# `I make up a silly name’: Understanding Children's Perception of Privacy Risks Online

**Jun Zhao**[1], Ge Wang[2], Carys Dally[3], Petr Slovak[4,5], Julian Edbrooke-Childs[6], Max Van Kleek[1] and Nigel Shadbolt[1]

[1]Department of Computer Science. Oxford University of Oxford. Oxford. UK

[2]Department of Information Studies. University College London. UK

[3]Department of Experimental Psychology. University of Oxford. Oxford. UK

[4]UCL Interaction Centre, University College London. London. UK

[5]. Department of Informatics, King’s College London

[6] Anna Freud National Centre for Children & Families. London. UK

Presented at the 37th Annual Conference of Human Factors in Computing Systems (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK

# Children growing up in a "smart" society

In the UK,

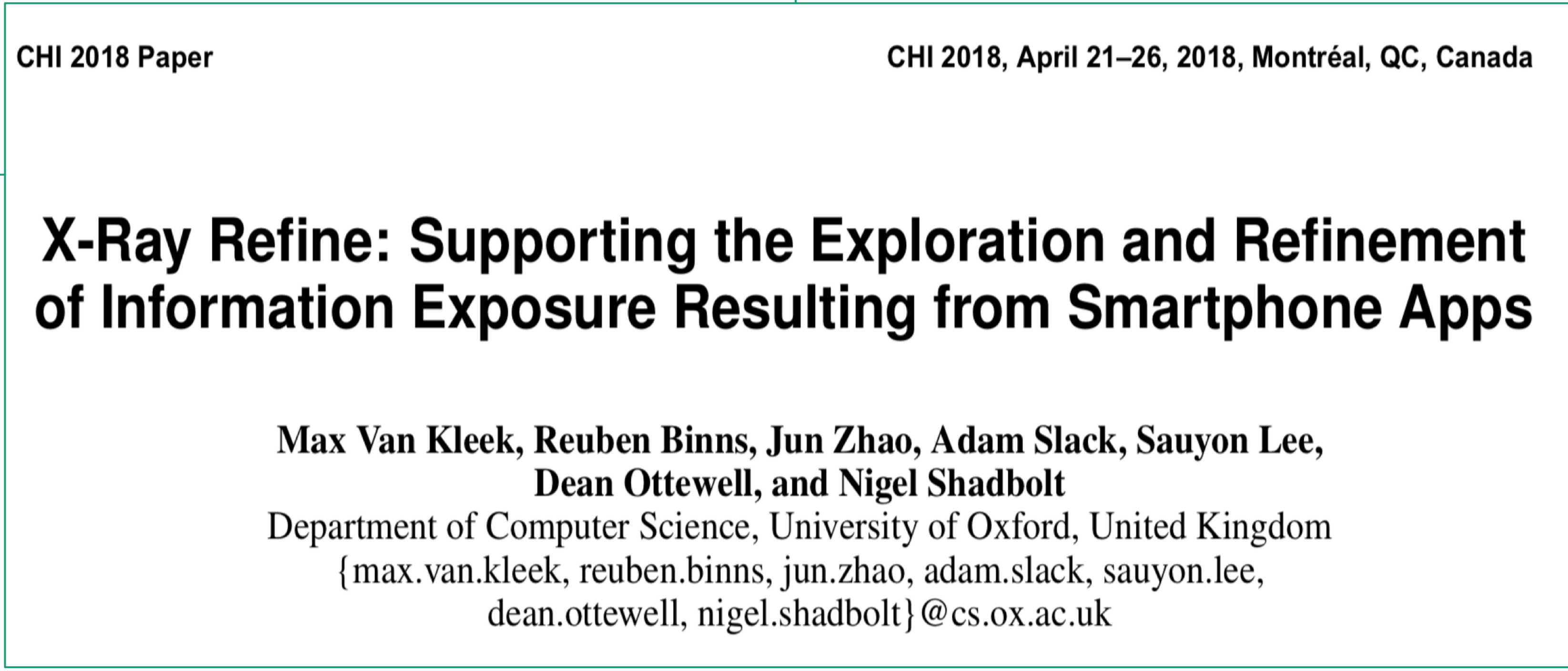
- 52% of 3-4yo go online, for nearly 9h a week
- 44% 5-10yo have been provided with their own tablets

*Source: 'Children and Parents: Media Use and Attitudes Report'*, Ofcom, 29 November 2018

# Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps

**Max Van Kleek**[*] {max.van.kleek} **Ilaria Liccardi**[†] {ilaria} **Reuben Binns**[*] {reuben.binns} **Jun Zhao**[*] {jun.zhao} **Daniel J. Weitzner**[†] {djweitzner} **Nigel Shadbolt**[*] {nigel.shadbolt}

[*]{}@cs.ox.ac.uk
Department of Computer Science
University of Oxford, UK



# X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps

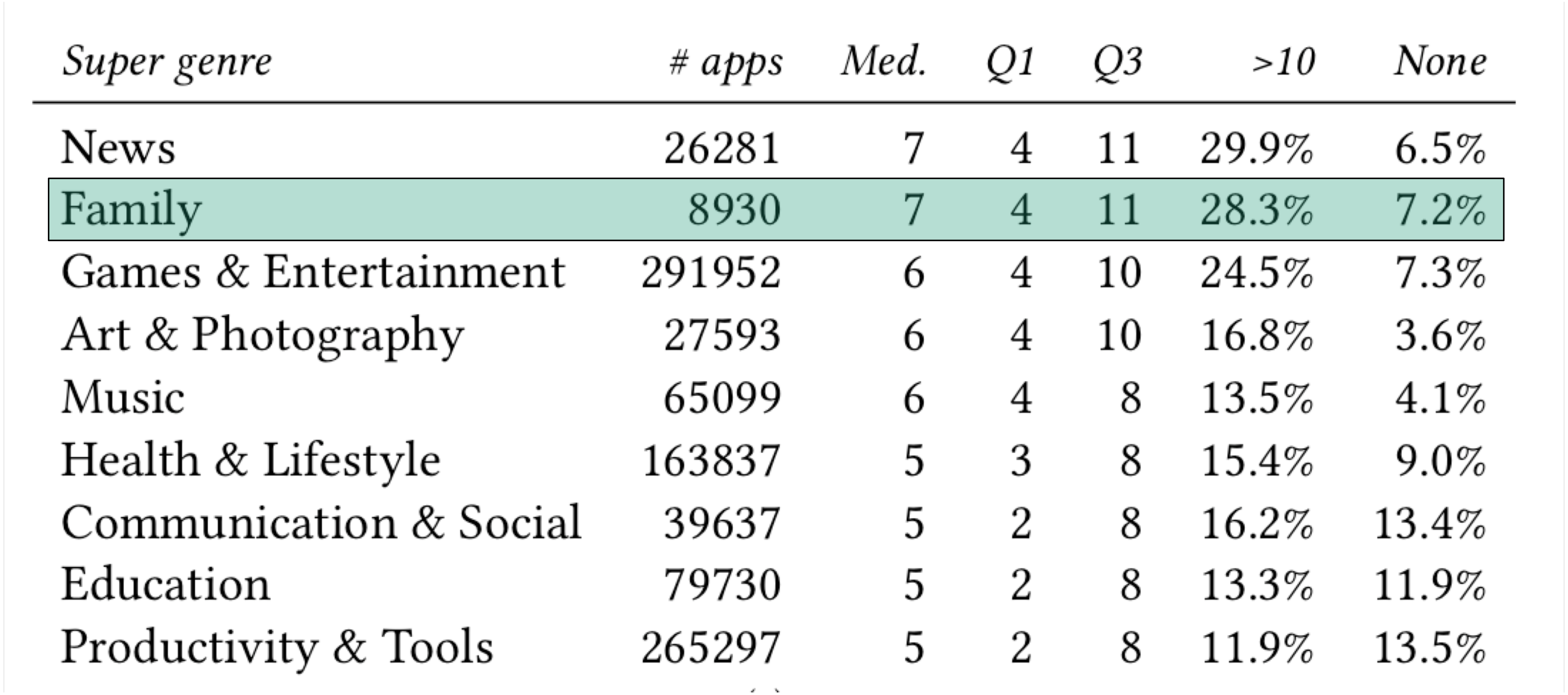
**Max Van Kleek, Reuben Binns, Jun Zhao, Adam Slack, Sauyon Lee, Dean Ottewell, and Nigel Shadbolt**
Department of Computer Science, University of Oxford, United Kingdom
{max.van.kleek, reuben.binns, jun.zhao, adam.slack, sauyon.lee, dean.ottewell, nigel.shadbolt}@cs.ox.ac.uk

"9 in 10 Google Play Store apps are sending data to Google"

"participants demanded more control and transparency"

Financial Times: https://ig.ft.com/mobile-app-data-trackers/.
Binns et al. "Measuring third party tracker power across web and mobile". TOIT. 18 (4) p52.

