they need to make the necessary changes.

Breakout session 2: the way forward for children's data and privacy online: sharing the responsibilities among stakeholders – who should do what and how

The attendees were asked to discuss in groups what should be done when it comes to children's data and privacy online, who is responsible for what, who should be doing what, what are the other actors beyond ICO, and what they should be doing. They were then asked to reconvene and share what they had discussed:

The actors and responsibilities that were emphasised are as follows:

(1) The Government and public bodies:

- A multi-stakeholder approach is crucial, but the government (and the private sector) should bear more responsibility than other actors, such as parents.
- Other government departments should be involved, not just ICO.
- ICO should encourage and reward best practices. Sharing good examples is vital. Successful child safety measures online for ICO entail fewer complaints and enforcement action.
- The information has become a utility. We need universal technical standards for all online service providers to guide them to design their services and ensure that they are safe.
- We need to regulate internet corporations' nudge techniques.
- Digital literacy needs to be firmly embedded in the national curriculum.

(2) The private sector:

- Companies need to start brainstorming and considering alternative business models. There should be alternatives to the current tech monopoly. An alternative could be to ask users to use platforms for free and accept advertising or pay a subscription that involves no advertising. But this is rather elitist and could reinforce inequalities.
- Companies should think in advance about the risks that children could face when accessing their services.
- Even after Cambridge Analytica, there is still so much that we do not know about how our data is handled. Internet companies need to be more transparent and accountable.

(3) Academics:

- They need to identify what successful child safety measures online look like and what practices we do not want.

(4) The public (including parents and educators):

- Need to mobilise young people to join our efforts to change how internet companies operate.
- Parents and teachers have a responsibility to get children's attention and provide them with insights into how their data is used.

Panel discussion: “Challenges and solutions for children’s data and privacy online” with Victoria Betton (NHS), Jen Persson (Defenddigitalme), Liz Moorse (Association for Citizenship Teaching), Vicki Shotbolt (Parent Zone) and Sally Greig Lockwood (BBC)

Sally Greig Lockwood ([BBC](#)) focused on raising awareness and creating a dialogue:

- She showed a BBC video created to raise awareness among young people as to how their data is used, in relation, for instance, to facial recognition.
- She emphasised that the BBC has a duty to support children.
- She has worked on a project on child safety, and she is now working on a broader project on multiple areas concerning children's lives.
- Her job is not just about creating informative content that can reach children, but also to create a dialogue between industry and relevant stakeholders.

Victoria Betton ([NHS](#)): the role of clinicians

- The NHS has launched a new app called NHS Digital with age verification associated. It has also engaged with young people to create a website for mental health.
- Clinicians are mindful about the privacy risks that relate to children. Most of them, however, are not actively talking to young people about such risks, nor about the consequences of data sharing. Clinicians would not know how to proceed if they found something problematic.

Jen Persson ([Defenddigitalme](#)): schools and surveillance

- When it comes to the health system you can opt out and not share your data for commercial purposes. In education, we do not have that choice.
- Children are constantly monitored via CCTV, and their data is permanently stored in databases, with longitudinal records. They often need to use their fingerprints to access their school libraries. And they have personalised logins set up by their schools, and parents are not even informed before this happens. Everything children type when

using the digital devices provided by their schools is recorded for safety reasons. Schools do not know what to do with all this data. But if they delete it, they would not know how to protect them from potential risks.

- Parental consent needs to be addressed in education. Children's external emails can be accessed and shared with others, even when they are under the age of 13.

Vicki Shotbolt ([Parent Zone](#)): parents need support, but what about sharenting?

- Parents tend to lack confidence. We need to support parents in explaining to their children about their data and privacy. But as a society, we do not know enough.
- The practice of sharenting can also be problematic. Parents routinely share a huge amount of information about their children. Why do they do so? A small number of parents think that sharenting will boost their children's careers. While some young people wish their parents would stop sharing their photos, their parents just dismiss their concerns.

Liz Moore ([Association for Citizenship Teaching](#)): citizenship education as part of the solution

- The aim of her association has been to support high-quality citizenship education since 2002, which is when citizenship became part of the national curriculum. And it is also about helping teachers feel more confident when teaching students.
- When it comes to protecting children and equipping them with the knowledge they need in the digital age, education should be part of the solution. We need to approach digital citizenship and media literacy as central to citizenship education, which places emphasis on citizens' equality, rights, freedom, and how to discern facts from fiction.
- Unfortunately, citizenship is not always taught as not every school has to follow the national curriculum.

