European Cybersecurity Competence Centre (ECCC) ECCO

Community Group on Human Factors

Kai Rannenberg / Narges Arastouei

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Objectives

- Build a community of experts and "end users" for the WG domain by initiating work on a sequence of prioritized topics in the WG domain
- Support selected actions prioritised in the ECCC Strategic Agenda matching the WG domain, especially within
  - 1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs
  - 1.2.3 Promote security and privacy 'by design'
  - 2.1.4 Promote security and privacy 'by design' approach in training and education

Methodology

- Start with actions related to one or several of the topics listed in the ECCO technical offer:
  - 5G applications, ICT in mobility, security of day-to-day tools like smartphones, web meeting systems and services, Internet access technologies, digital money.
- Deep dive on proposals for priorities for DEP or other appropriate support measures
- Build sub-groups as needed
- …

Matching: ECCC Strategic Agenda actions Topics from Technical Offer

Action/Topic	1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs	1.2.3 Promote security and privacy 'by design'	2.1.4 Promote security and privacy 'by design' approach in training and education
5G applications			
ICT in mobility			
Security of day-to-day tools, e.g.			
Smartphones			
Web meeting systems and services			
Internet access technologies			
Digital money			
…			
…			

> Work on topics within the matrix prioritized by the community of experts and "end users"

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

Activities and deliverables

- Identification of relevant achievements / best practices (e.g. developed in the ECCC pilots) to address the Strategic Agenda
  - 1st webinar (March 8): **A Footprint of CyberSec4Europe: two prominent cybersecurity tools (Keynotes: Vashek Matyas et al, Masaryk University Brno, CZ)**
  - 2nd webinar (May 22): **Security-by-design for SMEs exploiting trusted hardware (Keynote: Antonio Lioy, Politecnico di Torino, IT)**
  - 3rd webinar (19 June): **Engaging Citizens and Civil Society in Cybersecurity (Dr. Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research)**
  - 4th webinar (23 July): **LINDDUN GO, Lightweight & Gamified Privacy Threat Modeling (by Jonah Bellemans at the DistriNet Research Group of KU Leuven (Belgium)).**
  - **Today's webinar (16 Sepmteber): From Awareness to Action: Enhancing Parental Engagement in Online Privacy Protection (by Ann-Kristin Lieberknecht at Goethe University Frankfurt)**

Activities and deliverables

- Recommendations for future specific priority "Joint Actions" (e.g. DEP projects) and other actions for the ECCC
  - Based on matching of goals with action types also considering the ECCC action plan

- Possible cooperation in immediate Joint Actions
  - Deep dive on specific topics: e.g. stemming from the needs of SMEs for easily accessible and user-friendly cybersecurity tools considering privacy

- Knowledge sharing events: presentations for EC, NCCs, ECCC
  - Webinars on the progress including refinement of the topics

ECCO CG on Human Factors (End Users, Consumers' / Civil society organisations, Human rights and Forensics)

How to join the CG

- Email: community_humanfactors-owner@list.cyber-ecco.eu with your
  - Contact details
  - Affiliation and role therein
  - Area of expertise

Keynote & Speaker

- **From Awareness to Action: Enhancing Parental Engagement in Online Privacy Protection**

This webinar will address the urgent and critical issue of protecting children's personal data in the digital age. As the collection of children's data continues to increase, many parents are finding it challenging to safeguard their children's online privacy—often due to a lack of knowledge and awareness. This highlights an essential need for privacy literacy training specifically designed for parents. The primary objective of this webinar is to shed light on the unique challenges faced by parents and to explore potential avenues for future research and EU coordinated activities.

- **Keynote Speaker: Ann-Kristin Lieberknecht**
    - She is a doctoral candidate at Goethe University Frankfurt, specialising in online privacy and its impact on families. She has studied and gained valuable experiences at the Dresden University of Technology, École de Management Strasbourg, and Goethe University Frankfurt, from which she obtained her Master's degree in Information Management and Marketing Analytics. Her passion for data protection has led her to pursue a doctoral degree to deepen her knowledge of the field. Her research focuses specifically on assisting parents in navigating and mitigating the potential risks associated with online privacy for their children. Through her work, she aims to create a safer digital environment for families and children.

