"How technical do you get? I'm an English teacher": Teaching and Learning Cybersecurity and AI Ethics in High School

Zachary Kilhoffer[1], Zhixuan Zhou[1], Firmiana Wang[2], Fahad Tamton[1],
Yun Huang[1], Pilyoung Kim[3], Tom Yeh[4], Yang Wang[1]
[1]University of Illinois at Urbana-Champaign, [2]University of Illinois Laboratory High School,
[3]University of Denver, [4]University of Colorado Boulder
{dzk2, zz78, fywang, ftamton2, yunhuang, yvw}@illinois.edu, pilyoung.kim@du.edu, tom.yeh@colorado.edu

***Abstract*—Today's cybersecurity and AI technologies are often fraught with ethical challenges. One promising direction is to teach cybersecurity and AI ethics to today's youth. However, we know little about how these subjects are taught before college. Drawing from interviews of US high school teachers (n=16) and students (n=11), we find that cybersecurity and AI ethics are often taught in non-technical classes such as social studies and language arts. We also identify relevant topics, of which epistemic norms, privacy, and digital citizenship appeared most often. While teachers leverage traditional and novel teaching strategies including discussions (treating current events as case studies), gamified activities, and content creation, many challenges remain. For example, teachers hesitate to discuss current events out of concern for appearing partisan and angering parents; cyber hygiene instruction appears very ineffective at educating youth and promoting safer online behavior; and generational differences make it difficult for teachers to connect with students. Based on the study results, we offer practical suggestions for educators, school administrators, and cybersecurity practitioners to improve youth education on cybersecurity and AI ethics.**

***Index Terms*—cybersecurity, AI ethics, education**

1. Introduction

Young people are tomorrow's designers and decision makers; they are often heavy users of technologies, navigating the online world as part of their education and personal lives [47]. However, young people can be especially vulnerable to falling for misinformation, unknowingly disclosing personal information to dangerous apps or websites, and behaving inappropriately on social media [47]. Cybersecurity is thus a crucial topic for K-12 education [39].

Ethics is increasingly recognized as a key component of cybersecurity education [22]. A quarter century ago, Ellenwood wrote, "there is a real danger of teaching adolescents in a manner that ignores personal or moral development, but focuses entirely on academic achievement. Adolescence is a time of upheaval when young people need guidance" [27]. The same could be said about today's ever-changing technological society; with new cybersecurity risks, and expansive AI technologies, we need to ask ourselves, how can we best prepare students to flourish [2]?

High schoolers are an especially interesting group for ethical education as they are in the last required stage of formal education, beginning their adult lives, and in the final 'formal operational' stage of cognitive and emotional ability development [59]. Adolescence is a key period for developing a deeper understanding of moral values and concern for others [36], but low empathy can lead to moral disengagement [3]. It is therefore important to promote empathy for vulnerable people in ethics education [63]. Further efforts are urgently required to educate high schoolers about cybersecurity, AI, and surrounding ethical issues [14], [70].

Cybersecurity ethics is a relatively new and interdisciplinary topic, and the research community diverges somewhat on its parameters [73]. As such, it would be difficult or even counterproductive for us to use a strict definition of cybersecurity and AI ethics. Instead of imposing our own definitions, we rely on high school teachers' own conceptualizations.

Effectively teaching K-12 students about cybersecurity and AI ethics can be instrumental in ensuring ethical development and use of tomorrow's technologies. However, little is known about how K-12 teachers cover cybersecurity/AI ethics. To help bridge this gap, we conducted an exploratory qualitative study in which we interviewed 16 high school teachers and 11 high school students in the US.

The main goal of our study is to understand how cybersecurity and AI ethics are currently taught, and ought to be taught, if not already. We focus on the teachers' views and struggles, as our main goal is to inform practitioners. The students' views allow us to elaborate on and verify our findings. We aim to answer three main research questions:

- **RQ1**: What topics do high school classes cover relating to cybersecurity and AI ethics?
- **RQ2**: What are the teaching strategies and resources used to cover these topics for high schoolers?
- **RQ3**: What challenges remain for teaching these topics to high schoolers?

To answer these questions, multidisciplinary expertise is required [61]. Therefore, our research team includes developmental psychologists, K-12 curriculum designers, two high school students, and privacy/security researchers.

Our work makes three main contributions: (1) uncovering what kinds of topics related to cybersecurity/AI ethics are taught in American high schools, and how; (2) presenting

novel results about challenges encountered in teaching high schoolers about cybersecurity/AI ethics; and (3) providing concrete recommendations on how to better support high school teachers in covering cybersecurity/AI ethics.

2. Related Work

We situate this work in two groups of literature - teaching ethics in high schools, and cybersecurity and AI ethics education.

2.1. Teaching Ethics in High Schools

Ethics concerns statements and judgments about how the world is and how the world should be. Ethics deals with norms and values, and expresses approval or disapproval through a specialized vocabulary (e.g. duty, right) [37], [57].

Ethics is always taught in American high schools by teachers modeling acceptable behavior [57]. More formally, ethics is part of high schools' curricula, aiming to teach skills like reflective judgment and moral sensitivity. Revell and Arthur argue that high school teachers and students would like more opportunities to discuss ethical issues, but their subjects and/or schools limit this attempt [62].

While teachers can include ethics instruction in all subjects, social studies is especially conducive to teaching ethics [24], [52], [57]. Subject matter like current and historical events provide ready-made case studies, allowing students to discuss and immediately apply ethical principles [66]. Imagined scenarios are also useful to spur ethical debate and discussion in the humanities [21], [13].

2.2. Cybersecurity & AI Ethics Education

A fundamental goal of cybersecurity ethics education is to prepare future decision-makers in the realm of cybersecurity [25]. To this end, it is more useful that students learn ethical frameworks to apply in an unknown future, rather than memorize codes of ethics and learn compliance [11]. Multiple ethical frameworks converge on issues including fairness, balancing the "good" versus harm or risk, and the protection of innocent parties [25].

AI is very much a part of this discussion given its large and growing impact on individuals and society [23], [67]. AI is immensely helpful in many domains, yet it may be a fundamental threat to individuals' privacy, security, and autonomy [67]. Thus, contemporary AI relates to value dilemmas such as balancing fairness [7] and bias [38], or surveillance [28] and privacy [72], while raising fundamental questions about the meaning of being human [33].

With the volume of ethical issues brought by AI and cyber attacks, many have called for more and better AI ethics education [14], [31], [55], [73]. Topical empirical research often focuses on college students [35]. AI ethics are taught relatively frequently in computer science courses at universities. Garrett et al. found that common topics in standalone AI ethics courses included bias, automation and robots, law and policy, consequences of algorithms, philosophy/morality, privacy, future of AI, and history of AI. Common topics in technical AI/ML courses were bias, fairness, and privacy [31]. Similarly, Raji et al. found that the current AI ethics education space relies on a form of "exclusionary pedagogy," and proposed a shift towards a more collaborative and holistic approach [61]. In addition to CS courses, medical students benefit from AI ethics education [41], [60], [77], as AI is heavily used in medicine.

A variety of methodologies are useful in teaching cybersecurity/AI ethics. In 2015, Burton et al. reported using sci-fi to teach college students AI ethics [16]. Furey and Martin created a modular approach to AI ethics education which requires two days of instruction in a one semester course [30]. Green described a pilot AI ethics course in undergraduate level where students learned to incorporate ethics in explicit ethical agents [34]. An experimental course taught cybersecurity with a case study-based ethics curriculum through readings, group discussions, and a final project. As suggested in earlier studies [25], students indicated that complex case studies and open discussions were central to their understanding of cybersecurity ethics [11].

At present, AI/cybersecurity ethics education is not mandatory in US high schools. Still, practitioners are actively developing AI/cybersecurity ethics education, especially for extra- and co-curricular programs for high school students [16]. Ali et al. developed curricula to teach grade school students about AI with an emphasis on constructionism, ethics, and creativity [2]. Short stories with embedded ethical dilemmas were effective for secondary school students to develop a more nuanced understanding of AI ethics issues, such as fairness, bias and privacy [29]. The "AI in My Life" project engaged 500 teenagers from disadvantaged backgrounds in a workshop series, and empowered them to evaluate the ethical implications of AI in their lives [8]. A card-based design workshop allowed high school students to reflect on ethical dilemmas by designing their own machine learning applications [10]. A gamified program called PicoCTF introduced cybersecurity to high school students through challenges tied to a story, while requiring little familiarity with command line or technical tools [20]. The GenCyber summer camp introduced high school students to cybersecurity (ethics) principles through computer game-based learning, hands-on labs, and group discussions [40].

In addition, cybersecurity and AI ethics may incorporate digital citizenship, and especially online safety or cyber hygiene. Digital citizenship typically concerns online participation that is safe, ethical, and legal [32]. Online security is a particular concern for teens, as existing evidence shows that they are quite vulnerable to attacks like phishing [54]. Interactive and gamified training has been found to be useful to educate young adults to improve cyber hygiene, especially their awareness of phishing attacks [40], [43], [69].

In recent years, the US has increased efforts to teach young people cybersecurity and digital citizenship, as evidenced by the passage of the K–12 Cybersecurity Act of 2021 [1]. According to the International Society for Technology in Education, three states (Virginia, California,

Nevada) are leaders in digital citizenship education [71]. As of 2022, 14 states require some form of digital citizenship or media literacy instruction at the K-12 level [46].

Teachers and students generally had a favorable impression of these cybersecurity and AI ethics materials, but important challenges remain. For example, simultaneously learning new tools (i.e. command line) and concepts (i.e. cybersecurity ethics) can be difficult for students [20]. Jin et al. found the gamified approach effective, but male students enjoyed game-based learning more than females [40]. It follows that cybersecurity and AI ethics learning materials must be carefully designed to ensure accessibility and inclusion for all high school students.