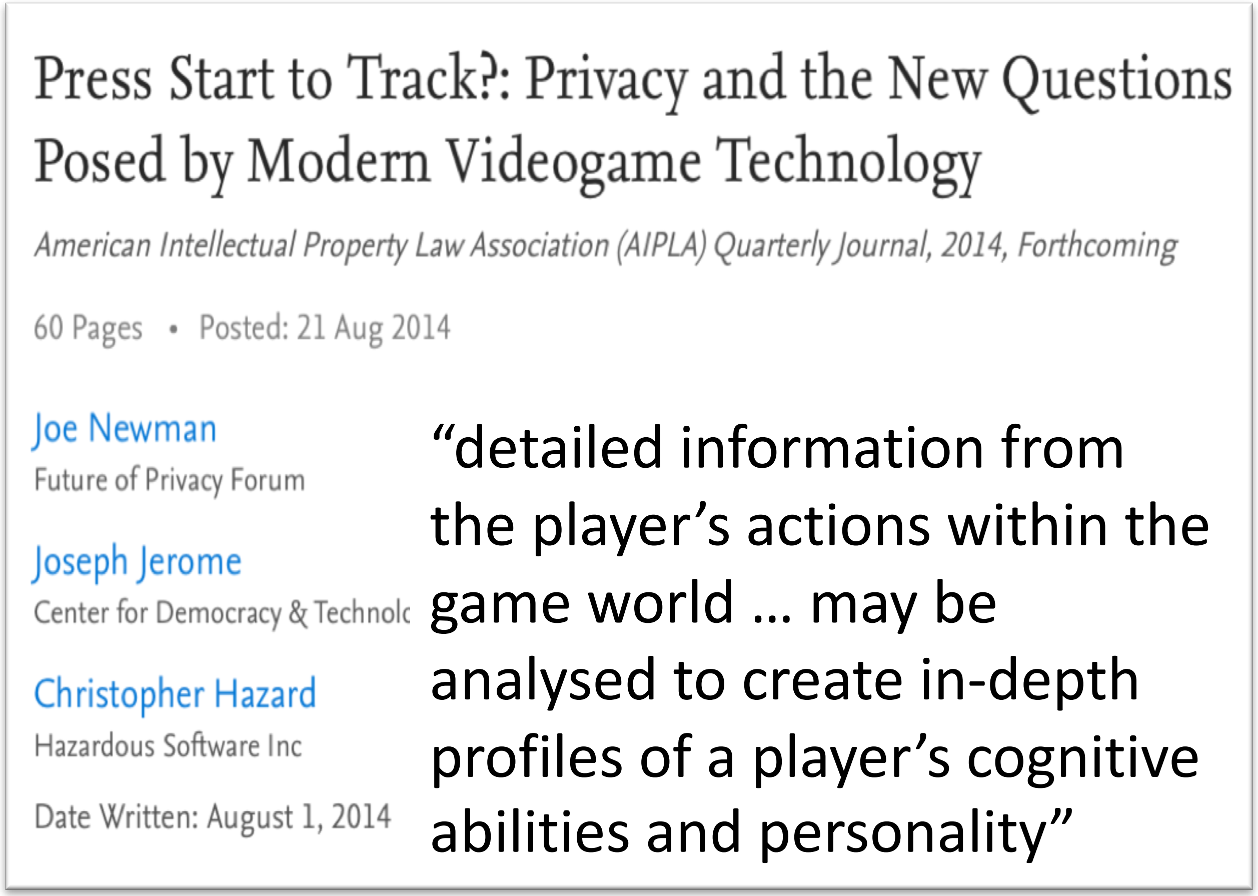
# Family apps are amongst the top associated with distinct trackers



| *Super genre* | *# apps* | *Med.* | *Q1* | *Q3* | *>10* | *None* |
|---|---:|---:|---:|---:|---:|---:|
| News | 26281 | 7 | 4 | 11 | 29.9% | 6.5% |
| Family | 8930 | 7 | 4 | 11 | 28.3% | 7.2% |
| Games & Entertainment | 291952 | 6 | 4 | 10 | 24.5% | 7.3% |
| Art & Photography | 27593 | 6 | 4 | 10 | 16.8% | 3.6% |
| Music | 65099 | 6 | 4 | 8 | 13.5% | 4.1% |
| Health & Lifestyle | 163837 | 5 | 3 | 8 | 15.4% | 9.0% |
| Communication & Social | 39637 | 5 | 2 | 8 | 16.2% | 13.4% |
| Education | 79730 | 5 | 2 | 8 | 13.3% | 11.9% |
| Productivity & Tools | 265297 | 5 | 2 | 8 | 11.9% | 13.5% |

"Third party tracking in the mobile ecosystem." Proc. of the 10th Web Science, 2018.