ECCO Community-driven Knowledge Sharing Events

European Cybersecurity COmmunity

Children are vulnerable

Children are vulnerable people:

- Digital footprint often starts from (before) birth

- Often do not get the benefits and/or cannot exercise their right to privacy

- Privacy violations have a deeper impact on children
  (Clemons & Wilson, 2015)

Children's Privacy: A Shared Responsibility

Dimensions of Parental Privacy Protection
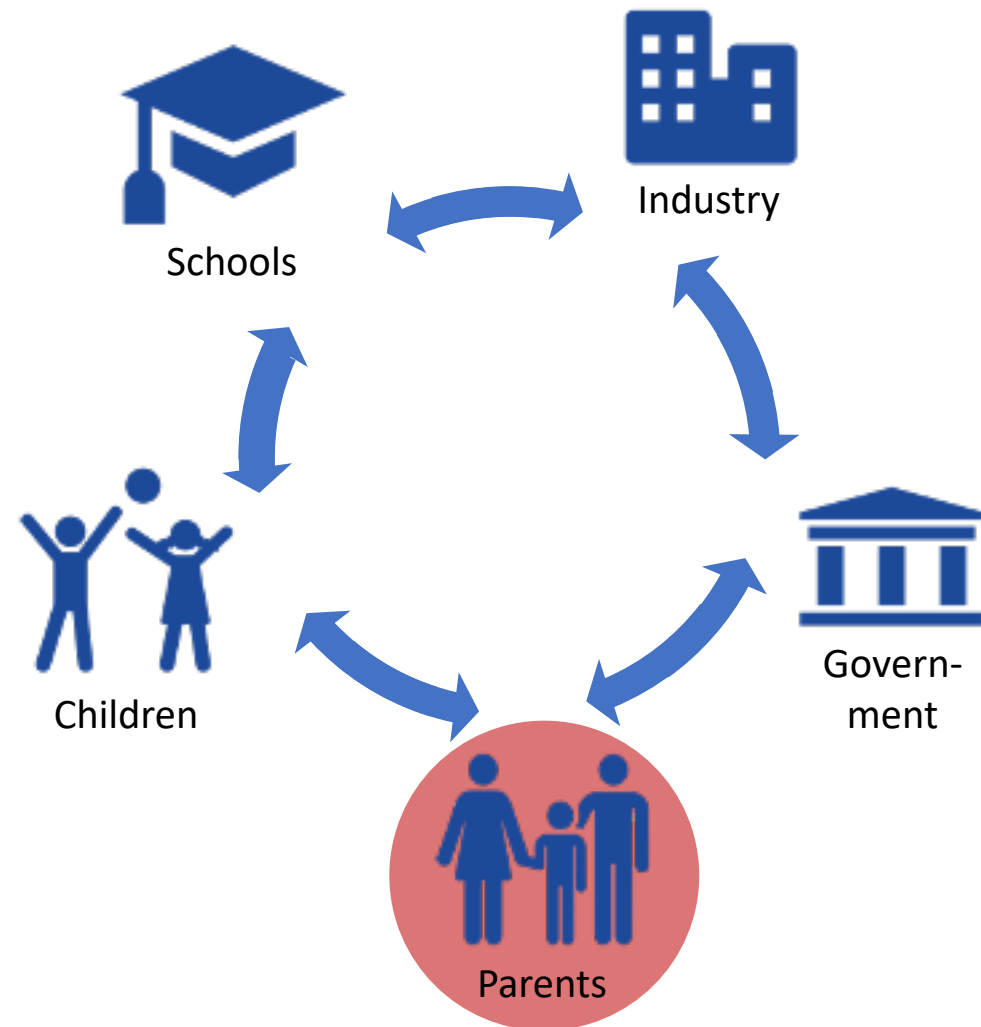
5 Dimensions in Children's Online Privacy Protection

1. Oversee own deeds (i.e. sharing, device buying, app usage)

2. Oversee children's deeds (i.e. sharing, app usage)

3. Oversee other stakeholder's action (i.e. sharing)

4. Teach children about online privacy

5. Respect children's privacy

   (Lieberknecht, 2024)

Current (EU) Initiatives and Offerings

Infrastructure

- Safer Internet Programme with Safer Internet Centres (SICs) in Europen Member States

- European Strategy for a Better Internet for Children (BIK)

Legislation:

- General Data Protection Regulation (GDPR)

- Digital Services Act (DSA)

Work with Parents

- Awareness raising activities, e.g. „Safer Internet Day"

- Resources and Guidelines

- Trainings and Workshops

Parent's Reality

Parents work hard to protect their children online.
However:

- May not fully understand the risks themselves nor be fully aware of their responsibility (Brito & Dias, 2020; Zhao, 2018)

- Struggle to keep up with technology and the evolving online activities of their children (Quayyum, 2023; Zhao, 2018)

- As a consequence may inadvertently compromise children's privacy (Minkus et al., 2015)

→Still, children highly depend on their parents.

