Pedagog.ai

The Ethics of AI Child Monitoring: Surveillance or Safety?

Why?

This lesson builds critical thinking and ethical awareness in students as they navigate the complex issue of child monitoring apps and AI technology. By exploring real-world scenarios and ethical dilemmas, students gain a deeper understanding of the delicate balance between privacy and safety, consent and autonomy, and the impact on family relationships. This lesson equips students with the skills to make informed decisions about technology use, promoting responsible digital citizenship and open discussions within families and society at large.

Materials Needed	Time needed
• Printed Simulation handouts	• Approximately 45 - 60 minutes

Objectives

- Students will be able to analyze the ethical dilemmas arising from the use of child monitoring apps, distinguishing between privacy concerns and safety considerations.
- Students will be able to identify and describe the potential impact of AI-powered child monitoring apps on trust and communication within family relationships.
- Students will be able to evaluate the role of consent and autonomy in the use of child monitoring apps
- Students will be able to propose ethical guidelines and solutions to balance the benefits and challenges of AI in child monitoring apps

Key Concepts & Vocabulary

- **Geofencing**: A feature in child monitoring apps that allows parents to set virtual boundaries on a map, triggering alerts when a child enters or leaves specified areas, such as home or school.
- **Data Encryption**: A security measure to protect sensitive information, ensuring that data is converted into code to prevent unauthorized access.

Lesson Components

1. **Before You Watch**: Connect lesson to background knowledge of AI child monitoring apps and get students' attention
2. **Video**: Show the pedagogy.cloud video explaining the ethical considerations in the topic of child monitoring
3. **Case Study**: Detail a real-world scenario that relates to the issue of privacy and security in monitoring apps
4. **Simulation**: Lead students through an interactive activity exploring the possible ethical considerations

5. **Discussion**: Ask whole-class questions to reflect on experience and consider perspectives.
6. **Assessment**: Verify student understanding with an exit ticket

1. Before You Watch

- Begin the lesson by asking the students if any of them have family tracking apps installed on their phones, such as "Family360" or similar apps. Encourage students to raise their hands or simply share if they are comfortable.
- For those who indicate they have experience with such apps, ask them to briefly share their experiences. They can mention whether they find the app helpful, any concerns they or their parents have, and whether it has affected their family dynamics. Are there any positive stories where the app helped them? (Try to avoid a complaint session.)
- For students who haven't used such apps, ask them if they are aware of anyone in their family or friend circle who uses them, and whether they have any thoughts or questions about these apps.

While You Watch: Mention these topics and questions for students to look out for as they watch the video:

- Define real-time tracking. How does it work in child monitoring apps?
- Identify an example of how constant tracking affects trust in families.
- Look for examples of how monitoring apps can benefit kids.

2. Video Summary

The video discusses how parents often rely on technology, including AI-powered child monitoring apps, to ensure their children's safety. These apps offer features like real-time location tracking and emergency alerts, providing reassurance to parents. However, they also raise concerns about privacy, trust, and data security, emphasizing the need for open discussions within families and responsible use by technology companies. Balancing privacy and safety in this digital landscape is essential, and through understanding the ethics of AI in child monitoring apps, we can harness technology to strengthen family bonds while respecting individual privacy.

3. Case Study

Distribute or read Case Study handout.
Summary: The fictitious “EyesOut” app is designed to allow parents to monitor their children's real-time whereabouts, raising questions about the balance between privacy and safety, consent and autonomy, and the impact on child-parent relationships. The app’s data security measures and the risk of hacking are also key concerns. The company responds by considering customizable permissions and enhanced data security, but whether these changes fully address the challenges of creating an app that ensures safety while preserving relationships remains a question.

4. Simulation

1. Begin by introducing the case study scenario involving the “EyesOut” app and its ethical considerations.
2. Explain the roles students will assume: Tech Representative, Parent, Child, and Cybersecurity Expert.
3. Mention the objective of evaluating app features from different perspectives.
4. Break up the class into groups of about four. Assign each student a specific role (Tech Rep, Parent, Child, or Cybersecurity Expert). If groups have more than four, include additional Parent and Child roles. If a group only has three, eliminate the Cybersecurity Expert role.
5. Provide Simulation handout with feature descriptions to each group for the Tech Rep to share.
6. For each app feature, have the Tech Rep in the group explain the feature. Then the tech rep asks for comments from the students representing the Parent, Child, and Cybersecurity Expert roles.
7. After conversation on each feature, the Tech Rep should decide whether the feature should be added.
8. After going through all of the features (or as many as time allows), bring the whole class back together to discuss the simulation.
9. Go through the list of features one at a time and ask the different groups’ Tech Reps whether they would add the feature or not, and why.
10. Finish off with whole-class discussion questions.

5. Discussion

These questions are designed to be used in whole-class discussion. Ask questions that relate most effectively to the lesson.