# Data tracking and surveillance raise less widely known privacy concerns



## Press Start to Track?: Privacy and the New Questions Posed by Modern Videogame Technology

*American Intellectual Property Law Association (AIPLA) Quarterly Journal, 2014, Forthcoming*

60 Pages • Posted: 21 Aug 2014

Joe Newman
Future of Privacy Forum

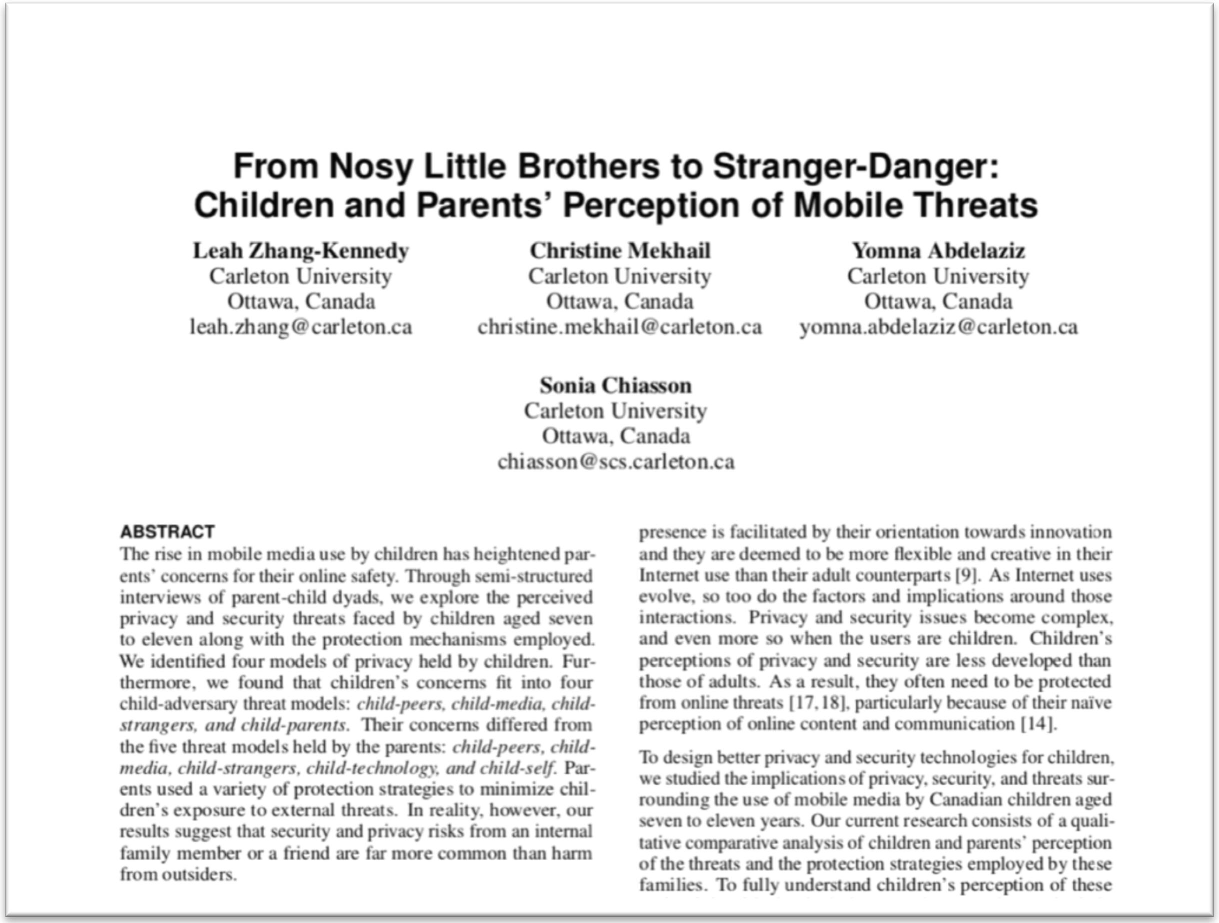
Joseph Jerome
Center for Democracy & Technolc

Christopher Hazard
Hazardous Software Inc

Date Written: August 1, 2014

“detailed information from the player’s actions within the game world … may be analysed to create in-depth profiles of a player’s cognitive abilities and personality”