3. Methods

We conducted semi-structured interviews online with 16 high school teachers in the US about their experiences in teaching cybersecurity and AI ethics. We enrich and contextualize these findings with 11 student interviews.

Ethical considerations. Teachers were asked to read a consent form and verbally consent to the interview being recorded. Minors verbally assented, and a parent/guardian signed a consent form. This study was IRB approved.

3.1. Participants

Participant recruitment. We strove to recruit teachers and students with experience teaching/learning about cybersecurity and AI ethics from a diverse set of schools, across multiple states, and representing urban and rural areas. We started with our own professional networks, sending emails describing the project and soliciting their participation if they have relevant experience. The recruitment texts are in the appendix. We also recruited through snowball sampling and social media - particularly a Facebook group for cybersecurity educators. Student recruitment was similar; most participants responded to posts on a social media group dedicated to women in technology, and two students were referred by a teacher we interviewed.

Participant background. To encourage participation and shorten the study duration, we decided not to directly ask about our participants' demographic data but instead asked them to self-describe themselves. We still strove to recruit interviewees from schools with diverse student bodies. We also considered that characteristics of the schools could provide important context. We therefore asked interviewees to describe their school in terms of factors such as location (i.e. proximity to a large city), size of the student body, and school demographics (i.e. race and ethnicity, socioeconomic level). Due to our snowball recruitment, we interviewed teachers and students from the same school in two instances.

To make students feel comfortable with the study, we asked them to describe themselves. Several students chose not to share specific information about themselves, such as their age, the name of the school they attend or the city they live in. Students ranged from sophomores to seniors in public schools across five states. Two students attended a cybersecurity course in a nearby affiliated technical college, and their answers focused on this course. Six students attended selective enrollment schools. Further details of interviewees are provided in Table 1, and schools in Table 2 in the Appendix.

TABLE 1. OVERVIEW OF INTERVIEWEES

Alias	State	Primary topic/role	School
T1	IL	Librarian	SCH1*
T2	IL	Computer Literacy	SCH1*
T3	CO	Director of Extracurricular	SCH4
T4	IL	Library Director	SCH3
T5	UT	Cybersecurity	SCH12
T6	IL	Library Director	SCH2
T7	CO	English and Language Arts	SCH11
T8	CO	English	SCH10
T9	CO	Dean of Students	SCH9
T10	IL	Political Science	SCH2
T11	IL	Media Literacy	SCH2
T12	NJ	Librarian/Maker space	SCH7
T13	CO	Cybersecurity	SCH8
T14	CO	Teacher of Students w/Visual Impairment	SCH6
T15	WI**	Computer Science	SCH5
T16	IL	Social Studies	SCH1
S1	IL	Student	SCH1*
S2	IL	Student	SCH1*
S3	IL	Student	SCH1*
S4	UT	Student	SCH12
S5	UT	Student	SCH12
S6	IL	Student	SCH13*
S7	TX	Student	SCH14*
S8	IL	Student	SCH15*
S9	IA**	Student	SCH16
S10	IA**	Student	SCH16
S11	UT	Student	SCH17

hline

* indicates schools with selective admissions.

** indicates a state with no requirement for digital citizenship/media literacy instruction at K-12 level [46].

Interviewees included teachers with a particular topic area (i.e. Computer Science, English) as well as librarians, and two with administrative responsibilities. The interviewed librarians taught relevant materials, and the administrators were included due to their excellent overview of what is taught in their school districts. Multiple teachers also taught high schoolers in summer programs or co-curricular activities (i.e. Yearbook, Multimedia).

Despite our best efforts, we struggled to recruit from rural and lower-income schools. To an extent this was expected; K-12 cybersecurity education is especially lacking outside wealthier urban areas [19]. While our interviewees were quite diverse, we cannot claim that they are representative of US high school teachers and students in general.

3.2. Data Collection

Interview protocol. Our interviews aimed to understand the content and format of cybersecurity/AI ethics lessons and curricula. We asked all teachers about their teaching background and school to provide context and better understand their relevant experience. We then probed for relevant teachings, asking questions such as "Could you tell us what

you covered related to cybersecurity and AI ethics?" We also asked if the topics were covered elsewhere in the school.

Afterwards, we went in-depth, asking questions like "How was your experience teaching that topic?", "How did students react?", and "Did you feel like you really got through to the students on that topic?" We followed with questions about lesson details (e.g. concrete examples of discussions, tools used for exercises). As most teachers were not teaching curricula with cybersecurity, AI, and ethics explicitly embedded, we explored any relevant experience in depth. When time permitted, we sought out opinions on specific topics students should be taught and when, as well as strategies and best practices on cybersecurity and AI ethics educational materials. We followed roughly the same format for students, but asked for their perspective, and that of other students. The interview scripts are in the Appendix.

Interview procedure. We used Zoom for interviews, except for one teacher, who preferred to answer via email. Interviews lasted about 30 to 60 minutes and were recorded. Teachers and students were offered an Amazon gift card of $30 or $15, respectively. We used OtterAI to produce rough transcripts, then manually corrected them.

3.3. Analysis

We analyzed interviews using thematic analysis [15]. One co-author coded each interview, and a second co-author independently coded six interviews. We coded iteratively over the course of the project, regularly discussing and (re)creating codes, and identifying emergent themes. We started with over 200 codes, then reached consensus on around 50. Examples codes include surveillance (theme: privacy), participatory approach (theme: teaching method), and disengaged (theme: student attitudes). Because of the exploratory nature of the study and the collaborative coding process, we do not calculate inter-rater reliability as guided by the best practices [50].

The research team frequently discussed the data and used mind-mapping tools to develop and refine groupings of similar information and synthesize results. We observed signs of saturation for the answers to our research questions, as our most recent interviews presented no new themes.

4. Results

Drawing from interviews from both high school teachers and students, we present our findings on topics high school teachers cover relating to cybersecurity and AI ethics, strategies and resources they use, and challenges they encounter.

4.1. Cybersecurity/AI Ethics Topics Taught (RQ1)

Our expectation was that mostly STEM teachers would agree to interviews on teaching cybersecurity and AI ethics topics, given the literature on undergraduate courses. However, 12 of 16 teachers taught non-technical subjects such as social studies and language arts, and nevertheless covered relevant content.

One reason is that any class can incorporate current events discussions in class, and cybersecurity and AI ethics are increasingly relevant in current events. Moreover, civics/social studies teachers saw technology ethics as important for democracy, while English and language arts (ELA) teachers emphasized the need to be critical information consumers. More generally, teachers pursued interesting and engaging discussions when time permits, even when they had no obvious relationship with the curriculum. "Somehow we got way off track, which happens a lot in a high school classroom, if you've not been in one before" (T4). Below, we present a list of topics discussed.

Epistemic norms. Epistemic norms refer to what we believe to be true and telling the truth [51]. Relevant topic areas include media and information literacy, fake news, dis/misinformation, and conspiracy theories, with the goal of making students critical consumers of information, good researchers, and informed citizens. In practice, lessons and discussions on epistemic norms often entail treating something in the news as a short case study.

> "You can do this with most any current event. I'm like, 'Okay, do you believe this at its face value? Is it a conspiracy theory? Is it accurate?' And then we talk about like, okay, if you were going to [...] make a decision, how would you go about proving whether or not this was true?" (T15)

Teachers noted a special need to discuss current events in the 'post-truth' and COVID era. T7 said that students "see their parents struggling, they see people protesting [...]" Fake news, roughly meaning information that the creator knows to be false [18], came up a great deal. Primarily in ELA classes, students learned how to identify fake news as part of broader lessons on proper sourcing in research. T4 and T8 emphasized how constant exposure to misleading information can lead to radicalization.

> "I think this English department is very much about teaching research, [...] cite sources, bias, and all that kind of stuff. And so to [the teachers], misinformation, or the age of Donald Trump, really freaked them out. [...] For me as the librarian, misinformation is the most essential, both in terms of consumption and in production." (T4)

'The big lie' that the 2020 election was stolen from Donald Trump [12], [64], and other conspiracy theories, came up in discussions. At times, these issues were very personal for students: "We were describing these various conspiracy theories, and how they tie into extremist views. One of the kids, I remember saying 'This is - this is my mom, and my dad, both to a tee. Like, they believe in all of this stuff.' [...] I felt bad for him." (T11)

T6, T8, and T15 spoke to students about the potential for recommender systems to influence our autonomy and view of reality.

> "We've had this conversation around recommendation algorithms and [students will say] 'Well, it gives me good content, why should I care? [...]

> Especially with my ninth graders, they struggle to connect that those recommendation algorithms are influencing how you think about the world." (T8)

Privacy. Privacy is one of the most commonly acknowledged cybersecurity ethics issues [72], [75], and nearly all interviewed teachers approached it to varying degrees. Privacy came up in discussions on current events, such as the Facebook–Cambridge Analytica data scandal, and students' own online behavior. Thematically, teachers highlighted access control, the vulnerability of personal data, selective sharing and consent, and surveillance.

Most teachers voiced their opinion that students place little value in privacy, believing it to be a relic of the past.

> "They're a little disconnected. They've already resigned themselves, like 'Eh, it's privacy."' (T15)
> "My definition of privacy is far, far different from my students. They basically don't have any expectations. It is not a concern." (T5)
> "As one kid said, 'They already have us."' (T8)
> "I think kids understand for the most part, there's really no privacy in a lot of these apps and just anything that they do online." (T12)

This may be somewhat surprising, given previous findings that teens value privacy, but they often negotiate perceived privacy risks and expected benefits of information disclosures differently than adults [48], [49]. However, high schoolers are not far removed from childhood, and children have a limited understanding of privacy [42]. Children recognize that privacy involves autonomy, but lacking the autonomy of adults, it is less of a concern [78].

