LSE MEDIA POLICY PROJECT
Promoting media policy communication between academics, civil society & policymakers

ico. Grant Recipient

Regulating children's data and privacy online:
The implications of the evidence for age-appropriate design

London School of Economics and Political Science (LSE)

This report is a brief summary of the public meeting on *Regulating children's data and privacy online: the implications of the evidence for age-appropriate design* held at the London School of Economics and Political Science (LSE, 7th September 2018).

The ICO consultation on the age-appropriate design code

1. Lisa Atkinson (ICO) kicked off the meeting, emphasizing that this is the beginning of long discussion. She gave an overview of:
    - ○ The context and wider frame in which the Code is to be set;
    - ○ ICO's overall vision for the Code;
    - ○ The plan for developing the Code

    a) General concerns about children's privacy have been mounting over children's uses of websites, the over-collection of their data, and disclosure of their data to third parties, and the vagueness of language used in addressing children (Terms & Conditions, etc.), among others.

    b) ICO aims to help create a better and safer (online) environment for children (in the UK) in order for them to engage and safety develop citizenship of future.

    c) ICO is committed to producing the Code that specifies what online service providers to do and NOT to do, providing "practical" guideline for the providers to use. The Code should be "used, not sitting on the shelf". It will not be a standalone application but should fit a "wider jigsaw" that concerns children's online safety.

    d) ICO has devised the current age bracket (3-5; 6-9; 10-12; 13-15; 16-17) tentatively, based on that children have different needs at different ages, but is consulting on how this difference will actually map onto the service providers' dealing with each age group. ICO therefore hopes to hear from the meeting and further research.

To respond to the Call for evidence - Age Appropriate Design Code visit: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-evidence-age-appropriate-design-code/

2. In the second section, Sonia Livingstone (LSE) and Mariya Stoilova (LSE) shifted the focus from regulatory discussions to the *direct research with children*, through their project that started in April 2018 to provide evidence on children's understanding of privacy, media skills, and vulnerabilities online. The key is to understand the online context *from children's perspective* in order to identify any significant gaps in knowledge about children's online privacy and commercial use of data, and clarify future lessons for policy practice *informed by the children's view*.

    a) Based on a literature review (131 empirical studies, 266 framing studies), the project conceptualizes privacy as, in line with Helen Nissenbaum, "the right to appropriate flow of information" rather than about secrecy or control.

b) As the literature is revealing (work still in progress), developing a privacy-friendly online environment can be demanding because:
   - (i) Online platforms provide opportunities for development, but at the same time introduce and amplify risks.
   - (ii) Over-protection may hinder free expression of children.
   - (iii) At different ages children have different needs, and their understanding of privacy (distinguishing "interpersonal privacy", "institutional privacy", and "commercial privacy") becomes more complex over time – hence the need for an age-appropriate design.

c) Evidences from research to contribute to the consultation:
   - (i) Children are "naïve experts", who care about privacy and know how to deploy privacy protection strategies, but lack awareness of consequences. Privacy concerns, therefore, do not always trigger protective behaviours when there are compensatory benefits (e.g. socializing with friends), or when they have a sense of control over information and higher trust towards audiences and/or platforms.
   - (ii) Controlling parents have suppressive effect, as it reduces privacy risks but also child development by decreasing the frequency of internet use, digital skills and online opportunities. Also, a parent-centred approach may create a sense of privileges (e.g. against those who have no parents).
   - (iii) Children's needs and level of understanding of risks vary for different age groups to groups (e.g. 8-11-year-olds see monitoring more favourably than 12-17-year-olds who develop a sense of 'personal space'). They, thus, show different privacy concerns and online behaviours.

d) Main challenges identified
   - (i) Children's incapacity to fully understand and consent
   - (ii) Children's understanding of privacy and risks differs from that of adults
   - (iii) Online environment can incentivize self-disclosure and so prevent privacy protection
   - (iv) Long-term implications are hard to predict
   - (v) Different degrees of vulnerabilities among children, and their exclusion from decision-making processes.

e) Recommendations based on the evidence include the following:
   - (i) Age-appropriate approach to data/privacy online
   - (ii) Balance between protection and autonomy
   - (iii) Media literacy and privacy education at an early age
   - (iv) Focus on individual differences and psychological factors
   - (v) Support children by supporting adults
   - (vi) Improve the privacy affordances of the online environment
   - (vii) NO discrimination based on personal data
   - (viii) Better evidence-base, including children's vote

The slides from this presentation are available here: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Children's-data-and-privacy-online-exploring-the-evidence.pdf
Further information about the project is available here:
http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

3. After the open discussion and coffee break, Beeban Kidron (5 Rights) began the third section by pointing out the vision of the early inventors of the internet, was to "democratizing technology, no gatekeepers, and **all users are equal**". As she observed, if all users are equal, that means children will be (inappropriately) treated as adults. Hence the need for the age-appropriate Code.

a) The Code should focus on the "systemic re-design" of online environment in which children are treated fairly, thereby beginning to "retro-fit 150-years of societal knowledge, norms and values into the design of the digital environment so as to respect and value children's rights and wellbeing. The Code could and should achieve this by:

   (i) Moving responsibilities (to manage privacy and personal data) from children/parents/teachers to online service providers. It is not acceptable to expect children to understand the complex digital environment, or to expect them to be resilient in the face of systematic abuse (or, at best, indifference).