# HCI Research of children under 11



## From Nosy Little Brothers to Stranger-Danger: Children and Parents' Perception of Mobile Threats

**Leah Zhang-Kennedy**
Carleton University
Ottawa, Canada
leah.zhang@carleton.ca

**Christine Mekhail**
Carleton University
Ottawa, Canada
christine.mekhail@carleton.ca

**Yomna Abdelaziz**
Carleton University
Ottawa, Canada
yomna.abdelaziz@carleton.ca

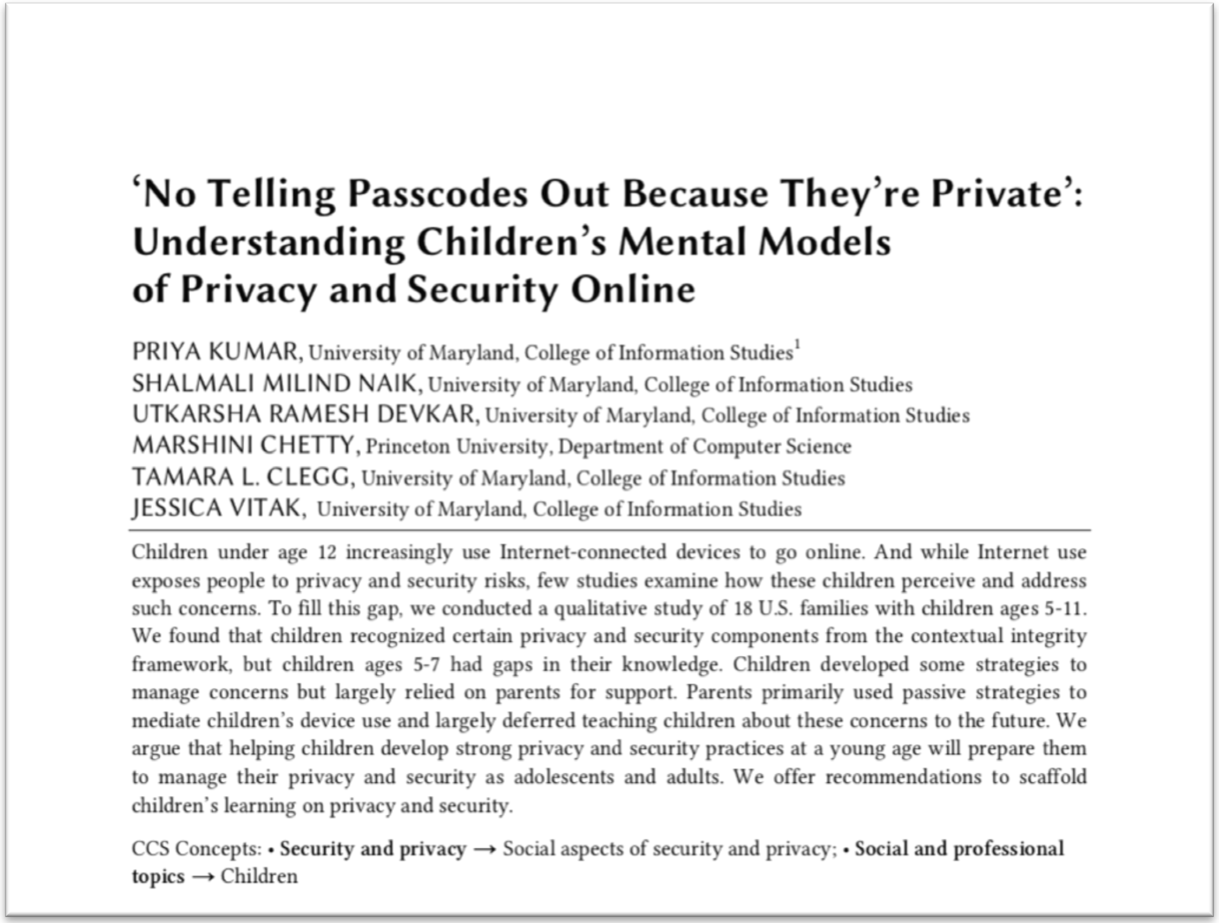
**Sonia Chiasson**
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

