Horizon Digital Economy Research, University of Nottingham – written evidence (CHI0032)

Submitted by Dr. Ansgar Koene, Prof. Derek McAuley, and Dr. Elvira Perez Vallejos, Horizon Digital Economy Research Institute, University of Nottingham

1. Horizon[1] is a Research Institute at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley is Director of Horizon and was principal investigator on the ESRC funded CaSMa[3] project (Citizen-centric approaches to Social Media analysis) within Horizon to promote ways for individuals to control their data and their desired level of privacy. Dr. Perez and Dr. Koene conducted research as part of the CaSMa project. An important part of this work has included the facilitation of 'youth juries' - workshops with 13-17 year old youths designed to identify experiences, concerns and recommendations about the internet. A pre-print draft of the report summarizing the outcomes of the youth juries process is available from the CaSMa website[4]. This work was done in collaboration with the 5Rights[5] coalition and Prof. Stephen Coleman from the University of Leeds.

Questions

1. What risks and benefits does increased internet usage present to children, with particular regard to: … iii. Data security

2. Data security for children revolves primarily around preventing the undesired dissemination of personal (or otherwise personally valued) data to third-parties by actors with whom the data was voluntarily shared, whether explicitly (e.g. social media platforms), or implicitly (e.g. by search engines or web trackers).

3. A recurring issue that was raised by the children during the youth jury deliberations was the way in which Internet users are invited to consent to having their data stored. As one juror put it: "It's the way it's like marketised; it's so friendly and appealing. It's like, 'Enable cookies'. It's like, you wouldn't reject a cookie because a cookie is … a nice thing to have."[6]

4. In all of the juries, discussion moved at some point from third-party data collection to the 'terms and conditions' (T&Cs) that people are required to sign up to when entering commercial sites. The general attitude on this topic is clearly expressed in the following quotes by two of the young participants. The first expressing the difficulty of understand the T&Cs "The companies are really smart, because they know most young people don't want to sit there reading, like, paragraphs and paragraphs about it. And even if you did the way it's worded it's complicated so they know people won't understand it". The second highlighting the sense of being manipulated and exploited "And so I think things like that are quite interesting, because it's like, then they, they ... they're backing themselves up and saying, "Well, it was stated in the terms and conditions which you

agreed that you'd read," and it's like really they know that, that no one would read it. So I think that's when they can use it against us."[6]

5. It is worth bearing in mind that the problems with the comprehensibility of 'terms and conditions' are an issue that applies equally to adults, as was shown by a previous study from our lab[7].

6. Among the recommendations from the young people for solving these issues were demands for clearer and more accessible presentation including video and audio formats, as well as fines for platforms that do not comply with minimum requirements such as word limits, clarity, or accessibility. Specific recommendations include more transparency regarding third party data-gathering and storage, for example: users should be informed and their explicit consent should be required for their personal data to be used, shared or tracked; the length of time personal data is stored should be limited; there should be an award for best practice in personal data sharing and protection of user's privacy.

7. Youth Juries participants also pointed out that removing personal online content should be easier and suggested a self-tracking tool to gain control over their own content, as well as screenshot blocking tools.

2. Which platforms and sites are most popular among children and how do young people use them? Many of the online services used by children are not specifically designed for children. What problems does this present?

8. The popularity of sites among children can change rapidly when new services are offered. A clear example of this is the PokemonGo app which is currently very popular but could quickly loose popularity once the novelty of the experience wears off and a new competing app is launched. Based on discussions with parents and with the youth jury participants, sites that have managed to maintain popularity for a prolonged period are:

- Popular sites with young (pre-teen) kids: Swiggle, YouTube, CBeebies
- Popular sites with young teens: Facebook, SnapChat, Instagram, Whatsapp, Tumblr

Among these, only Swiggle and CBeebies are specifically designed for children.

9. A 2012 report by MinorMonitor[8] surveyed 1000 parents of children under 18 who used Facebook. More than 38% of the children were found to be 12 years or younger and 40 children were reported to be 6 years old or younger.

10. A 2011 study by Dana Boyd and colleagues[9] in the US investigating the efficacy of the Children's Online Privacy Protection Act (COPPA), which regulated the use of commercial Web sites by children under 13, found that 84 percent of parents were aware when their under 13 years old child first created their site account, and 64 percent helped create the account.

11. Exposure of children on and to online platforms and sites commonly start much earlier than their first personal accounts. According to a 2010 study by internet security firm AVG, 92% of children in the United States have an online presence (due to their parents' disclosure) by the time they are two years old.

12. Some service providers, like Microsoft and Apple, have introduced 'family accounts' or 'family sharing' as a way to allow children under 13 to create an account ID that will provide access to approved services and give parents greater abilities to monitor their child's activities online. An example application for this is video chat where the family account can allow the child to call family members but not be exposed to strangers.