→Considering the existing initiatives and offerings, **how can we enhance our support for parents** and address their unique situations and needs?

Research Objectives

1) Investigate **obstacles** that prevent parents from actively managing their children's online privacy

2) Investigate field-/time-tested **strategies** to engage parents in privacy education

3) Analyse **parents' and media educators needs** in relation to support

Methodology

Qualitative, explorative interviews for in-depth exploration

Media Educators working with parents on privacy

- Gain a deeper understanding of the target group, including their perspectives on the topic and motivation to participate in privacy literacy training

Parents of babys and toddlers

- Learn about parent's insights into their own behaviours, attitudes, and responses to privacy education
- Gain a more comprehensive understanding of privacy education from the recipients' point of view.

Methodology

Qualitative, explorative research

- 19 interviews with parents and media educators, working with parents

- Between 15-70 minute physical/virtual interviews in May-September 2023

- Analysis following Miles' and Hubermann's (1994) iterative qualitative data analysis model
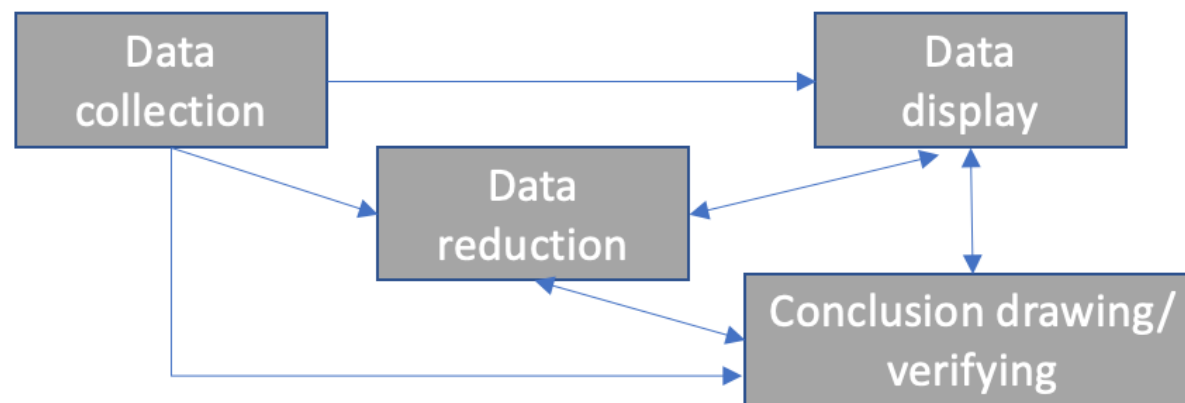
Parental Threat Awareness (total number of parents)

	Stranger Danger	Overexposure to Acquaintances	Surveillance	Data Brokers	Digital Integrity
Apps			3		
Retail Loyalty	1		7	2	
Social Media	7		1		3
Messengers	8	1	5		
Connected Devices	2		7		

Adapted from Minkus et al., 2015

1) **Parents exhibited limited awareness about…**

…the value of their data

…implications of certain privacy threats

…various types of data

…certain threats such as identity theft, threats to digital integrity, questionable data practices

…certain threat directions, i.e. acquaintances, commercial actors

→Teaching the basics of privacy protection is already likely to have a significant impact.

10

Key Findings

2) Parents are generally **not concerned** about their data being collected and often exhibit the belief that they have nothing to hide

→ Parents **will not search for information** on online privacy by themselves

→ **Privacy education** for parents needs to be **pushed**

3) Parents have the **strong wish to protect their children** and prevent conflicts with their children

4) Parents are often **happy to accept offerin**gs from schools, etc.

→ Strong contact point as well as prenatal class or the waiting room of the paediatric

Key Findings

5) Media educators observed **a fear of getting in contact with technology**. Additionally, parents exhibited limited awareness about protection strategies

→If parents can overcome this fear, they can get a feeling of control and will be able to stay up-to-date with the ever-evolving digital landscape and its threats.