Teachers speculated about why students feel this way about privacy. T5 cited the frequency and publicity of cybersecurity breaches as indications that privacy violations are inevitable. This attitude seems to reflect learned helplessness [58] - particularly the belief that efforts to protect their privacy would not make a difference [35]. Other teachers highlighted generational differences. T9 said "We also have a generation of kids that are born after 9-11, after the Patriot Act. And this is their norm."

Simultaneously, teachers recognize contextual nuance in students' privacy expectations. Students appeared less concerned by invasions of privacy by tech companies and the government, but had clearer privacy expectations regarding schools and parents, aligning with previous literature [74]. Some students reacted strongly to perceived violations of privacy at their schools, expressing shock that someone could monitor what they Google or send in an email.

> "It's like the end of the world, they are just floored! Some of them mentioned how in our school, there's certain words - if you say it in an email, sometimes you get called down to the office. [And students say] 'Oh my gosh, I didn't know my emails are being monitored!"' (T13)

For their part, students represented a wide spectrum of privacy preferences and behaviors. S11 stated: "Some [students] won't even post their face online. Other people will, on a daily basis, maybe even hourly, post about what's going on in their lives." Students maintain privacy in different ways, like using multiple social media accounts, pseudonyms, or managing apps their parents installed: "Students ask, 'Hey, my parents installed this on my cell phone to track me. [...] How can I hack that?"' (T5).

Multiple teachers addressed what they consider the main problem with teenagers' attitudes on privacy and social media usage: managing their digital footprint. Some teachers emphasized maturity, suggesting that sharing inappropriate content was largely a problem for underclassmen. "[At] high school level, it's pretty obvious [...] because they know someone who's been burned by it" (T5). T4 noted seniors applying to 'serious' colleges take proactive steps to make it harder to link their identities with their online personas.

Sexting and nude selfies were an important topic for librarians who guest-taught in health classes on mental health and interpersonal relationships. These discussions concerned peer pressure, and the trust and risk associated with intimate relationships. Such discussions are preventive or in reaction to specific incidents.

> "What happened was a bunch of boys asked their girlfriends to send them nude pictures. And one boy was like, 'Hey, guys, let's all put these photos into a Google Drive under our school account, and then we can just share it and everybody can see everybody all the time. Wouldn't that be great?' And so they did it. So then the school is in trouble for like, child pornography. Huge thing." (T6)

The teachers' responses confirm previous findings that high school teachers are eager to provide students with guidance on online privacy, but often feel unqualified to do so [26]. However, we observe much of the issue relates to perceived generational divides in privacy paradigms, rather than a lack of knowledge on the teachers' part.

Digital citizenship. Digital citizenship is defined as "skills enabling people to find, evaluate, and share information responsibly, engage in constructive conversation with others from diverse backgrounds, and ensure their online participation is safe, ethical, and legal" [32].

All interviewed teachers discussed the potential of technology to build community, entertain and educate, and contribute to students' personal growth. Some teachers emphasized social media's potential as a positive and empowering tool: "Social media means controlling your narrative" (T9). Similarly, several teachers emphasized the value of AI-powered websites as sources for learning virtually anything. T7 had students develop chat bots to help others.

> "Students could pick a topic where that chat bot would help, and they could pick their audience. So some students made a chat bot for teens to help them with mental health, or some of them made it for adults to help them with figuring out where they want to go with their job." (T7)

Simultaneously, teachers characterized social media as a source of myriad ethical problems and dilemmas. Teachers related social media to cyberbullying, toxicity and harassment, hate speech, loss of privacy, fake news, cyberstalking,

brainwashing, and addiction. T8, for example, explained that some of their students use Instagram, TikTok, and Snapchat in a never-ending cycle. T9 relayed their students' perception that "our addiction to technology, our connection to technology, is what makes us human."

Teachers largely agreed that students are aware of risks in online interactions (i.e. cyber bullying, hate speech, harassment) and the need for decorum. T8 quipped that students don't care about inappropriate content online ("they want to find it!"), but "[they] care about how people treat each other on these platforms, and how content incentivizes people to treat each other different ways." (T8) Nevertheless, several teachers mentioned cyberbullying incidents on Instagram and Discord that their schools needed to address. T16 observed "a general lack of empathy" in students surrounding one cyber bullying incident.

ELA teachers in particular stressed the importance of online information sharing. In journalism class, T9 taught "what it means to be ethical in that sense - in sharing the news." T4 challenges students to consider "Are you even looking up the info and verifying it before you repost?"

Lastly, several teachers address legal compliance and liability. In classes like Media Studies, Journalism, and clubs like yearbook and school newspaper, ethical content creation and curation are important. Content creation requires adherence to laws and norms - especially when students act on behalf of the school. Teachers were quite creative with copyright and intellectual property rights. T15 taught in the context of Fortnite dances (i.e. can a dance be copyrighted?), and T4 based an activity on the show Shark Tank. In this exercise, students have to develop a new product without "basically stealing an already existing product."

Emerging technologies. Emerging technologies typically involved discussions of new and interesting technology, especially involving AI. Examples included deep fakes, facial recognition, social credit scores (in China), police robots, predictive policing, and self-driving cars. Of these, self-driving cars appeared most often (n=4) as a case study because "it's so fascinating. And it's so tangible. [...] We're close. We're really close" (T15). Self-driving cars lend themselves to interesting hypotheticals to explore.

> "This box falls off the car [driving in front of you]. You're in your self driving car, there's a motorcycle left, there's a family and a minivan right. Should your car risk your own life and crash into the box and save the people around it? [...] We give them that ethical dilemma to start." (T9)

Emerging technology discussions also ventured into more speculative 'sci-fi concepts'. In T9's sci-fi literature class, they lead conversations over the distinction between cyborgs with advanced AI and humans, and the ethical implications of AI in law enforcement.

> "We also talk about predictive policing, and they use these algorithms to determine where crime is going to happen before it happens. Then I show that scene from Minority Report where they bust in that guy's house at the beginning. And I said, 'Yeah, that seems extremely futuristic. But here's *real* predictive policing.'" (T9)

Ethical hacking. Ethical hacking concerns people and activities that might fall under black, gray, or white hat hacking. These lessons often center on: actual cyberattacks on individuals, organizations, or governments; how to defend against specific types of attacks; motives of the attackers; and the responsibility to defend the vulnerable. Generally, this topic arises in a very specific cybersecurity class context, where students gain advanced proficiencies (i.e. AP Computer Science), potentially earn college credits or professional accreditation, and may already lean towards careers in STEM or cybersecurity.

The teachers who taught dedicated cybersecurity courses (T5, T13, T15) emphasized their discussions with students about responsibly using the skills they learned. "What I teach them is just dangerous, and I tell them that all the time. They're learning to defend and attack" (T5). At the start of the school year, both the students and their parents were required to sign a form stating they understand the potential dangers in what they are learning, and promise to use their skills legally and responsibly.

Although classes covering ethical hacking tend to be very technical, they include discussions on current and historic events. For example, S5 noted that one of their first lessons concerned the 'white to black' spectrum of hacking, and the class learned from real-world examples throughout the semester. T15 emphasized that discussing the 'bad guy' hackers consistently hooked students' attention while teaching technical concepts like DDoS. "They all understood DDoS [from] Minecraft. So it was like, 'How can I stop it!? This needs to stop!'"

T5 had a very novel strategy to teach the ethical component of hacking in their cybersecurity class: lock picking. Lock picking is a skill with practical and ethical uses (entering one's own house after forgetting the key), and the potential to do harm (circumventing barriers to enter a restricted space): a tangible metaphor for hacking skills and the responsibility to use them only for good.

Cybersecurity and the state. Cybersecurity and civics/government teachers in particular discussed ethics in a context that might be called 'cybersecurity and the state' [65]. This entails concepts like national security, governmental control of their populations, intergovernmental conflict, criminal groups, and police/governmental authorities. T5 explicitly discussed cyber warfare, especially in the context of remarkable attacks, and the potential for non-state actors and relatively weak groups to inflict significant damage on the US using very little resources. Stuxnet [44] evokes technical and ethical questions about zero days, covert government cyber attacks, and asymmetric warfare.

> "I do love those moments where I can kind of blow their minds and, you know, talk about Stuxnet. [...] When that happened, that's game over. Now it's

> open season for everybody. That means it doesn't matter if you're the United States, or if you're a group somewhere in Thailand, the power is now equal. You can take down a nation now." (T5)

Teachers discussed authoritarian countries' control and suppression of their citizens. Several brought up cyberattacks believed to be sponsored by the Chinese government, as well as the Chinese government's use of facial recognition and related tracking systems, and Black Mirror-esque system of social credit scores [45], [68]. In discussing these technologies, T8 poses the question to students: "Would you want this in your school? Would you want this here?"

Several teachers, especially in social studies or cybersecurity courses, extensively discussed Russia's interference in the 2016 US elections. Teachers approached the topic as an attack on truth, the US, and democracy. Similar to privacy and personal safety issues, students often reacted with an ambivalence that concerned and frustrated teachers.