   (ii) Making "default" better (because very few people change the default options provided): many do not change the default privacy settings.

b) The Code is mandated by section 123 of the Data Protection Act. In developing it, it is important to be clear also about what the Code can't do. It is not about regulating safety or harmful contents, but more about building "a proper data protection regime". By having this regime, contents are expected to change. The code must also be proportionate, and useful. To build this regime, some suggestions and examples are made:

   (i) Online service providers **must be required to show** how they take the best interests of children into account (e.g. under what circumstance can sharing personal data be the best interest of a child?). Even from an economic perspective, 1/3 people on the internet are under 18 and that is a huge market whose interests are a commercial proposition on their own.

   (ii) Automated data collection, such as collection of geo-location, should be turned off by default –for children under 18

   (iii) Industry must work together to make data collection and privacy protection look familiar to people, without them having to read terms and conditions to understand the general settings (especially important for children who have little awareness of the consequences of data sharing). This does not mean abandoning each company's own branding or strategies, but it is about establishing a "labeling infrastructure" (like traffic signals) that indicates the level of privacy on offer and provides proper environment online for children.

   (iv) "Rights by design" is vital – so a child could check, contest, rectify, erase, or edit information about themselves - similar systems exist for editing profiles and or inferences (such as Google's ad management page).

   (v) Child and data impact assessment required, but currently children are also creating the assessment on their own (to include their voice).

   (vi) The list of design features identified in the consultation document should be considered seriously, asking the question – what does a child need online? An argument can be made for the highest privacy settings by default, collecting personal data only for a good reason, upholding terms and conditions.

   (vii) It is significant and should be commended that the Data Protection Act explicitly mentions the UNCRC, especially the importance of ensuring the best interests of all children under 18 years old. The best interest of children should be the key question to answer in any systematic design of services.

   (viii) The principle of data minimalisation is crucial. Data must be service-critical, and that does not include sharing with third parties.

(ix) Should be provision for collective redress, so that each child need not make his or her own individual complaint

(x) How far can the Code be made future-proof? By setting expectations.

4. Elvira Perez Vallejos (University of Nottingham) wrapped up the meeting by providing a brief summary, re-stressing the significance of focusing on renewing the relationship with technology.

Key ideas and concerns emerged

1. GDPR-related

a) What is the relation between the Code and its relationship to the Article 8 of the GDPR. The Code provides another "layer of details" of what to comply with the GDPR requirements, and it has a wider application than the Article 8. The Code could also be used in terms of enforcement.

b) It was noted that health data has a special status and treatment in the GDPR as a sensitive data. Will there be other different/special/sensitive categories of data in the Code, would go beyond the remit of GDPR?

c) Related to the point above, what about the status of physical location in the Code? In the Article 9 of GDPR, location is not treated sensitive data (although mentioned in the recital). But in French case, the GDPR and the French Code apply to children with French passport/citizenship regardless of their current location. Can the ICO treat children's location data as sensitive, regardless of their use within or outside the UK? This is a way for the Code to make difference from the GDPR.

d) It was asked how the UK legislation would apply to all British children whatever websites they access and wherever they are physically located. The Code is a domestic legislation and UK regulator is applying the Code, so people using UK services are also expected to follow the Code.

e) The right to be forgotten is crucial, but do children understand right? It is also part of the GDPR (as the right to erasure), but the Code will be more focused on children's right (to be forgotten).

2. Remit of the Code

a) Age verification will be included in the Code but often this is designed to "restrict the access of children", whereas ICO's main focus is not so much keeping children out as "creating suitable environment". The aim is thus more about the overall design of online environment rather than single regulatory measures.

b) Question was raised regarding the potentially international reach of the Code, and about whether there has been consultation between ICO and the rest of the world. The conversation is ongoing internationally and it will be interesting to develop an internationally common code. Several jurisdictions are showing interest and children's privacy is being talked about, but the discussion has just begun, and it will require global data regulator meetings.

c) Is there a call for privacy ratings and would people understand this? What matters is to have certain standard against which principles can be established.

d) Should the focus remain on designing for children, instead of for everyone?