### ABSTRACT

The rise in mobile media use by children has heightened parents' concerns for their online safety. Through semi-structured interviews of parent-child dyads, we explore the perceived privacy and security threats faced by children aged seven to eleven along with the protection mechanisms employed. We identified four models of privacy held by children. Furthermore, we found that children's concerns fit into four child-adversary threat models: *child-peers, child-media, child-strangers, and child-parents*. Their concerns differed from the five threat models held by the parents: *child-peers, child-media, child-strangers, child-technology, and child-self*. Parents used a variety of protection strategies to minimize children's exposure to external threats. In reality, however, our results suggest that security and privacy risks from an internal family member or a friend are far more common than harm from outsiders.

presence is facilitated by their orientation towards innovation and they are deemed to be more flexible and creative in their Internet use than their adult counterparts [9]. As Internet uses evolve, so too do the factors and implications around those interactions. Privacy and security issues become complex, and even more so when the users are children. Children's perceptions of privacy and security are less developed than those of adults. As a result, they often need to be protected from online threats [17,18], particularly because of their naïve perception of online content and communication [14].

To design better privacy and security technologies for children, we studied the implications of privacy, security, and threats surrounding the use of mobile media by Canadian children aged seven to eleven years. Our current research consists of a qualitative comparative analysis of children and parents' perception of the threats and the protection strategies employed by these families. To fully understand children's perception of these



## 'No Telling Passcodes Out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online

PRIYA KUMAR, University of Maryland, College of Information Studies[1]
SHALMALI MILIND NAIK, University of Maryland, College of Information Studies
UTKARSHA RAMESH DEVKAR, University of Maryland, College of Information Studies
MARSHINI CHETTY, Princeton University, Department of Computer Science
TAMARA L. CLEGG, University of Maryland, College of Information Studies
JESSICA VITAK, University of Maryland, College of Information Studies

Children under age 12 increasingly use Internet-connected devices to go online. And while Internet use exposes people to privacy and security risks, few studies examine how these children perceive and address such concerns. To fill this gap, we conducted a qualitative study of 18 U.S. families with children ages 5-11. We found that children recognized certain privacy and security components from the contextual integrity framework, but children ages 5-7 had gaps in their knowledge. Children developed some strategies to manage concerns but largely relied on parents for support. Parents primarily used passive strategies to mediate children's device use and largely deferred teaching children about these concerns to the future. We argue that helping children develop strong privacy and security practices at a young age will prepare them to manage their privacy and security as adolescents and adults. We offer recommendations to scaffold children's learning on privacy and security.

CCS Concepts: • **Security and privacy** → Social aspects of security and privacy; • **Social and professional topics** → Children

# The open challenge

- How do children *describe* privacy risks
- How do children cope with different types of privacy risks

# Theory I: Inspiration

**Vygotsky’s Zone of Proximal Development (ZPD), motivating us to focus on children’s current knowledge and ability**

*“Start from what learners can do independently to what can be achieved by through guidance by a skilled partner”*

Seth Chaiklin. 2003. The zone of proximal development in Vygotsky’s analysis of learning and instruction. Vygotsky’s educational theory in cultural context 1 (2003), 39–64.

# Theory II: Data Analysis

**Nissenbaum's Contextual Integrity framework, guiding our unpacking of children's knowledge**

Yan Shvartzshnaider†*, Noah Apthorpe†, Nick Feamster, and Helen Nissenbaum

**Analyzing Privacy Policies Using Contextual Integrity Annotations**

- **Attributes**: the types of information being transmitted, such as personal information, etc.
- **Contexts**: the situation or scenario to which the social norms may be applied.
- **Actors**: the entities involved in the information transmission, which can be the subject, sender or recipient of the information.
- **Transmission principles**: the way information is transmitted from the sender of information to the recipients, such as unidirectional or bidirectional etc.

# Methodology --- data collection

- Focus groups with children aged 6-10

1. Warm-up discussions (10’)
2. Discussion of use of tablets at home and what they enjoy (10’)
3. Discussions of 3 hypothetical scenarios (story cards) (20’), broken into groups and facilitated by one facilitator

Bertie: an 8-yo koala bear who likes playing tablets

Bertie was watching a video about Lego on YouTube.

When it's finished, another video about "making objects out of candy" was played automatically.

- What should Bertie do?
- Why did Bertie see a very different video?
- Has something like this ever happened to you?
- Did you mind watching the video?

(a) Auto play

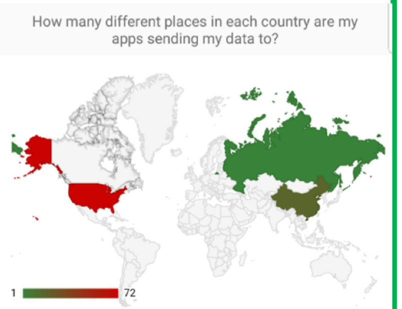
When Bertie was playing with a game, a window popped up and asked Bertie to talk to the game.