> "It is almost a shrug. They're interested in the technique of how it was done. For example, the Russian manipulations of the US elections, which we probe very deeply in a technical way and an ethical way, their reaction is not one of outrage. Their idea is that democracy has not been violated. I don't understand that." (T5)

For their part, most students, even those who had discussed the 2016 election hacks in classes, lacked a clear understanding of the events. S6 viewed it as a partisan issue ("I thought everyone was wrong, and no one was right") and S10 thought the election interference was untrue: "I didn't even know that was a thing. I thought that in itself was fake news, [the] Russian hackers. That did actually happen?"

Finally, teachers addressed ethical dilemmas involving free speech and censorship (especially on social media), and a few covered whistle blowing in the context of NSA surveillance. T15 taught about steganography in laser printers, and how the US government used the technology to prosecute counterfeiters and whistle blowers. "Basically, that laser printer allows the serial number of each machine to be coated into these little yellow dots. They're really tiny little things, [...] but it's a trail back to you" (T15). T15 joked that it remained a good lesson, even though "most kids don't even have a printer at home anymore."

Cyber hygiene. Cyber hygiene refers to the practical behaviors individuals take to stay safe from cybersecurity threats. Teachers occasionally speak to students about these practices, and several interviewees noted that a short cyber hygiene lesson was required for new student orientation.

When discussing cyber hygiene, teachers sometimes brought up predators or used the metaphor of 'stranger danger' [5]. For example, teachers tell students (especially younger ones) not to speak to strangers online, and certainly not to meet them in real life. Librarians and those responsible for computer labs stress using strong passwords, not sharing them, and logging out of school PCs when not in use. Similar to how teachers viewed teens' apparent lack of concern for privacy, several teachers expressed some exasperation at their inability to make students care about cyber hygiene practices. A younger teacher, T15, recounted their own cyber hygiene lessons and how they fell short, connecting that to the present.

> "I know I had countless 'cyber safe' lessons and 'stay safe online'. And it was presented in such a dry and kind of elementary fashion. And I think today's students got that same thing, 'Never talk to strangers online!' Which you shouldn't do. But they do anyway." (T15)

Almost half of students (S3, S7, S10, and S11) described cyber hygiene lessons they had in school as overly basic and just common sense. However, they also noted concern for young children being exploited by predators or hurt in social media 'challenges', and their own and their peers' mixed records on using safe online practices. S7, for example, had to contend with a person who cracked their weak Google password and sent uncouth messages to their contacts.

Concurring with the prior literature [17], [54], most interviewed teachers and students agreed that students need better cyber hygiene: "When they followed the link, it was asking them to put their social security number. And I'm like, 'You guys, don't do that!'" (T11) On the other hand, several students emphasized their savvy in navigating their social networks of choice. They learned from friends or personal experience rather than school.

S4 and S5 learned about phishing attacks in school, and S9 and S11 learned about them from paid summer courses. Each of these students said they remember the main ideas well, and appreciated the combined approach to teach cybersecurity and cyber hygiene practices together. This success echoes previous findings, which suggest hands-on phishing training can be effective [43], [69].

> "My teacher gave out two worksheets about phishing scam, and then also the DDoS attacks. And then she also put together a Google slide presentation and [...] two to three minute videos, that shows how those things work, and how to prevent yourself from getting trapped in those schemes. [...] So it's more like a prevention warning for students like, Hey, if you see an email like this, [...] you know that it's a cybersecurity risk." (S9)

4.2. Strategies and Resources Used (RQ2)

Teachers employed a great assortment of traditional and more novel teaching methods to teach cybersecurity and AI ethics. The teacher's choice of method relied on factors including the unique characteristics of the topic, interests and capacities of students, and their own skills and knowledge.

The most traditional teaching method consisted of the teacher leading a lecture or presentation, then a discussion, then assigning homework consisting of reading some material, and answering questions. Most teachers tried adamantly to avoid this, saying that giving students independent time for reading, writing, and reflecting resulted in "spacing out" more often than effective learning.

Teachers considered projects, (hands-on) activities, labs, and exercises to be the most successful in terms of keeping students on-task and motivated, and facilitating the best learning. The exercises themselves usually entailed some mixture of 'the technical' and 'the ethical' in cybersecurity and AI. Teachers also saw case studies very positively, especially to present ethical dilemmas in a real-world context.

Discussions. Discussions are spontaneous or regularly occurring dialogues, and can be a part of any other teaching strategy, or used by themselves. The goals of discussions include fostering critical thinking skills, recognizing ethical ambiguity, and considering multiple perspectives.

Ethics discussions occur in a number of formats including storytelling, roleplay, or Socratic seminar. Teachers often use some variant of the following formula: present a current event, especially involving new and emerging technologies; note an ethical dilemma from the event; facilitate student discussion, considering multiple perspectives; and ask students what we/they should do about it. Essentially, this resembles a case study approach for building ethical decision-making skills [25].

Current events discussions, while typically the domain of social science, also occur in the more technical courses. T15 made every Friday 'current event day', and T5 began every day with a 'cyber briefing', which focused on cybersecurity events in the news.

Sometimes discussions accompanied a reading or video (from short clips to full-length movies). T7 and T13 showed parts of the documentary "The Social Dilemma" [56] to spur conversations on privacy. Many teachers noted that videos help to get students' attention and keep them engaged.

Students, too, were very fond of videos as a learning tool generally or to facilitate discussion, provided they are not too long. S8 and S9 recommended CrashCourse, a YouTube series. "I really like watching Crash Course videos because it's very short, to the point. And it's animated!" (T8).

Several teachers used sci-fi and horror stories alongside discussions on technology ethics. T8, a literature teacher, described surveillance capitalism [79] with a metaphor.

> "We're using the text Frankenstein as a way of talking about monsters. And what do we do with monsters? Who do we blame - the creator?" (T8)

Technical (with coding). Technical (with coding) refers to topics taught in a way that requires reading and writing code. Due to the technicality of these exercises, they mostly occur in dedicated computer science classes and may last multiple class sessions. Generally, these activities aim to teach students ethical hacking skills.

Examples included: (1) Write programs to simulate cyber attack/ defense; (2) Develop a password cracker; (3) Design secure and accessible websites using HTML; (4) Write secure and accessible software; (5) Penetration testing; and (6) Various hacking exercises using command line.

Technical (without coding). Technical (without coding) refers to activities that teach about a technical issue, but don't require special technical skills of the students, typically because of a readily available tool. These tend to be short activities or projects that may occur in one or a few class periods. Part of the goal of these activities is to show students that they can better understand very technical concepts that affect them, even without more advanced computer proficiencies.

Examples included: (1) Train a machine learning program to recognize faces with/without a medical mask using Google's Teachable Machine; (2) Design an AI chat bot using Juji to help with a social problem; (3) Test their password strength with a website; (4) Check if accounts have been compromised using haveibeenpwned.com; and (5) Create assistive technologies using 3D printers.

Several teachers were very excited to share tools that they use, and noted constantly searching for new ones.

Gamified approach. The gamified approach is essentially a scored game, test, or challenge [39]. The examples described mostly correspond with media literacy, and teaching students to think critically about what they see or read online. 'Gamified" can refer to students competing against themselves or one another. The goal tends to be teaching students about complex topics in a fun, engaging, and memorable manner.

Examples included: (1) SpotTheTroll.org, where students attempted to distinguish real from fake Twitter profiles; (2) Spot the deep fake, guessing which video clips are deep fakes; (3) Spot the fake person, distinguishing images of the faces of real people from those created by AI; (4) Compete in a class-wide 'Shark Tank' styled competition to design a product without copyright infringement.

Content creator approach. The content creator approach allowed students to express themselves using some medium. Typically this consists of projects that require multiple class sessions or out of class time. The goal with this approach is to teach students about ethical consumption and creation of content and information.

> "We did a challenge a few years back where classes could make videos about media security and things like that. And those teachers then told us anecdotally, Yeah, they really got into it, and they really came away with some understanding of it. [...] It's kind of playing into what they want to do anyway, which is to create and to post and to be seen and heard." (T4)

Examples included: (1) Create an informational video clip about self-driving cars using WeVideo; (2) Create a public service announcement about a harm associated with AI; (3) Run a social media page for the school; (4) Create announcements or tutorials; (5) Create a digital comic about an AI dilemma using Pixton; (6) Design a 'museum exhibit for humanity', showing future humans what it means to be human at present.

Hands-off approach. The hands-off approach is when teachers step back and allow students to learn and do work by themselves at their own pace. The level of independence

varies, and both teachers and students noted that not all students effectively use independent time.

For S3 and S7, this meant independent time doing readings and exercises with Khan Academy. S3 said the Khan Academy exercises were part of a dynamic lesson on web development. For S7, the course A.P. Computer Science Principles was essentially a semester sitting in silence and working on Khan Academy content alone.

> "There are more cons than pros [with this approach]. It was just sitting around reading the articles. So I didn't retain anything. It was not that engaging, and I didn't get the stuff explained to me because, for some reason, that topic had no videos at all." (S7)

This was a rather extreme example. S7 speculates that the reason for the teacher's hands-off strategy is that they were a last minute replacement for someone better qualified.

Several teachers emphasized the importance that students discover on their own, lead class themselves, or execute projects of their own design. Two teachers stated that class projects which will actually see use are effective extrinsic motivators that connect well to empathy development.

T9 stressed a nuanced "lead from behind" approach, allowing students more agency in the learning process. In describing a project on AI ethics, they stated:

> "How are they forming their own knowledge? It has to be through them being able to critically think about the subject matter. [...] Listen - kids have amazing ideas. I realized we don't ever give them the opportunity to really talk about it. So yeah, it puts them in the driver's seat and gets them to really critically think about it and how it applies to their lives." (T9)

4.3. Remaining Challenges (RQ3)

Generational differences. Several teachers and students noted difficulties arising from generational differences. The main issues seem to be (1) different understandings and expectations of privacy, and (2) many (especially older) teachers lacking credibility on internet-related topics.