13. The most frequently encountered problems that arise from the use of platforms that were not specifically designed for children is inadvertent exposure to material that is targeted at adults, for example through advertising on the site or automatically generated recommendations, such as on YouTube. For example, a 2015 study by A.E. Barry and colleagues[10] revealed that Instagram accounts that were set up with profiles of fictitious users with ages 13 to 19 were able to follow alcohol brands and received an average of 362 advertisements within 30 days.

3. What are the technical challenges for introducing greater control on internet usage by children?

14. One method for providing greater control on internet usage by children is to use filtering software, such as NetNanny, or 'safe' settings such as the 'SafeSearch' setting that is available in most popular web-browsers. Some browsers, like DuckDuckGo have opted to have SafeSearch on as default. Others like Google require users to access a settings menu to turn in on, with an option to lock the on setting that can only be reached ***by logging in to a google account*** and hence submitting to further tracking. Bing uses a filtering model with three setting where the default 'moderate' setting blocks adult images and video but not text from search results. Various Internet Service Providers (ISPs), also provide filtering services that allow parent to centrally set Child Safe filters that apply to all devices that connect through the home internet connection.
15. Most filtering services rely on either blacklisting or whitelisting of internet content. In the case of Blacklisting all content/pages are accessible except those that have been explicitly listed as unsuitable. In the case of Whitelisting everything that hasn't been listed as suitable is blocked. Both typically rely on humans to view and evaluate the content in order to populate the filtering lists; contracting such work can be costly at large scale.

16. However, even with the most carefully curated Whitelisting based filtering, in-site linked advertising can still cause problems because the advertising content hosted on websites is usually under the control of an ad delivery service, like AdSense, which run real time auctions to determine which advert to show. Various ad delivery services do include customization options that allow the site owners to tune the type of ads they allow on their site, but often these setting are not used or fail to match the age appropriateness of the whitelisted site content.

17. An important factor that needs to be taken into account is that there are discrepancies between PC and mobile platforms. Whitelist tools are often not available for mobile platforms, only for PC. Furthermore, when parents decide to use a Child Safe filter service from their ISP the filter will only apply to the smart phone of the child if it is connecting to internet via the home WiFi, not when the child is connecting via the mobile network. Since the way in which the device is connecting to the internet does not significantly change its user experience, parents might easily not be aware of this distinction.

4. What are the potential future harms and benefits to children from emerging technology, such as AI, Machine Learning and the Internet of Things?

18. The flow of information on social network sites is increasingly mediated by filtering and recommendation algorithms that select and rank the messages and news items presented to users, including children. Although critical in shaping the experience of social media, these algorithms and their effects remain opaque to users. This lack of transparency has the potential to be abused for censorship or manipulation purposes. Without transparency it is very difficult to identify what kind of bias these systems put on the information flows that children are exposed to. Furthermore, the increasingly smooth interfaces and high rates of success in producing satisfying results can lead to an uncritical acceptance of the information that is given.

19. If current trends continue, the Internet of Things is likely to become one of the largest problem areas for cybersecurity and for privacy. Far too often security and privacy concerns are given too low a priority in the design process, resulting in easily hackable IoT devices. Particularly concerning are the examples, including connected baby monitors, voice controlled TVs and toy dolls (e.g. Hello Barbie), that continuously stream very personal video and audio information to data centres, often outside of the jurisdiction of the UK (and EU) data controllers.

Education

5. What roles can schools play in educating and supporting children in relation to the internet? What guidance is provided about the internet to schools and teachers? Is guidance consistently adopted and are there any gaps?

20. Internet advice courses for parents provided by schools or external organisations via the school (e.g., NCPCC or Internet Matters) are reported by parents as very repetitive and lacking in interaction and engagement elements. Funding for quality educational, even online, materials should be a priority building on leading activities such as 5Rightsframework.com.

21. The advice that the schools deliver to parents should be tuned to the age of their children and the changing internet usage patterns for the different age groups. Currently the focus of the guidance is mostly on the risks of internet usage. This needs to be balanced more with guidance about the opportunities that the digital world can offer when services and apps are appropriately configured and used.

6. Who currently informs parents of risks? What is the role for commercial organisations to teach e-safety to parents? How could parents be better informed about risks?

22. Parental guidance comes primarily from schools. Some commercial organizations provide very short bullet lists of safety information, usually in the context of advertising Child Safe 'whitelisting' or 'safe search' services (e.g. BT, Virgin Media).

23. Organizations like Mozilla and Guardian have run campaigns to raise awareness of online safety. These campaigns however were targeted at adults and did not deal with child specific issues. There is a need for better awareness raising/improving internet literacy interventions for both parents and young people. These are contemporary societal issues that could be addressed through well considered plot lines in popular TV drama.

24. Participants of our Youth Juries suggested the creation of peer-group advice services to support both parents and children with practical advice based on personal experiences.

Governance

7. What are the challenges for media companies in providing services that take account of children? How do content providers differentiate their services for children, for example in respect of design?

25. A complicating issue arising is one of definition and appropriate regulation. The recent House of Lords inquiry into Online Platforms[11] and continuing EU activities highlight the complexity of categorization of platforms.