- What should Bertie do?
- Why did the game want Bertie to talk to it?
- Has this ever happened to you?
- Did you talk to the game?

(b) in-app pop-ups

Bertie's Mum found that that one of Bertie's games sends a lot of information to many other people. Mum wants to remove this app, but Bertie is not sure … …

- What do you think Bertie should do?
- Should Bertie listen to Mum and delete the game?
- Would you mind if one of your favorite apps did this?
- Would you stop using your favourite app if your knew it collects your data?


How many different places in each country are my apps sending my data to?
1
72

(c) Data track associated with their favorite app

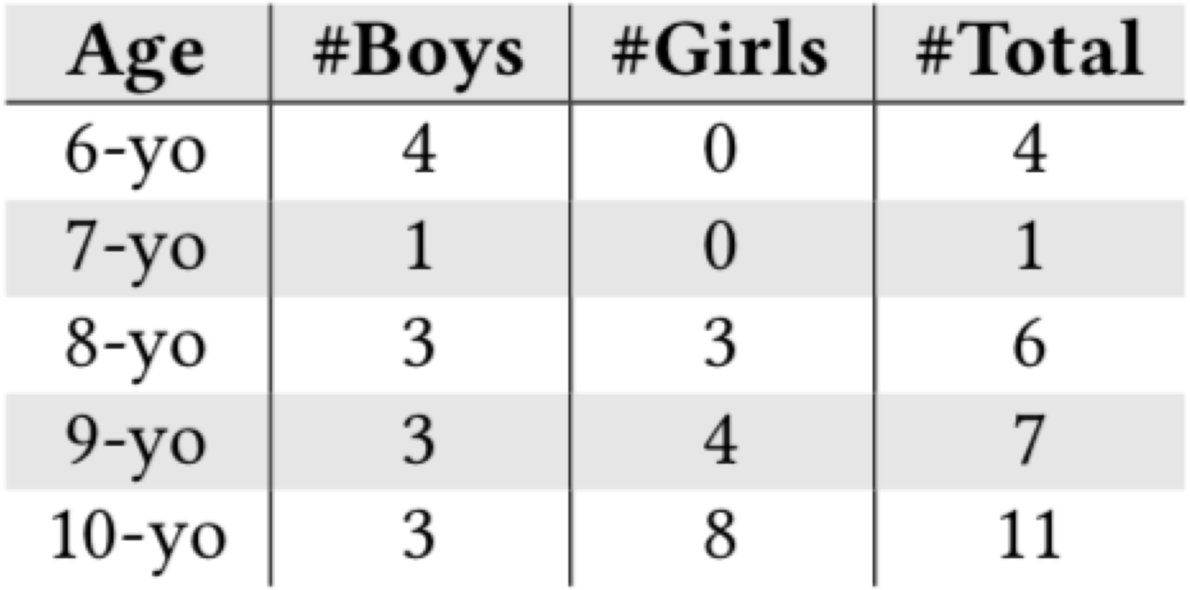
Bertie was watching a video about Lego on YouTube.

When it's finished, another video about "making objects out of candy" was played automatically.

- What should Bertie do?
- Why did Bertie see a very different video?
- Has something like this ever happened to you?
- Did you mind watching the video?

| | |
|---|---|
| What should Bertie do? | Why did Bertie see a very different video? |
| Has something like this ever happened to you? | Did you mind watching the video? |

# Participants Information



| Age | #Boys | #Girls | #Total |
|---|---|---|---|
| 6-yo | 4 | 0 | 4 |
| 7-yo | 1 | 0 | 1 |
| 8-yo | 3 | 3 | 6 |
| 9-yo | 3 | 4 | 7 |
| 10-yo | 3 | 8 | 11 |

- 29 participant children, including 14 boys and 15 girls, with an average age of 8.5 (range = 6-10, s.d. = 1.4).
- 12 focus group and the group size varied between 2 and 4, with an average group size of 2.4.