Points from the discussion

- Should the citizenship curriculum do a better job at teaching students about the broader digital environment? Also, should the notion of digital citizenship be approached as entailing more than teaching students what is acceptable in terms of online behaviour?: the national curriculum is a compromised document, which is very narrow and not conceptually articulated. It has to be translated by teachers, who work hard to give meaning to it. The Association for Citizenship Teaching runs a quality insurance process on their teaching resources. As for digital citizenship, it should entail more than teaching etiquette in the digital age. It should be about participating more actively in society and it is called digital citizenship because it places emphasis on aspects that are new and typical of the digital landscape.
- Are data and privacy topics that come up when speaking to children?: Not really. Their issues tend to be more personal and tangible, less abstract. Children do

not feel as passionately about privacy until they realise what happens with their data. E-safety and digital education have generally been more interested in the personal, but we have to start having more conversations about the implications of the digital environment when it comes to data and privacy.

- Any identity programmes that identify citizens will inevitably be used to censor and exclude. There are moves to match children's education data with their health data. But data has been misused by public bodies like the Home Office. There have been too many misuses for citizens to trust how the government holds their data. We need more transparency as to what data the government holds, how it uses it, and who it shares it with.

Final remarks (Sonia Livingstone, LSE)

- We need to listen to what children have to say: when designing the GDPR or the UK's Data Protection Act (2018), the voice of children was not included. But it is important to listen to them in ways that can inform how policy should be designed and implemented.
- Many questions remain: on the one hand, there are big questions that we need to keep addressing (e.g., What is harm? Where does all the data go in today's complex data ecology?). On the other hand, there are many practical questions (How does this or that app protect privacy? Can age-verification work?). But we need to ask ourselves: what are we going to do once we know what children understand and want to know? How will things change if people become more media literate? Will this alter the balance of responsibilities among educators, government and industry?
- This seminar event was fruitful for making connections when talking about data protection and online harms in ways that are thought-provoking and challenging.
- We have answered some questions and identified yet others: Do we want regulation for children or for everybody? How will the market innovate once the Code is in force? Will internet companies adjust their services? Will there be new market solutions? We are on the brink of something unknown.
- Moving forward: it is inspiring that ICO's age-appropriate code is based on the UNCRC. When thinking about solutions, we need to recognise the diversity that exists in terms of families and contexts. Hopefully, the market will innovate to do better on transparency and data protection. Hopefully, children and everybody else will be provided with real alternatives. For now, there are no real options to "giving consent" when using online platforms, as the only alternative is to be excluded from the world.
- Trust and shared responsibility: there are different stakeholders involved when it comes to protecting children's rights in the context of their data and privacy. It is not easy to find answers, but it is crucial to have conversations with all the actors involved. And it is crucial to share responsibility.

- The role of media: a lot of the media debate is focused on the platforms. But we also need to think about the role and responsibility of traditional media, parents and educators. And we need to address the question of whether citizens trust the state with their data.
- We need different areas of expertise to reach different actors, from the government to teacher trainers, from those who debate what platforms are acceptable to those who design them, from broadcasters to the public.

Appendix 1: Seminar agenda

9.30 – 10.00	Arrival, coffee & poster discussion: 'What do children want to know about privacy'
10.00 – 11.00	Children's data and privacy online: it's neither personal, nor private Launch of new findings and privacy toolkit (including Q&A) <i>Sonia Livingstone, Mariya Stoilova, Rishita Nandagiri (LSE)</i>
11.00 – 12.00	Breakout session, <i>chair: Helen Kennedy (University of Sheffield)</i> Children's data and privacy online – what the evidence tells us & what gaps matter
12.00 – 12.45	Outcomes from the Age appropriate design code consultation and the way forward for the Draft code of practice for online services (including Q&A) <i>Elanor McCombe (ICO), chair: Emma Goodman (LSE)</i>
12.45 – 13.45	Lunch & poster discussion: 'What do children want to change'
13.45 – 14.30	"A new deal between children and the tech sector?" (including Q&A) <i>Jay Harman (5Rights), respondent: Simone van der Hof (University of Leiden), chair: Leo Ratledge (CRIN)</i>
14.30 – 15.30	Breakout session, <i>chair: Rishita Nandagiri (LSE)</i> The way forward for children's data and privacy online: sharing the responsibilities among stakeholders – who should do what and how
15.30 – 15.45	Coffee break
15.45 – 16.45	Panel discussion: Challenges and solutions for children's data and privacy online (including Q&A) <i>Victoria Betton (NHS), Jen Persson (Defenddigitalme), Liz Moorse (Association for Citizenship Teaching), Vicki Shotbolt (Parent Zone), Sally Greig Lockwood (BBC), chair: Ioanna Noulas (LSE)</i>
16.45 – 17.00	Seminar summary and recommendations <i>Sonia Livingstone (LSE)</i>
17.00	Reception Fields Bar & Kitchen , Lincolns Inn Fields, WC2A 3LJ