Most teachers believed their students were not concerned enough about threats to their personal privacy.

> "They're like, 'I share my location with my family now anyway." [...] It's also kind of tricky, because you don't want to turn them into doomsday conspiracy theorists." (T15)

T9 emphasized that their students grew up in a world post 9/11 and post Patriot Act: "They don't have that context of what it was like before. They don't have any context of what it's like to not have social media."

Additionally, teachers are usually playing catch-up for technology and social media important to their students. Teachers voiced both excitement and exasperation with the rapid pace of technological and social change, and several noted their students tend to adopt new technologies faster than they do. This has made it difficult to design lessons that remain relevant for students in upcoming years.

Furthermore, this lack of familiarity makes it more difficult to teach cybersecurity/AI ethics in an engaging and meaningful way. For example, discussing social media centering on Facebook and Twitter is less than ideal considering that high school age students seldom use them. Contrarily, relatively few teachers are intimately familiar with the platforms their students do use frequently (TikTok, Snapchat, Instagram, Discord). S1 reflected on the issue:

> "It feels like the teachers don't know as much as we do, so it's hard to take them seriously. Like, I understand these people have many decades more knowledge than I do. But it also feels like they don't have the same level of [knowledge of] what's going on. And then on another level, they just don't know the kinds of nuances about Snapchat safety, Discord safety, and like, Instagram problems. These aren't really things that appear on the news that often, and if they're not themselves on the social media platform, it would be harder for them to know about these issues." (S1)

Student attitudes. Teachers often expressed a struggle to inspire an appropriate level of awareness and concern in their students in topics like cyber hygiene, personal autonomy, and data privacy. Many teachers described their students' overconfidence in their own ability to spot threats, which ultimately leaves them susceptible to security threats. T15 contrasted their students' lack of interest in personal safety with genuine interest in hacking and other types of cybersecurity issues. One probable reason is that online safety inevitably entail "Don't-do-this-isms". Students seem to immediately tune out such messages:

> "The last thing that a high schooler wants, or even an adult wants, is to be lectured at, and told, like, you can't post this or don't do this with your phone, cuz then for sure it's 'Okay, Boomer."' (T4)

An alternative explanation could be that students are tired of hearing about the risks, and would rather hear about practical solutions. One example is dealing with malware.

> "I would have preferred more on how to get rid of viruses than how not to open spam emails. Because not opening spam emails is kind of obvious. We even saw - you open a spam email, now you have a million viruses. They didn't tell us how to get rid of that. Sometimes when you install antivirus software, it gives you more viruses." (S3)

Teachers also voiced concern that their students are not wary enough of information online, and thus vulnerable to mis/disinformation. For example, most students dismiss the idea that their worldview is impacted by what recommender systems show them, or that they might fall for fake news. While most teachers saw this as aloofness or naivety, T8 took a less critical view:

> "I think that's something that takes a lot of time and understanding to develop, to think about how you participate within systems and how systems

influence you [...]. That's a developmental thing. I don't think it's naive." (T8)

T8 emphasized a general problem, supported by several other teachers, that while students recognize the importance of treating people decently online, they are not cognizant of the impact of online content on people. It is simply an area where most students fail to recognize their own cognitive limitations or empathize with others. Generally, students do not see "content as possibly harmful. Like when we talk about deep fakes. I think they're gonna think it's cool, but I don't think that they're gonna go, oh, that's an issue." (T8) This same attitude is likely related to students' failure to understand the impact of fake news and disinformation on themselves and others. As T11 simply stated, "They feel like that's not going to impact them".

Finally, and particularly with topics relating to information/media literacy, teachers said that students resent the burden of considering if a source is reputable, verifying a claim with multiple sources, and properly citing references.

> "For them, everything is always about speed. How quickly can this be done? And so the thoughtfulness that's required of them is off-putting and frustrating." (T4)

Students generally stated that they were very much interested in the easiest path towards their end goal (a good grade). S8 acknowledged that fact checking and proper citations are 'tedious but also crucial'.

Parents and politics. Several teachers discussed the need to tread carefully when addressing ethical issues with any appearance of political tilt. As illustration, T4 and T6 had to fill out a Freedom of Information Act request from a conservative Super PAC concerning whether the school's curricula included "critical race theory". Some teachers were nervous that their school board meetings would experience disruptive tactics from upset parents.

> "I think teachers nowadays are a little bit more gun shy about talking about some stuff [...] The last thing we need right now with everything we're dealing with is a pissed off parent saying 'How dare you expose my child to blah blah?"' (T4)

This challenge is closely related to epistemological norms, as topics like fake news, disinformation, and misinformation are closely related to identity politics in today's hyper-partisan atmosphere. For example, a teacher from a more conservative area (T5) said some parents approached them over teaching students about the 2016 election hacks. While the election interference is a well-established fact, former President Trump and many of his adherents continually assert that Russian meddling did not occur and was fake news; a claim that Politifact named its 2017 lie of the year [4]. T5 smiled recounting one incident:

> "I get parents coming up to me. Not often, but sometimes. But [the students] definitely talk to their parents about what we discussed in class. And every once in a while, there's 'Hey, what are you telling my kid about?' Well, I'm not telling 'em anything - we're just talking." (T5)

Students were also aware of this issue, with S10 speculating that fears of angry parents precludes discussions on controversial topics.

> "I think our school has moved away from discussions in person about that, but we are encouraged to write papers about it that reflect our own or maybe even the other side's opinions. [...] Maybe it's an Iowa thing, or maybe it's just my school, but classroom wise, we don't have a lot of discussions regarding super controversial topics, because then that means angry parents emailing." (S10)

Curricula. Several teachers mentioned time restrictions, due to required coverage of other topics and focus on standardized exams. In a few cases, teachers expressed the will to further build cybersecurity/AI ethics into their curricula, but a lack of class plans and ready-to-use resources, like those in the 'Technical (without coding)' category above. T6 spoke of the need to "work cybersecurity, media, and information literacy into what they're already doing", and is interested in any help they can get.

At times, the multidisciplinarity of cybersecurity/AI ethics makes it difficult to ascertain who is responsible to teach it. Although every teacher and student believed discussing social media ethics to be important, busy teachers might stick to required course material and hope that other teachers pick up the topic. This is even true of teachers tasked with teaching cybersecurity, like T15. Also of note, T15 teaches in Wisconsin: a state without K-12 requirements for digital citizenship or media literacy [46].

> "I intentionally don't talk about a lot of social media in my classes, because honestly, it's a time issue. [...] [Social media] is more like - maybe that's more of a social studies thing." (T15)

Students, too, felt that curricula restricted their ability to learn about cybersecurity and cyber hygiene.

> "The extent that our school goes to teach about cybersecurity is having a strong password and not sharing it with others. There's not much education within the classes, because there's just so much other material to go through." (S10)

On the other hand, T4 was glad to see their state (Illinois) begin requiring media literacy for high schoolers in fall 2022. "We're excited that it's a requirement because it's kind of giving more weight to the things that we've already been wanting to do" (T4).

COVID-19 fallout. The majority of teachers discussed two problems in teaching during the pandemic: socialization problems, and virtual learning problems. While these problems are general, they particularly impacted teachers' efforts to engage students in ethical discussions.

> "The freshmen are a hot mess. I think it was 70% of our fights this year have been freshmen. It's anecdotally true for every teacher I talk to - these kids don't know how to be in person again." (T4)

Teachers considered virtual learning hit-or-miss. Traditional classrooms allow teachers to use management structures like rules and seating arrangements to create an en-

vironment for students to maintain focus, but virtual classrooms entail a myriad of distractions that teachers cannot control [53]. Cheating was especially problematic for foreign language teachers, who could not prevent students from using Google Translate. This relates to an ethical dilemma identified in the literature: balancing students' privacy and exam integrity during the pandemic [6].

T8 observed that while social media was a lifeline for students during the pandemic, it also left students feeling more antsy and less able to calmly reflect and learn.

> "[Social media] provides instant gratification and response. [But] real classroom interactions are slower. For a lot of my kids it's really hard." (T8)

Lack of qualified personnel. Several teachers noted an acute lack of qualified cybersecurity teachers.

> "I actually teach cybersecurity to other teachers. [...] A lot of cybersecurity teachers are coming in because they're the old math teacher, or they're the old driver's ed teacher. And cybersecurity is so hot right now. They're just pulling people into it, and they have no idea what they're doing." (T5)

A few teachers considered the technicality of topics as a barrier in their own classrooms. This highlights the potential difficulties non-technical teachers can face in teaching cybersecurity and AI ethics.

> "How technical do you get? I'm an English teacher - with my level of expertise, how much can I make sure that kids actually understand 'what is a recommendation algorithm?"' (T8)

Accessibility and inclusion. A few teachers noted difficulties relating to accessibility and inclusion for students with disabilities, in the special education program, and girls.

The teacher of students with visual impairment, T14, stated that a braille reader was not allowed with the school's computer system. This was one of many frustrations that their students have to deal with, which discourage technical endeavors and careers.

> "The braille display needs to connect, and [they] have to log in, and put the password. And the school, whatever security, did not allow her to have that device be connected to her email system. So I had to go through the loops in my district to get her email ID set up." (T14)

One librarian (T4) was tasked with developing media literacy, as this is a new requirement in their state. As part of this process, they surveyed teachers in their school on their thoughts. "Special Ed teachers said they know it's important, but how can we gear this down for all levels and abilities to understand and have access to?" (T4).