# Methodology --- data analysis

- Thematic data analysis
  - Independently coded half of the transcriptions by three researchers
  - Discussed and consolidated the initial code book
  - Finished coding the rest of the transcriptions
  - Validated coding reliability with Fleiss' kappa (0.83)

# Data themes --- Risk recognition

| Top code | Example quotes |
|---|---|
| Age appropriateness | “... things for adult” |
| Content appropriateness | “... the video is too scary” |
| Information oversharing | “I don't want everyone to know who I am and everything” |
| Stranger danger | “... you just type and don't let others listen to your voice, so can't find you easily” |
| Hacking danger | c6: Because it's probably just trying to hack you.<br>c6: Like getting into your account and your mom’s or dad's. |
| Online baiting | “Cause my sister did it, and it cost quite a lot of money. It doesn't say if it cost money” |
| Recommendations | R: Does anyone know why the video started?<br>C12: …because they want you to watch it |

# Data themes --- Risk coping

| Top code | Example quotes |
|---|---|
| By myself | “I'll delete the game. Because I don’t want people coming in” |
| Ask for help | ”Well if you don’t know then you need to tell your parents” |
| Following rules | “My mom said you can but only add the people you know, cousins or friends.” |
| Familiarity overriding rules | “If I watched that video before. If I don't know which Youtuber, I will not watch it.” |
| Play-and-see | “Because I play it all the time and nothing has happened to me” |

# Methodology --- data analysis round 2

- Applying the CI framework
  - Attributes
  - Actors
  - Context
  - Information Transmission

# Risk recognition and the CI framework

Attributes
Actors
Context
Information Transmission

> “Because **it's** probably just trying to hack you. Like getting into your account and your mom’s or dad’s.”

- Privacy context according to the child: someone trying to get into your account
- Actual privacy context: tracking of your data with gaining your consent

- Risk comprehension: children struggled to pinpoint *who* or describe their *attributes*

# Children’s ability to describe risks

| When risks are recognized or not | Risk scenarios | Words -- examples |
|---|---|---|
| Risk recognized | Inappropriate content | *Weird things* |
| | Stranger danger | *strangers* |
| | Personal information oversharing | *Personal information* |
| Risks vaguely recognized | Online promotions | *Channel people, app developers, get more subscribers* |
| | Pop-ups (Hacking danger) | *Hacking (as stealing from your house)* |
| | Data tracking (Hacking danger) | *Hacking (as tracking your information)* |
| | | *Hacking (as try and find you, find your location, know more about what’s happening in this country )* |
| Risks not recognized | Online promotions<br>Online baiting | *scary, angry, upset, annoying, surprised* |

# Children’s ability to cope with risks

| When risks are recognized or not | Risk scenarios | Children’s risk coping strategies |
|---|---|---|
| Risk recognized | Inappropriate content | Ask for help |
| | Stranger danger | Stop |
| | Personal information oversharing | Stop oversharing |
| Risks vaguely recognized | Online promotions | It’s ok, let’s play |
| | Pop-ups (hacking danger) | Stop<br>Ask for help |
| | Data tracking (hacking danger) | Stop |
| | | Ask for help |
| Risks not recognized | Online promotions (new videos)<br>Online baiting (YouTuber/games) | it’s ok, let’s play |

# Recap of Key findings

- Children care very much about their online privacy and they have a good understanding of certain privacy risks

- Children may not fully comprehending the risks even though they applied good coping strategies, which should key scaffolding points

# Future Work and Limitations

- Interaction with more diverse study populations
  - Children from disadvantaged background
  - Children from a different cultural background
- Following up and gaining deeper understandings
  - Hacking
  - YouTube video promotions
- Tool development and assessment
  - Support active mediations of parents and educators
- Contribute to policy development
  - Children’s best interest is not protected
  - Children felt “annoyed”, “surprised” or “angry” when they are coerced
  - Transparency and control is desired

Standards of age-appropriate design

1. Best interests of the child
2. Age-appropriate application
3. Transparency
4. Detrimental use of data
5. Policies and community standards
6. Default settings
7. Data minimisation
8. Data sharing
9. Geolocation
10. Parental controls
11. Profiling
12. Nudge techniques
13. Connected toys and devices
14. Online tools
15. Data protection impact assessments
16. Governance and accountability

Age appropriate design: a code of practice for online services

Consultation document

ico.

Information Commissioner's Office

KOALA
Kids Online Anonymity & Lifelong Autonomy

EPSRC
Engineering and Physical Scier
Research Council

MATHEMATICAL PHYSICAL AND LIFE SCIENCES DIVISION

UNIVERSITY OF OXFORD

# We thank all the schools and families for their time and support!

This work is supported by

**KOALA: Kids Online Anonymity and Lifelong Autonomy**
Funded by Oxford University’s EPSRC Impact Acceleration Account (EP/R511742/1)

Contact: jun.zhao@cs.ox.ac.uk
KOALA Project web site: https://sites.google.com/view/koala-project-ox/