1. If your parents made you install an app like this as a requirement for having a cell phone, how would you respond?
2. How do you balance the safety of a child with their right to privacy in the context of child monitoring apps?
3. Should parents have the authority to monitor their child's social media activity and online interactions through an app? What benefits would this feature have for parents?
4. Can daily activity reports strike a balance between keeping parents informed and respecting a child's personal space and privacy?
5. Is there a specific age or level of maturity at which a child should have decision-making authority over their privacy?
6. What are the potential consequences of monitoring private chats, and how might this impact trust between parents and children?

6. Assessment

Exit Ticket: Provide a prompt for students to reflect on their learning, such as:

- What is one key lesson or insight you gained from today's discussion on child monitoring apps, and how has it influenced your perspective on the topic?
- If you were tasked with creating an ethical guideline for the development and use of child monitoring apps, what would be your top priority or principle, and why?

Pedagog.ai

Sources to Learn More

Reviews of popular monitoring apps -

- https://www.tomsguide.com/us/best-parental-control-apps,review-2258.html
- https://www.verywellfamily.com/best-parental-control-apps-4779963
- https://www.pcmag.com/picks/the-best-parental-control-software
- https://www.parents.com/parentsirl/best-parental-monitoring-apps/

News features about parents' decision to monitor -

- https://www.bbc.com/worklife/article/20211105-the-parents-who-track-their-children
- https://www.theguardian.com/media/2022/may/01/honey-lets-track-the-kids-phone-apps-now-allow-parents-to-track-their-children

Pedagog.ai

Case Study: Family Tracking

Description: A fictitious company has come out with the new “EyesOut” app, which is designed to allow parents to monitor their children's whereabouts in real-time – to “keep an eye out” for them. It provides a convenient way for parents to ensure their children's safety and know their location at all times. Families start using this app, and it isn’t long before the company starts getting complaints for a number of reasons.

- **Privacy vs. Safety**: The “EyesOut” app raises questions about the balance between a child's right to privacy and the parent's desire for safety. Should parents have the ability to track their child's every move?
- **Consent and Autonomy**: Do children have a say in whether they want to be tracked, or is this decision solely up to the parents? What age is considered appropriate for a child to have a say in such matters?
- **Impact on Child-Parent Relationships**: How does constant tracking through “EyesOut” affect the trust and relationship between parents and their children? Does it foster open communication or lead to a lack of trust?
- **Data Security and Hacking Risk**: Data collected by the “EyesOut” app is sensitive and could be valuable to criminals. How important are data security measures, such as secure storage and authentication? What are the consequences of a data breach and the impact on children's safety?

The company takes information from the complaints and makes the following decisions as a company:

- **Customizable Permissions**: "EyesOut" could offer customizable permissions, allowing children to have some control over when and how they are tracked. This way, parents can balance safety with respecting their child's autonomy.
- **Enhanced Data Security**: The developers of "EyesOut" can invest in robust data security measures, regular security audits, and encryption to protect the location data from potential breaches.

But are these two changes enough? Do they address all of the challenges in creating an app that provides safety but maintains relationships?

Questions

- How can we strike a balance between ensuring child safety and respecting their privacy?
- What role should technology play in parenting?

Pedagog.ai

Simulation Activity

Each group's Tech Rep should read the possible app features to the group. For each feature idea, the other team members discuss whether they are in favor of that feature, or opposed. The Tech Rep then decides whether to include that feature in the app.
Mark on your paper whether you are going to include the feature or not.

Role descriptions

Parent – Answer as if you were a parent wanting to use this app to keep your child safe
Child – Answer as if your parents required you to use this app in exchange for getting a cell phone
Cybersecurity Expert – Answer with the concern that any data could be stolen

App Feature	Include?
Real-Time Location Tracking: "EyesOut" allows parents to track their child's location in real-time, helping ensure their safety and providing peace of mind.	
Geofencing: With geofencing, parents can set virtual boundaries on a map, receiving alerts when their child enters or leaves predefined areas, such as school or home.	
Social Media Monitoring: The app monitors a child's social media activity, alerting parents to potentially harmful or inappropriate content and troubling interactions.	
Web Browsing History Tracking: "EyesOut" keeps a record of a child's web browsing history, enabling parents to review their online activities and ensure safe internet usage.	
Emergency Alerts: In case of emergencies, the app can send instant alerts to parents, providing location information and ensuring a rapid response.	
Daily Activity Reports: Parents receive daily reports summarizing their child's online and offline activities, helping them stay informed about their child's well-being.	
Private Chat Monitoring: The app can monitor private chats and conversations on various messaging platforms, aiming to detect signs of cyberbullying or harmful content.	
Data Encryption: "EyesOut" prioritizes data security by employing robust encryption methods to protect user information from unauthorized access.	
Child Consent Settings: Children can adjust privacy settings within the app, allowing them some control over what information is shared and monitored.	
Automatic App Blocking: To maintain a safe online environment, the app can automatically block certain apps or websites deemed unsafe, preventing access by the child.	

Pedagog.ai

Video Script for Animator

Hello Young Innovators! Today we're discussing the ethics of AI in child monitoring.
Title screen

In today's digital age, many parents use technology to ensure the safety and well-being of their children. One such technology is AI-powered child monitoring apps, designed to provide parents with peace of mind.