3. <u>Location of responsibility</u>

a) The code applies to all online services even when children are not their target audiences. Also added was that it is unfair that children have no power and no real choice but still bear the responsibility to manage privacy, and therefore this responsibility should be assigned to companies instead. By the same token, child protection by parents is not enough, not because this is negative, but because children themselves should also know what is happening to them.

b) Question was raised about the sense of ambiguity in the "intent" of access and data collection. For instance, apps (e.g. camera) ask for user's permission and notify that they will remember user's "choice" and will have access to certain set of data, but they don't specify the "intent" behind these actions, partly removing capabilities of users here. The words "choice" or "transparency" are often too ambiguous, and such intent of data collection *must be* aligned with the best interest of children.

4. Categorization of data, privacy, and media education

a) Does the distinction between interpersonal, institutional and commercial privacy work? And where do responsibilities lie for each? The idea of "data-given" should be separated into two categories: "data-given *freely*" and "data-given *because you have no other option*". This could be complicated, e.g. what if children want to give data because they want to play games with friends? Is this voluntary, compulsory? Perhaps the term "data-taken" is preferable, in contrast to "data-given", depending on the meaningful action that underlies data sharing by children.

b) Question about ethics of education was raised. If it is children who teach adults today how to use media, then do we need to *lie* to provide guidance? Framing adults as having little competency and experience can be problematic. Placing too much stress on media literacy may be problematic, since technology is too complex and fast-changing that nobody can fully understand it. What kind of media literacy campaign should be done?

5. Informing age brackets

a) Age may not be the most helpful paradigm vis-à-vis other variables such as gender. The starting point is that *fundamentally* children are under 18 and we add further nuance to it by bringing in other variables.

b) Question about age-appropriateness was raised. As the discussion went on, age ranges seem more fluid rather than fixed, and the fast-developing new technologies may mean the meaning of age-appropriate design for older groups might vary. So, having an age-appropriate design *now* and take it to the following years could be problematic.

Resources and suggestions of action/ideas

1. Research with children and also with parents required. The ICO will be commissioning this.

2. “Deceived by design” (https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf). A report by Norwegian Consumer Council on how big tech companies employ psychologists to design an environment that “hooks-up” children, in order to generate inflow and profits.

3. The new “Nurture network” has just been funded by government to focus on a better design for mental health and well-being of children in three different contexts: peer-to-peer; school; family.

4. Language consistency is essential across different laws, e.g. meaning of age, criteria for age group, age as starting-point, etc. should be regarded consistently, because it will be the general frame for practicalities. ICO should take this into account.

5. It was noted that having the age group of 12-14-year-old is crucial, because children reach puberty in that period. Relatedly, it was mentioned that there are currently not many studies with developmental approaches and more talk with children is required.

6. It was suggested we think too much of privacy as an individual matter but not as social contact, e.g. what if friends (not just platforms) post your stupid photos? In other words, people should care about “other’s privacy”.

7. The concept of “right to make mistake” is suggested, as it is crucial to think of children as explorers who lack some fear of consequences, and who are better than parents in bypassing the controls.

8. It was cautiously proposed that it *is* technology that could/should be the driving factor informing the new taxonomy of the Code, e.g. considering big data development that do not target each child but “particular groups” of children based on data collected.

9. In relation to the context of design concept, “dark patterns” and “good patterns” of online use should be distinguished and called out (e.g. related to the “Deceived by Design” where environment can be designed to encourage certain things).

You can access 5Rights submission to the ICO here:
https://d1qmdf3vop2l07.cloudfront.net/eggplant-cherry.cloudvent.net/compressed/c1b7f20a4609b9c963ae78889b780a23.pdf

Challenges expected

1. Difference across different ages is enormous, but it takes a long time to figure out what appropriate age ranges are, e.g. how do they learn, and where do they learn about things.

2. Children are not always using words in practical sense, e.g. they say “hackers” but without knowing what that really means or who they are. Should adults fill this knowledge gap and make children understand this? Danger is in misinterpreting what the real crisis *is*.

3. Industry opposition to offering better services to children.

Appendix 1

Regulating children's data and privacy online: The implications of the evidence for age-appropriate design

12.30 – 5pm, Friday 7th September 2018
London School of Economics and Political Science (LSE)

Agenda

12.30 – 1.00 Arrival

1.00 – 1.10 Welcome and introductions.
Prof Sonia Livingstone OBE (LSE)

1.10 – 1.40 The Information Commissioner's call for evidence and consultation on an Age-Appropriate Design Code: context and aims (including Q&A)
Lisa Atkinson (ICO)

1.40 – 2.10 Children's data and privacy online: the evidence so far (including Q&A)
Dr Mariya Stoilova (LSE)

2.10 – 3.10 Regulating children's privacy online: open discussion about the available evidence and its implications for the code
All participants, chaired by Prof Sonia Livingstone OBE (LSE)

3.10 – 3.30 Coffee break

3.30 – 4.30 Age-appropriate design code: 5Rights recommendations (including Q&A)
Baroness Beeban Kidron OBE (UK House of Lords, 5Rights)

4.30 – 5.00 Summary and recommendations: *Assoc Prof Elvira Perez Vallejos (University of Nottingham)*

5.00 Close