→Strengthening digital self-efficacy needs to be focus

6) Media educators in our study indicated that parents had a **"herd mentality"**

→A major obstacle for individuals

→Could be turned into a strength, building on word-of-mouth and communities

7) Current efforts to educate parents focus on **parent-teacher conferences**
   - Not all parents attend these conferences and it is difficult to reach those who do not
   - Limited time for all media topics
   - Parents may feel ashamed, interactive work is only limited possible
   - Evaluating the effectiveness is challenging

→ Existing studies have shown success with alternative formates, i.e. **games, peer learning, and practice** (Quayyum et al., 2021; Sağlam et al., 2023; Zhang-Kennedy & Chiasson, 2021)**,** in cybersecurity education that are untapped for this target group

→ Additionally, recent research has shown that shared learning between parents and children can enhance the experience and create trust (Quayyum, 2023)

Future Work

1. Investigate parental determinants in online privacy protection

2. Examine how children's attitudes influence their parents' attitudes in order to gain a better understanding of this dynamic.

3. Understand clusters and dynamics within parent group.

4. Study novel education formats, their feasibility, efficacy, and acceptance both among media educators and parents.

Children's Privacy: A Shared Responsibility
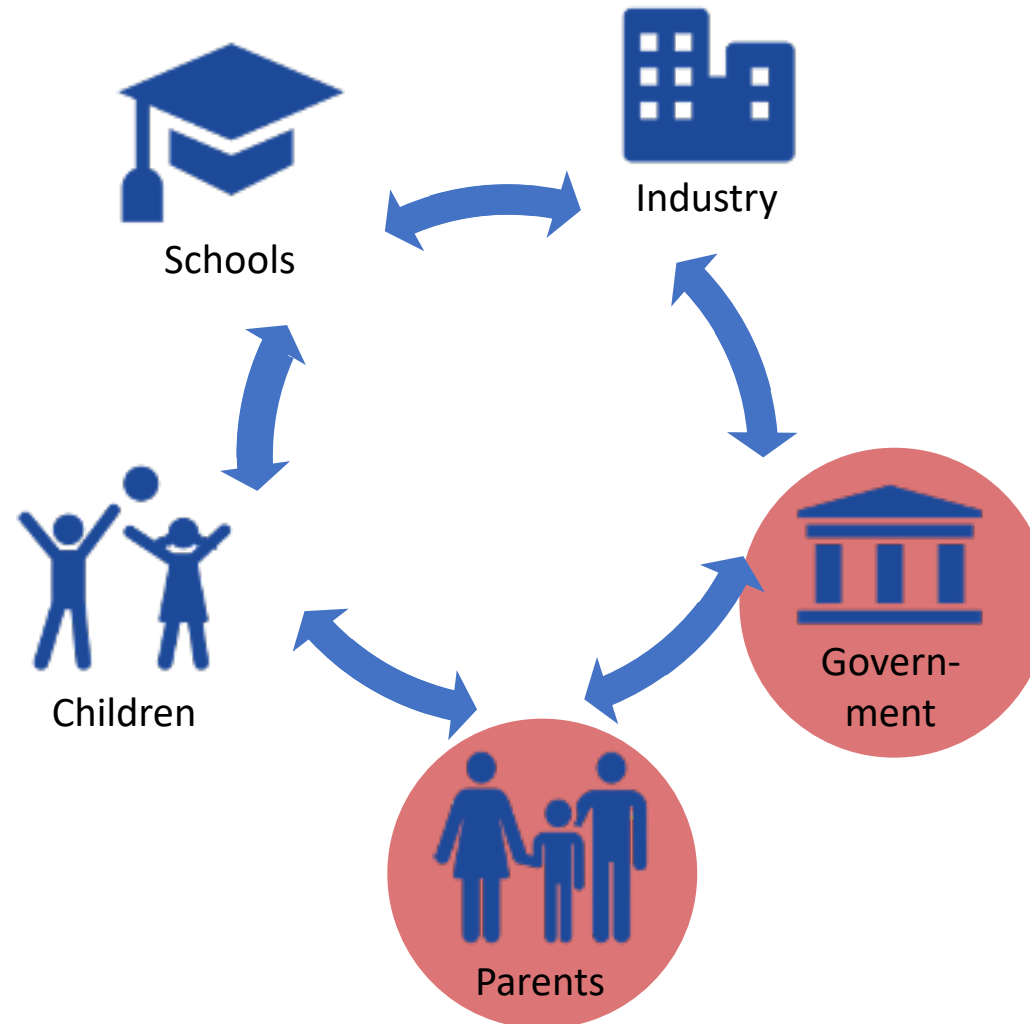
Possibilites for EU Coordinated Activities

1. Development of privacy literacy programs with focus on new formats

2. Public awareness campaigns

3. Research funding, e.g. on efficacy of literacy programs, determinants for parental engagement in privacy protection, parent-child interaction