26. For example, social media sites rely on protections afforded to communications service providers and prefer not to moderate content in advance, but rely on take down requests for illegal or inappropriate content. Some do provide the means to label content as "adult", which is a somewhat blunt distinction – in film, TV and computer gaming[12], age labelling and controls are more nuanced and online service providers could quite simply provide similar content labelling schemes – even better if adopted globally as international standards. In combination with aforementioned "family account" mechanisms, these could bring much greater control to families.

8. What voluntary measures have already been put in place by providers of content to protect children? Are these sufficient? If not, what more could be done? Are company guidelines about child safety and rights accessible to parents and other users?

27. Examples of services that provide good information to parents about child safety and access rights include platforms dedicated to promoting wellbeing and mental health

among children and young people including Kooth, Elefriends and YoungMinds (e.g., digital resilience section), which is only right given the very sensitive nature of challenges these services deal in.

28. User generated content sites like YouTube could adopt a policy of marking all content by default 'adult only', with users posting content able to suggest a lower age rating for content that is supposed to be child friendly. Other adult users could be requested to confirm or deny whether the rating is appropriate having watched the content – such a "crowdsourcing" mechanism can address the scaling issues of content rating, while having as a backstop the ability to refer the content to the site hosting service – invoking the current process for dealing with inappropriate content. Again a common international framework and ratings scheme broadly adopted would work best.

Legislation and Regulation

9. What are the regulatory frameworks in different media? Is current legislation adequate in the area of child protection online? Is the law routinely enforced across different media? What, if any, are the gaps? What impact does the legislation and regulation have on the way children and young people experience and use the internet? Should there by a more consistent approach?

29. Specific consumer protection concerns arise in dealing with unbounded "in-game" purchases. Certainly for children controls need to be in place to prevent excessive charging. Given the child is not the bill payer, it could be viewed as negligence on the part of the service provider to not provide the bill payer with the controls necessary to cap such payments, something the credit card industry could champion backed by the threat to refuse to honour payments.

10. What challenges face the development and application of effective legislation? In particular in relation to the use of national laws in an international/cross-national context and the constantly changing nature and availability of internet sites and digital technologies? To what extent can legislation anticipate and manage future risks?

30. International coordinated regulation is required in order to have impact, and specifically on large US corporations which have emerged within the US's specific regulatory framework. In this regard the EU has been an important player, where the UK will be a minor voice unless it continues to coordinate and support EU action in this area.

11. Does the upcoming GDPR take sufficient account of the needs of children? As the UK leaves the EU, what provisions of the Regulation or other Directives should it seek to retain, or continue to implement, with specific regard to children? Should any other legislation be introduced?

31. Several of the suggestions that were made by our youth participants would fit within a rigorous implementation of the impending EU General Data Protection Regulation by the Information Commissioners, bearing in mind the needs of children.

32. Many commentators assume that the GDPR will in fact come into force given the timeline for the UK departure from the EU. Whether the UK would then decide to replace it would beg the question "what could be achieved by doing that?". As we have seen with the overturn of the US "Safe Harbour" and the immediate challenging of the new "Privacy Shield", any UK regulation would need to provide rights on a par with GDPR to maintain effective trade with the EU in digital services, and enable UK companies to export effectively.

12. What more could be done by the Government? Could there be a more joined-up approach involving the collaboration of the Government with research, civil society and commerce?

33. Civil society needs to be consulted at early stages of any legislative process, including not only child protection but also those concerned with freedom of speech, freedom of access to information and privacy advocacy groups, in order to provide balanced perspective. The approach adopted in the definition of the gov.uk Verify scheme provides a useful template for consideration.

34. The RCUK Digital Economy theme has a programme of research in Trust, Identity, Privacy and Security. The use of extra targeted funding for a managed call specifically aimed at children and internet issues would be a very focussed way to bring together the research, civil society and policy makers across the UK to address these challenges.

26 August 2016

---

[1] http://www.horizon.ac.uk

[2] https://www.epsrc.ac.uk/links/councils/research-councils-uk-rcuk/digital-economy-research-rcuk/

[3] http://casma.wp.horizon.ac.uk

[4] Internet on Trial - Youth Juries Report on Internet and digital technologies http://casma.wp.horizon.ac.uk/casma-projects/irights-youth-juries/internet-on-trial-youth-juries-report-on-internet-and-digital-technologies/

[5] http://5rightsframework.com/

[6] Internet on Trial - Youth Juries Report section 3.1

[7] Google's terms and conditions are less readable than Beowulf, the Conversation, Oct 17, 2013 https://theconversation.com/googles-terms-and-conditions-are-less-readable-than-beowulf-19215

[8] MinorMonitor infographic http://www.minormonitor.com/infographic/kids-on-facebook/

[9] http://webuse.org/pdf/boydHargittaiSchultzPalfreyFM11.pdf

[10] http://dx.doi.org/10.1093/alcalc/agv128 cited in http://www.aappublications.org/news/2016/02/04/AlcoholAds012616

[11] http://www.publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/12902.htm

[12] Pan European Game Inforamtion http://pegi.info