[Socrat narrating throughout, facing the viewer.
First scene is a family living room, with a window behind them. The parents and about a 13-year-old (Daughter, black hair) are sitting on a couch. The parents should be looking at the viewer, and the child is looking at a cell phone. Example image: https://i.imgur.com/TKZlPSv.png]

They offer features like real-time location tracking, which lets your parents know where you are and instant emergency alerts when you need help. These features help parents feel more comfortable when their kids are away from home.

[The child hops up off the couch, and walks outside. The child is seen walking past the window looking at phone. The parents look out the window at her. Example image: https://i.imgur.com/dbBOALr.png]

Monitoring apps do provide some significant benefits. For example, imagine your phone gets lost. Location tracking can help you or your parents find it quickly.

[In the house scene. Child is looking various places for phone. Mother has a buzzing cell phone. Example image: https://i.imgur.com/RZy6UIC.png Child reaches under the couch cushion and pulls out phone. They smile and give each other a thumbs-up.]

They can also alert parents when you are in an emergency situation. This helps parents feel better knowing that they will find out if you need help.

[A street scene where there is a minor car accident. Smoke is coming up from the rear car's hood. Child is standing outside the car taking a picture with her cell phone. Example image: https://i.imgur.com/XfZXnL4.png
Scene shifts abruptly to the living room, where the father picks up his phone and looks at it. His eyes go wide, and then he calms down, having been reassured that everything is OK. He puts his hand on his chest and shows relief – head goes up and eyes close. Example image: https://i.imgur.com/R44k8eP.png]

These apps can be reassuring. But people also have some concerns about them. One concern is the issue of privacy. Do you want people to know where you are all the time?

And what about trust – how does using these apps affect your relationship with your family?

[Socrat now standing outside on the sidewalk. The child walks into the frame behind him, looks at phone, and frowns, then crosses a crosswalk and exits the other side. Example image: https://i.imgur.com/S3rHZqn.png]

This can make you feel like someone's always watching you. It's essential to find the right balance. Should kids have the option to control what information is tracked? Setting boundaries and talking with your family can help build trust and understanding.

[Child talking to parents – show mouths moving to represent conversation. At first they are frowning, but toward they end of the conversation, they smile and nod at each other. Example image: https://i.imgur.com/2AwG7JA.png]

Another issue with these apps is that they collect a lot of information about you. Companies say they don't use this information in bad ways, but sometimes people are concerned about the data getting into the wrong hands. Your data needs to be protected!

[Scene changes to a person trying to hack into a computer and files transferring before the screen flashes red and he leans forward in shock. Example image: https://i.imgur.com/YUNVxFv.png]

It's important for you to talk to your family about how these apps make you feel and what boundaries you're comfortable with. It's also important for companies to ensure that you are secure when using their apps. There is a delicate balance between privacy and safety. And we all have a part to play in making sure that balance is reached.

[Family having a conversation again. Same example image from before https://i.imgur.com/YUNVxFv.png.]

By learning, discussing, and understanding the ethics of AI in child monitoring apps, we can make technology work for us, keeping us safe, respecting our privacy, and strengthening the bonds with our loved ones.

[Dad puts his arm around child, and family looks at Socrat and smiles. Example image: https://i.imgur.com/V6dj4na.png]

Let's discuss: How can technology help us build trust and understanding within our families?
[Display question on screen at end of video: How can technology help us build trust and understanding within our families?]

Pedagog.ai

Video Script for Narrations

Hello Young Innovators! Today we're discussing the ethics of AI in child monitoring.

In today's digital age, many parents use technology to ensure the safety and well-being of their children. One such technology is AI-powered child monitoring apps, designed to provide parents with peace of mind.

They offer features like real-time location tracking, which lets your parents know where you are and instant emergency alerts when you need help. These features help parents feel more comfortable when their kids are away from home.

Monitoring apps do provide some significant benefits. For example, imagine your phone gets lost. Location tracking can help you or your parents find it quickly.

They can also alert parents when you are in an emergency situation. This helps parents feel better knowing that they will find out if you need help.

These apps can be reassuring. But people also have some concerns about them. One concern is the issue of privacy. Do you want people to know where you are all the time? And what about trust – how does using these apps affect your relationship with your family?

This can make you feel like someone's always watching you. It's essential to find the right balance. Should kids have the option to control what information is tracked? Setting boundaries and talking with your family can help build trust and understanding.

Another issue with these apps is that they collect a lot of information about you. Companies say they don't use this information in bad ways, but sometimes people are concerned about the data getting into the wrong hands. Your data needs to be protected!

It's important for you to talk to your family about how these apps make you feel and what boundaries you're comfortable with. It's also important for companies to ensure that you are secure when using their apps. There is a delicate balance between privacy and safety. And we all have a part to play in making sure that balance is reached.

By learning, discussing, and understanding the ethics of AI in child monitoring apps, we can make technology work for us, keeping us safe, respecting our privacy, and strengthening the bonds with our loved ones.

Let's discuss: How can technology help us build trust and understanding within our families?