4. Include parents in politcal discourse

5. Establish feedback mechanisms

Conclusion

We need to rethink and recognise parents as **vital assets** and **key stakeholders** in ensuring children's online privacy:
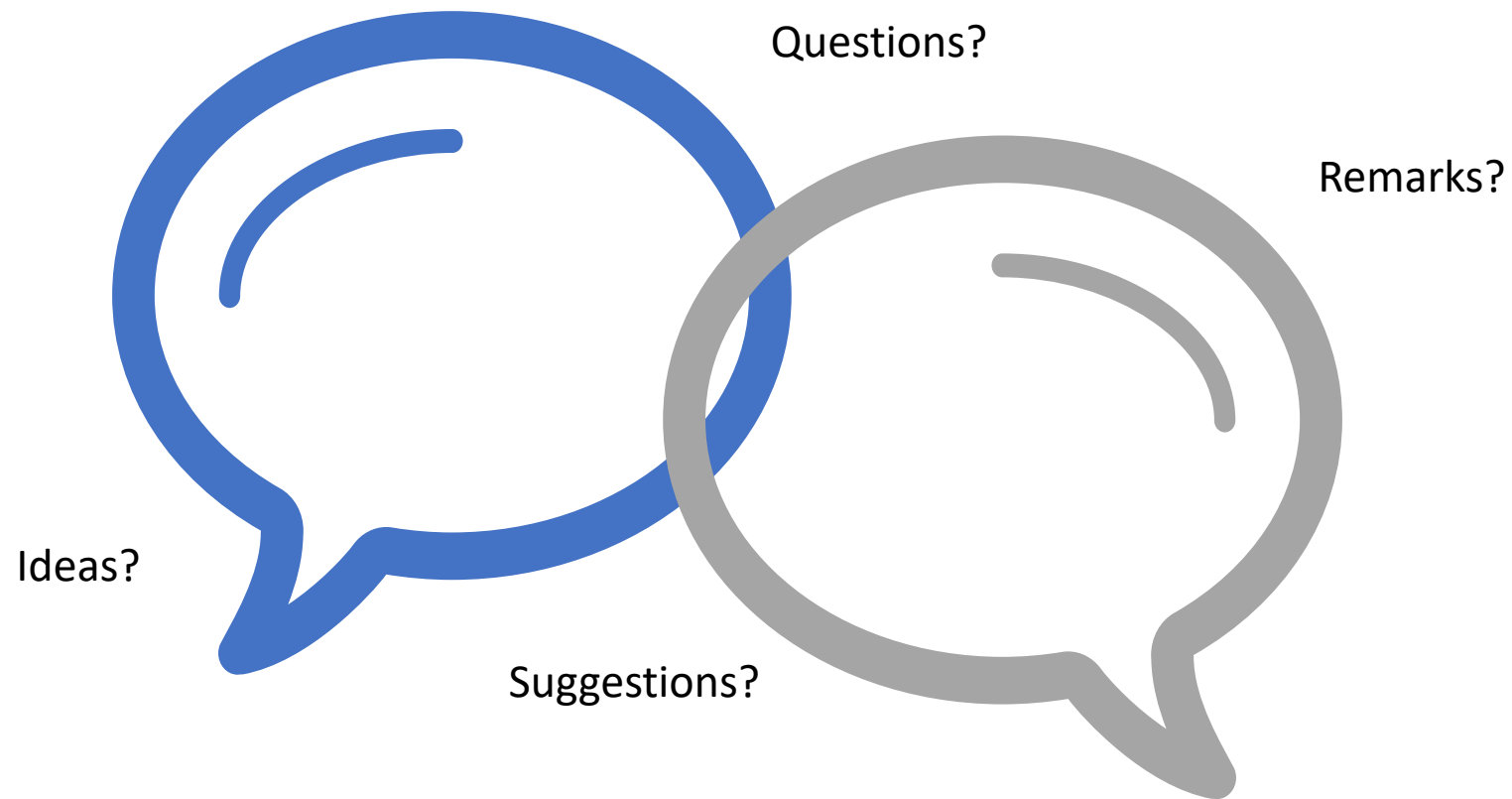
- Ideally situated with their child's best in mind
- Willing to accept offerings pushed to them
- "Herd mentality"
- Only teaching basic principles might already have a significant impact

We need to meet and reach parents in their specific context and make them feel understood and heard.

Thank you!

Questions?

Remarks?

Ideas?

Suggestions?