Gender balance and recruiting girls was a significant challenge for all teachers who taught elective computer science, as well as the students. T15, a cybersecurity teacher and a woman, is struggling to improve gender balance in her class, which currently stands at a 9-1 ratio of boys to girls. S4 and S9 were both the only girls in their Cybersecurity and AP Computer Science Principles courses, respectively. Neither said they were personally bothered very much, but they do worry about others.

> "Sometimes no one wants to partner with me. But it's still pretty cool because I'm really interested in it, so it doesn't bother me as much. And also my teacher is really inclusive. [...] But it can definitely be challenging for people signing up because they're like, hey, my friends aren't signing up for this. Like, it's just gonna be me." (S9)

S10 also stated they felt hesitation to pursue tech studies due to stereotypes of their race/ethnicity. In spite of their interest in cybersecurity: "I also kind of didn't want to play into the stereotypes that all Indian people are in IT."

5. Discussion

This work extends existing literature [19] on K-12 cybersecurity education. We used in-depth interviews with teachers and students, uncovering new challenges and details about how cybersecurity and AI ethics topics are taught.

Three main takeaways emerged. First, high school teachers in non-technical courses cover topics in cybersecurity/AI ethics. Second, the way we teach cyber hygiene is failing to make high schoolers safer. Last, some teachers are hesitant to approach epistemic norms in cybersecurity/AI, as these topics have become heavily politicized, and parents are increasingly activist about topics their children learn.

Multiple domains of cybersecurity/AI ethics. We observe that cybersecurity and AI ethics transcend the computer science classroom. Teachers in non-technical classes like ELA and social studies readily facilitate cybersecurity and AI ethics discussion with engaging content and probing questions. These domains have a longer tradition of ethics education than computer science [52], [57], making it natural for them to discuss contemporary current events as ethical case studies. Technology ethics issues are increasingly salient in current events, which means any discussion of current events is likely to include such topics.

An important benefit of the multidisciplinary approach to cybersecurity/AI ethics relates to accessibility. Teachers can leverage conversations on current events to discuss ethics, without any requirement for technical savvy, or for the school to have dedicated cybersecurity teachers or IT hardware. Only the larger and better-funded schools, especially selective enrollment or "magnet" schools, seem to have specialized computer science courses, and a variety of advanced placement (AP) courses. However, virtually all schools have civics and ELA classes in the core curriculum.

Ultimately, the multidisciplinary approach means more students can access education about these pertinent topics. Cybersecurity/AI ethics are inherently interdisciplinary, and some have already criticized an overly technical approach to ethics in computer science pedagogy [61]. There may well be benefits to integrating and contextualizing cybersecurity and AI ethics in existing courses.

However, this also entails a trade-off; computer science teachers are much better equipped to combine technical and

ethical content than their ELA and social science counterparts. English teachers are excellent at teaching epistemic norms, but we should not expect them to suddenly become experts on machine learning and cyberwarfare.

The failure of cyber hygiene education. Cyber hygiene is a critical topic to avoid a host of cybersecurity disasters [17]. However, the way we teach cyber hygiene needs a complete rethinking. Basic computer safety seems to be a general requirement for high schoolers, whether on an annual basis, or as part of Freshman orientation. Yet teachers, with the exception of some computer science teachers, seem to treat online safety as a required box-ticking exercise. Neither teachers nor students appreciate this approach.

This is one domain where the computer science teachers did notably better than their counterparts in ELA and social studies. Computer science teachers went in greater depth, combining cybersecurity and cyber hygiene, and incorporating hands-on exercises, which have proven effective in cybersecurity education in non-school settings [43], [69]. For example, instead of emphasizing the need to not write down passwords - something students have heard (and often ignored) since middle school - T12 and T5 taught about how phishing emails and other social engineering works. These lessons went in depth, showed examples, incorporated fun hands-on exercises, and had immediate relevance to students. S4, S5, S9, and S11 agreed that such lessons were memorable and useful, and still guide their online practices. Such an approach does not fall under the "don't-do-this-isms" often encountered in cyber hygiene. "Don't-do-this-isms", where necessary, are best communicated with compelling examples and stories with immediate relevance to the high school audience. Computer science teachers seem better equipped to facilitate these lessons [76]. This is somewhat concerning given that many high schoolers have limited possibilities to study computer science.

Students seem to hold paradoxical opinions on cyber hygiene lessons. Students say online safety is "crucial" and many students do not follow safe practices. On the other hand, the lessons are patronizing, "common sense", or irrelevant. For example, "don't talk to strangers online" is probably not realistic or age appropriate advice for high schoolers, who are accustomed to using social media and accessing online communities. "Don't share your passwords" is not always reasonable, considering families share subscription plans. It is not merely that students ignore such advice; it harms the credibility of the teacher and lesson.

Finally, computer safety lessons do not focus on privacy in a sense that concerns high school students [49]. Students are relatively unconcerned about having their identity and banking information stolen, as most of them have no assets and little autonomy. If privacy were presented differently, such as "How would you feel if an angry ex could log into your Instagram?", or other age-appropriate hypotheticals, lessons may have more impact. Lessons could also focus on concrete ways students can protect their privacy and security, which may reduce learned helplessness [35].

Activist parents and hyper-polarization. We have presented evidence that current events discussion is crucial in cybersecurity/AI ethics education. This creates a dilemma - how do we discuss current events in the classroom when they are so politically charged? The problem is important to consider now, as more states are adding media literacy as a required component of high school curricula [46].

In contrast to earlier work [9], we have found that high school teachers are working hard to increase emphasis on critical analysis of fake news. Yet, some teachers have difficulty approaching epistemological norms such as media and information literacy. Several teachers explicitly stated they want to avoid hot-button issues that could anger parents and invite conflict. This is not only a cybersecurity/AI ethics issue, but one that affects all discussion of current events.

Unfortunately, this may represent a silencing effect in education. As S10 stated, their Iowa school has moved away from open discussions on controversial topics to individual writing assignments. This should be concerning, given the importance of an informed populace and pluralism in democracy. At present, Iowa has no legislation requiring K-12 instruction in digital citizenship or media literacy [46].

Relatedly, students struggle to discern biased/partisan news and fake news/disinformation, and generally fail to recognize the potential harms of online content. This implies we need to find a better way to educate about such topics in a way that doesn't come off as inflammatory or partisan.

5.1. Implications for design and policy

Students and teachers were unanimous on the importance of cybersecurity/AI ethics education. However, they also indicated the present shortcomings that they have experienced. Here we present suggestions for educators, practitioners, and policy-makers to consider.

Experts should develop more nifty tools. Teachers raved about tools like Google's Teachable Machine, MIT's Moral Machine, and games to spot deep fakes. Students were 'absorbed', 'fascinated', and 'really came away with an understanding'. However, teachers often struggled to find tools that were free, engaging, up-to-date, and readily available to teach a given topic. T15 noted that tools and case studies date quickly, so teachers have a constant need for up-to-date material.

Furthermore, certain tools (like SpotTheTroll.org) are excellent, but have limited content and replay value. It may be worth revisiting and expanding such tools. The non-technical teachers particularly appreciated tools that make complex topics accessible. Students with less technical background will benefit by more easily learning concepts, without simultaneously needing to learn new tools [20].

Teachers may benefit from resources that help them discuss cybersecurity/AI ethics using current events as case studies. For example, most teachers struggled to connect with students about the ethics of privacy in current events (i.e. data leaks, surveillance). This is one area where practitioners can consider developing materials and guidelines.

Finally, make it as easy as possible for teachers to find resources. High school teachers' time is already very

overstretched, so it is unlikely they will find resources if they are not well-publicized and easily found.

Overhaul cyber hygiene. Students are not uninterested in online privacy and safety; they spend a huge part of their lives online. For example, S3 wished they had learned how malware works, and what to do if you suspect you might have some. While some teachers are required to teach cyber hygiene, they are often unqualified to do so [76], and treat it as a box-ticking exercise. One outcome is that students feel patronized and ignore what they hear. At present, cyber hygiene lessons come off as tone deaf, and mostly serve to damage teachers' credibility ('OK, boomer').

One promising approach is to combine cyber hygiene and cybersecurity ethics concepts together when possible, especially in the computer science classroom. Computer teachers are better equipped to go in-depth, use hands-on exercises, and address both the technical and ethical aspects of online safety. The lessons on how phishing attacks are one example of a good practice that students internalize, and having learned, become safer.

Do it in any context. Cybersecurity and AI ethics can and should be discussed outside the computer science context. Social science and language arts classes have especially good thematic fits for these topics (e.g., current events and national security, sci-fi and journalistic integrity). No technical requirements exist for such content. Moreover, these classes can well utilize the content creator approach, playing into what many high schoolers love doing.

We were struck that despite lacking official courses on AI and cybersecurity ethics, teachers understand the importance of talking about these topics in other contexts. Our evidence shows that discussions and exposure of these topics can be fruitful in courses like ELA and social studies. This could imply the benefits of integrating and contextualizing these topics in existing courses [61]. This is an important consideration for future research, given debate on how important it is to impose new requirements for cybersecurity/AI into already packed high school curriculum.

Make a personal connection. Teachers should pay serious attention to engaging students effectively, remembering 'the hook'. Many teachers described frequent struggles to keep students focused and productive - especially students in the freshman or sophomore class, and especially in the context of a 'captive audience' (i.e. required course). To mitigate the problem, they may open class by presenting a dramatic event or concept. Finding what works requires knowing the class. For example, students understand privacy very differently than their teachers, so teachers should carefully consider how to make privacy education personally and practically meaningful to students.