Project info at <http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline>

Appendix 2: List of attendees

Bojana	Bellamy	Centre for Information Policy Leadership
Victoria	Betton	Leeds and York Partnership NHS Foundation Trust
Jane	Bürger	
John	Carr	Children's Charities' Coalition on Internet Safety
Laura	Clarke	NSPCC
Natalia	Clifford	
Charlie	Cock	Internet Matters
Stephanie	Comey	Broadcasting Authority of Ireland
Natasha	Connors	Ofcom
Jutta	Croll	Stiftung Digitale Chancen
Julie	Dawson	Yoti
Moushami	Debnath	
Hannah	Ditchfield	University of Sheffield
Sarah	Doherty	eNurture
Maria	Donde	Ofcom
Roland	Earl	British Toy and Hobby Association (BTHA)
Patrick	Forman	Privacy Lawyer at BT plc
Sally	Greig Lockwood	BBC
Louise	Golding-Hann	Head of eLearning at Forest School
Karolina	Gombert	Children's Commissioner
Emma	Goodman	LSE
Malgorzata	Hardie	
Jay	Harman	5 rights
Kate	Jones	Childnet
Helen	Kennedy	University of Sheffield
Theo	Knott	British Computer Society
Ansgar	Koene	University of Nottingham
Jie-min	Lee	UCL
Sophie-Charlotte	Lemmer	King's College London
Claire	Levens	Internet Matters
Sonia	Livingstone	LSE
Cliff	Manning	Parent Zone
Elanor	McCombe	Information Commissioner's Office
Robert	McCombe	Information Commissioner's Office
Liz	Moorse	Association for Citizenship Teaching
Victoria	Nash	Oxford Internet Institute
Rishita	Nandagiri	LSE
Nóra	Ni Loideain	Institute of Advanced Legal Studies
Ioanna	Noula	University of Leeds
Louise	O Hagan	Cyber Safe Ireland
Tunde	Olatunji	
Derek	Palmer	Live Nation Entertainment
Jen	Persson	Defenddigitalme

Gianfranco	Polizzi	LSE
Alison	Preston	Ofcom
Leo	Ratledge	Child Rights International Network
Ralph	Rogobete	GSMA
Ravinder	Roopra	Saltridge
Renate	Samson	Open Data Institute
Chia	Seiler	Ofcom
Julia	Senior-Soule	Hunton Andrews Kurth LLP
Amy	Shepherd	Open Rights Group
Vicki	Shotbolt	Parent Zone
Mariya	Stoilova	LSE
Zoetanya	Sujon	University of Arts London
Bhagyashree	Swami	
Mimi	Tatlow-Golden	The Open University
Jimmy	Tang	Google
Yu-chen	Tao	UCL
Bridget	Treacy	Hunton Andrews Kurth LLP
Simone	van der Hof	University of Leiden
Simone	Vibert	Children's Commissioner's Office
Jenna	Wall	Common Sense Media
Ge	Wang	University College London
Helena	Webb	Department of Computer Science, University of Oxford
David	Wright	South West Grid for Learning
Rui-feng	Xu	King's College London
Jun	Yu	LSE
Ssu-Han	Yu	LSE
Frauke	Zeller	Ryerson University
Jun	Zhao	University of Oxford

Appendix 3: 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.'](#) The 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.

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Search Menu

My Privacy UKFor parentsFor educatorsFor policy makersAbout

My privacy



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









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.