Show don't tell. An additional way to engage students is to demonstrate something and let students try it themselves. For example, a lecture on password safety is abstract, but students could also use HaveIBeenPwned.com and see exactly how and when their personal data were exposed. A PowerPoint on Russian trolls may be useful, but using SpotTheTroll.org probably forms a stronger impression.

Consider technology-agnostic course material. Teachers described students as very accepting of change, and students inevitably take up technologies that teachers are unfamiliar with. In some cases, it may be more effective to develop technology agnostic course materials. For example, a lesson on TikTok may be appropriate now, but perhaps not in a few years. Teachers should consider framing the ethics and providing (historical) perspective, but allowing students to determine the specific technology of focus.

Work within their attention spans. Lessons should be adapted for the students' age and maturity. Long lectures and readings will rarely be effective - especially for younger students. Independent time works well for some, but not others. Teachers need to know and respect students' limitations.

One simple strategy is to use short, high-quality video clips. An additional strategy might be fast(er) transitions between activities. For example, a teacher might combine a short YouTube video, a hands-on activity in small groups, and a short wrap-up discussion in an one-hour period. This ensures that students with diverse learning styles can benefit.

5.2. Limitations

Our interviewee pool may not be generalizable to the whole US, given the states' leading role in implementing high school education, the sample size, and difficulty in recruiting from lower-income and rural schools. Only three teachers taught classes exclusively focused on cybersecurity, and none taught classes exclusively focused on cybersecurity or AI ethics. This is not necessarily a limitation, as it may simply reflect that most high schoolers learn about cybersecurity and AI ethics tangentially, if at all. It proved difficult to clarify the meaning of cybersecurity and AI ethics without naming specific examples. By giving some examples (i.e. the Russian cyberattacks on the 2016 US election, cyber hygiene practices), we may have imposed a particular framing of the topic. Finally, most students attended actual computer science classes, so their answers focused on technical rather than social science or humanities courses.

6. Conclusion

Cybersecurity and AI ethics education is essential to prepare the next generation's decision-makers to confront an uncertain future. It is therefore critical to understand how cybersecurity and AI ethics are taught in American high schools, and how teaching strategies can improve.

We have shown that teachers in multiple disciplines include cybersecurity and AI ethics in their curricula. We found teachers leverage a variety of traditional and novel strategies for cybersecurity and AI ethics education, and encounter diverse challenges. Finally, we provided evidence of the need for more and better quality cybersecurity/AI ethics instruction, and practical suggestions to this end.

Future work should check if our findings hold true in the broader US context. It would also be helpful to delve further into how teachers can best introduce AI/CS ethics into already-packed curricula.

Acknowledgments

We thank Chuck Gardner and Charlene Cooper from cyber.org, and Genevieve Patterson of University of Colorado Denver, for their invaluable inputs to this work. We further thank the anonymous reviewers and shepherd for their constructive feedback. This work was supported in part by NSF grant 2114991.

References

[1] 117th Congress (2021-2022). Actions - h.r.4691 - 117th congress (2021-2022): K–12 cybersecurity act of 2021, 2021.

[2] Safinah Ali, Blakeley H. Payne, Randi Williams, Hae Won Park, and Cynthia Breazeal. Constructionism, ethics, and creativity: Developing primary and middle school artificial intelligence education. In *International workshop on education in artificial intelligence K-12 (EDUAI'19)*, pages 1–4, 2019.

[3] Rebecca P. Ang and Dion H. Goh. Cyberbullying among adolescents: The role of affective and cognitive empathy, and gender. *Child Psychiatry & Human Development*, 41(4):387–397, 2010. Publisher: Springer.

[4] Angie Drobnic Holan. 2017 Lie of the Year: Russian election interference is a 'made-up story', December 2017.

[5] Karla Badillo-Urquiola, D. Smriti, B. McNally, E. Bonsignore, E. Golub, and P. Wisniewski. Co-designing with children to address "stranger danger" on Musical. ly. In *SOUPS, The Fourteenth Symposium on Usable Privacy and Security*, 2018.

[6] David G. Balash, Dongkun Kim, Darika Shaibekova, Rahel A. Fainchtein, Micah Sherr, and Adam J. Aviv. Examining the examiners: Students' privacy and security perceptions of online proctoring services. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 633–652, 2021.

[7] Rachel KE Bellamy, Kuntal Dey, Michael Hind, Samuel C. Hoffman, Stephanie Houde, Kalapriya Kannan, Pranay Lohia, Jacquelyn Martino, Sameep Mehta, and Aleksandra Mojsilovic. AI Fairness 360: An extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias. *arXiv preprint arXiv:1810.01943*, 2018.

[8] Malika Bendechache, Irina Tal, P. J. Wall, Laura Grehan, Emma Clarke, Aidan Odriscoll, Laurence Van Der Haegen, Brenda Leong, Anne Kearns, and Rob Brennan. AI in My Life: AI, Ethics & Privacy Workshops for 15-16-Year-Olds. In *13th ACM Web Science Conference 2021*, pages 34–39, 2021.

[9] Hal Berghel. Lies, Damn Lies, and Fake News. *Computer*, 50(2):80–85, February 2017. Conference Name: Computer.

[10] Karl-Emil Kjær Bilstrup, Magnus H. Kaspersen, and Marianne Graves Petersen. Staging reflections on ethical dilemmas in machine learning: A card-based design workshop for high school students. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pages 1211–1222, 2020.

[11] Jane Blanken-Webb, Imani Palmer, Sarah-Elizabeth Deshaies, Nicholas C. Burbules, Roy H. Campbell, and Masooda Bashir. A case study-based cybersecurity ethics curriculum. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*, Baltimore, MD, August 2018. USENIX Association.

[12] Melissa Block. The clear and present danger of Trump's enduring 'Big Lie'. *NPR*, December 2021.

[13] Wayne C. Booth. The ethics of teaching literature. *College English*, 61(1):41–55, 1998. Publisher: JSTOR.

[14] Jason Borenstein and Ayanna Howard. Emerging challenges in AI and the need for AI ethics education. *AI and Ethics*, 1(1):61–65, February 2021.

[15] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006. Publisher: Taylor & Francis.

[16] Emanuelle Burton, Judy Goldsmith, and Nicholas Mattei. Teaching AI Ethics Using Science Fiction. In *Aaai workshop: Ai and ethics*. Citeseer, 2015.

[17] Ashley A. Cain, Morgan E. Edwards, and Jeremiah D. Still. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42:36–45, October 2018.

[18] Kevin Matthe Caramancion. An Exploration of Disinformation as a Cybersecurity Threat. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, pages 440–444, March 2020.

[19] EdWeek Research Center. The state of cybersecurity education in k-12 schools: Results of a national survey. June 2020.

[20] Peter Chapman, Jonathan Burket, and David Brumley. PicoCTF: A Game-Based computer security competition for high school students. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, San Diego, CA, August 2014. USENIX Association.

[21] Suzanne S. Choo. *Teaching Ethics through Literature: The Significance of Ethical Criticism in a Global Age*. Routledge, London, July 2021.

[22] Markus Christen, Bert Gordijn, and Michele Loi. *The ethics of cybersecurity*. Springer Nature, 2020.

[23] David De Cremer and Garry Kasparov. AI should augment human intelligence, not replace it. *Harvard Business Review*, 2021.

[24] John Dewey. *Democracy and Education: An Introduction to the Philosophy of Education*. Macmillan, 1923.

[25] David Dittrich, Michael Bailey, and Sven Dietrich. Building an active computer security ethics community. *IEEE Security & Privacy*, 9(4):32–40, 2011. Publisher: IEEE.

[26] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. The teaching privacy curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, pages 591–596, 2016.

[27] Stephan Ellenwood. Resisting Character Education: From McGuffey to Narratives. *Journal of Education*, 187(3):21–43, 2007. Publisher: SAGE Publications Sage CA: Los Angeles, CA.

[28] Steven Feldstein. *The global expansion of AI surveillance*, volume 17. Carnegie Endowment for International Peace Washington, DC, 2019.

[29] Stacey Forsyth, Bridget Dalton, Ellie Haberl Foster, Benjamin Walsh, Jacqueline Smilack, and Tom Yeh. Imagine a More Ethical AI: Using Stories to Develop Teens' Awareness and Understanding of Artificial Intelligence and its Societal Impacts. In *2021 Conference on Research in Equitable and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*, pages 1–2. IEEE, 2021.

[30] Heidi Furey and Fred Martin. AI education matters: a modular approach to AI ethics education. *AI Matters*, 4(4):13–15, January 2019.

[31] Natalie Garrett, Nathan Beard, and Casey Fiesler. More Than "If Time Allows": The Role of Ethics in AI Education. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pages 272–278. Association for Computing Machinery, New York, NY, USA, February 2020.

[32] Benjamin Gleason and Sam von Gillern. Digital Citizenship with Social Media: Participatory Practices of Teaching and Learning in Secondary Education. *Journal of Educational Technology & Society*, 21(1):200–212, 2018. Publisher: International Forum of Educational Technology & Society.

[33] Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, and Owain Evans. Viewpoint: When Will AI Exceed Human Performance? Evidence from AI Experts. *Journal of Artificial Intelligence Research*, 62:729–754, July 2018.

[34] Nancy Green. An AI Ethics Course Highlighting Explicit Ethical Agents. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, pages 519–524. Association for Computing Machinery, New York, NY, USA, July 2021.

[35] Kristin Haltinner, Dilshani Sarathchandra, and Nicole Lichtenberg. Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. In Kristin Haltinner, Dilshani Sarathchandra, Jim Alves-Foss, Kevin Chang, Daniel Conte de Leon, and Jia Song, editors, *Cyber Security*, Communications in Computer and Information Science, pages 69–81, Cham, 2016. Springer International Publishing.

[36] Daniel Hart and Gustavo Carlo. Moral development in adolescence. *Journal of research on adolescence*, 15(3):223–233, 2005. Publisher: Wiley Online Library.

[37] H.L.A. Hart. *The Concept of Law*. Clarendon Press, Oxford, 2nd edition, 1961.

[38] Tenghao Huang, Faeze Brahman, Vered Shwartz, and Snigdha Chaturvedi. Uncovering Implicit Gender Bias in Narratives through Commonsense Inference. *arXiv:2109.06437 [cs]*, September 2021. arXiv: 2109.06437.

[39] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, 12(1):150–158, 2018.

[40] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Game based Cybersecurity Training for High School Students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, SIGCSE '18, pages 68–73, New York, NY, USA, February 2018. Association for Computing Machinery.

[41] Gali Katznelson and Sara Gerke. The need for health AI ethics in medical school education. *Advances in Health Sciences Education*, 26(4):1447–1458, October 2021.

[42] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–21, 2017. Publisher: ACM New York, NY, USA.

[43] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[44] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011. Publisher: IEEE.

[45] Fan Liang, Vishnupriya Das, Nadiya Kostyuk, and Muzammil M. Hussain. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4):415–453, 2018. Publisher: Wiley Online Library.

[46] Media literacy now. Your state legislation, Apr 2022.

[47] Sana Maqsood. *The Design, Development and Evaluation of a Digital Literacy Game for Preteens*. PhD Thesis, Carleton University, 2020.

[48] Alice Marwick, Claire Fontaine, and Danah Boyd. "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society*, 3(2):2056305117710455, 2017. Publisher: SAGE Publications Sage UK: London, England.

[49] Alice E. Marwick and Danah Boyd. Networked privacy: How teenagers negotiate context in social media. *New media & society*, 16(7):1051–1067, 2014. Publisher: Sage Publications Sage UK: London, England.

[50] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019. Publisher: ACM New York, NY, USA.

[51] Seumas Miller. Freedom of Political Communication, Propaganda and the Role of Epistemic Institutions in Cyberspace. In *The Ethics of Cybersecurity*, pages 227–243. Springer, Cham, 2020.

[52] Thomas Misco. The moral nature of elementary social studies methods. *Theory & Research in Social Education*, 33(4):532–547, 2005. Publisher: Taylor & Francis.

[53] Sharon Mistretta. The New Netiquette: Choosing Civility in an Age of Online Teaching and Learning. *International Journal on E-Learning*, 20(3):323–345, July 2021. Publisher: Association for the Advancement of Computing in Education (AACE).

[54] James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele Ajayi, and Philip Anderson. Investigating teenagers' ability to detect phishing messages. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 140–149, 2020.

[55] Illah Reza Nourbakhsh. AI ethics: a call to faculty. *Communications of the ACM*, 64(9):43–45, September 2021.

[56] Jeff Orlowski. The Social Dilemma, 2020.

[57] Susan Pass and Wendy Willingham. Teaching Ethics to High School Students. *The Social Studies*, 100(1):23–30, January 2009. Publisher: Routledge _eprint: https://doi.org/10.3200/TSSS.100.1.23-30.

[58] Christopher Peterson and Martin E. P. Seligman. Learned Helplessness and Victimization. *Journal of Social Issues*, 39(2):103–116, 1983. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1540-4560.1983.tb00143.x.

[59] Jean Piaget. *Judgement and reasoning in the child*. Routledge, 2002.

[60] Thomas P. Quinn and Simon Coghlan. Readying Medical Students for Medical AI: The Need to Embed AI Ethics Education. *arXiv:2109.02866 [cs]*, September 2021. arXiv: 2109.02866.

[61] Inioluwa Deborah Raji, Morgan Klaus Scheuerman, and Razvan Amironesei. You Can't Sit With Us: Exclusionary Pedagogy in AI Ethics Education. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '21, pages 515–525, New York, NY, USA, March 2021. Association for Computing Machinery.

[62] Lynn Revell and James Arthur. Character education in schools and the education of teachers. *Journal of Moral Education*, 36(1):79–92, March 2007. Publisher: Routledge _eprint: https://doi.org/10.1080/03057240701194738.

[63] Pedro Ortega Ruiz and Ramon Minguez Vallejos. The role of compassion in moral education. *Journal of moral education*, 28(1):5–17, 1999. Publisher: Taylor & Francis.

[64] Jim Rutenberg, Jo Becker, Eric Lipton, Maggie Haberman, Jonathan Martin, Matthew Rosenberg, and Michael S. Schmidt. 77 Days: Trump's Campaign to Subvert the Election. *The New York Times*, January 2021.

[65] Eva Schlehahn. Cybersecurity and the State. In *The Ethics of Cybersecurity*, page 205. Springer, 2020.

[66] Donald Schneider and Others. *Expectations of Excellence: Curriculum Standards for Social Studies. Bulletin 89*. National Council for the Social Studies, 3501 Newark St, 1994.

[67] Dawn E. Schrader and Dipayan Ghosh. Proactively Protecting Against the Singularity: Ethical Decision Making in AI. *IEEE Security Privacy*, 16(3):56–63, May 2018. Conference Name: IEEE Security Privacy.

[68] Chris Fei Shen. Social credit system in China. *City University of Hong Kong*, 2019.

[69] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99, 2007.

[70] Carie Smith. *Cyber Security, Safety, & Ethics Education*. PhD Thesis, Utica College, 2018.

[71] Ji Soo Song and Divya Sridhar. How states can support the next generation of digital citizens, Jun 2021.

[72] Bernd Carsten Stahl and David Wright. Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation. *IEEE Security Privacy*, 16(3):26–33, May 2018. Conference Name: IEEE Security Privacy.

[73] Behnam Taebi, Jeroen van den Hoven, and Stephanie J. Bird. The Importance of Ethics in Modern Universities of Technology. *Science and Engineering Ethics*, 25(6):1625–1632, December 2019.

[74] Zeynep Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008. Publisher: Sage Publications Sage CA: Los Angeles, CA.

[75] Ibo van de Poel. Core values and value conflicts in cybersecurity: beyond privacy versus security. In *The Ethics of Cybersecurity*, page 45. Springer, 2020.

[76] Justin Wang, Dennis Brylow, and Debbie Perouli. Implementing Cybersecurity into the Wisconsin K-12 Classroom. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 312–317, July 2019. ISSN: 0730-3157.

[77] Steven A. Wartman and C. Donald Combs. Reimagining Medical Education in the Age of AI. *AMA Journal of Ethics*, 21(2):146–152, February 2019. Publisher: American Medical Association.

[78] M. Wolfe. Childhood and privacy. Altman, I. and Wohmill, JF Children and the Environment, 1978.

[79] Shoshana Zuboff. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile books, 2019.

Appendix

TABLE 2. OVERVIEW OF SCHOOLS PRESENTED IN OUR STUDY

Alias	Area	Type	State	Teacher count	Student count
SCH1*	Suburban	Public/"Laboratory"	IL	3	3
SCH2	Suburban	Public	IL	3	0
SCH3	Suburban	Public	IL	1	0
SCH4	Urban/Suburban	Public	CO	1	0
SCH5	Rural/Suburban	Public	WI**	1	0
SCH6	Suburban/Urban	Public/Charter	CO	1	0
SCH7	Urban	Public	NJ	1	0
SCH8	Suburban	Public	CO	1	0
SCH9	Suburban	Public	CO	1	0
SCH10	Suburban	Public	CO	1	0
SCH11	Rural/Suburban	Public	CO	1	0
SCH12	Suburban	Public Technical School	UT	1	2
SCH13*	Urban	Public	IL	0	1
SCH14*	Suburban	Public	TX	0	1
SCH15*	Urban	Public	IL	0	1
SCH16	Suburban	Public	IA**	0	2
SCH17	Urban	Public	UT	0	1
			SUMS	16	11

* indicates schools with selective admissions.
** indicates a state with no requirement for digital citizenship/media literacy instruction at K-12 level [46].
School 12 is a special program for high school students run by a technical college.
Rural, Suburban, and Urban were stated by interviewee or inferred by interviewer.

Interview script for teachers

This has been lightly edited for length and privacy.

Introduction

[REDACTED]

Interview questions

- Could you tell us a little bit about yourself?
- What's your educational background?
- How long have you been a high school teacher?
- What do you usually teach?
  - Do you have any training in teaching topics related to cybersecurity, AI, or ethics?
- Could you tell us a little about your school, in terms of size, socio-economic diversity in the student body, etc.?
  - How many students do you usually teach?
- Have you ever covered anything related to [ethics / cybersecurity / AI / emotional or social skills] in your teaching?
- If so, could you tell us what you covered related to [ethics / cybersecurity / AI / emotional or social skills]?
  - Could you give us a concrete example?
  - How was your experience teaching that topic?
  - What was your students' reaction to the topic?
  - Did you give any in-class exercise or home assignment on that topic? Could you give us a concrete example?
- Do you think high school students should be introduced to cybersecurity/AI ethics? One goal is to improve their awareness of tech ethics issues that affect themselves.
- Another goal is to improve their awareness of tech ethics issues that affect others (e.g., younger children). Could you elaborate on any specific topics you think the students should be introduced to?
- For example, we intend to cover smart toys, social media, mobile apps, and online games.
- *Explain what we plan to do - design hands-on labs to educate high school students to be more knowledgeable of and empathetic to people who might be affected by AI technologies or cybersecurity issues, especially young children in the context of social media, smart toys, online games and mobile apps.*
  - Have you taught anything related to these topics?
  - If so, what has been your experience?
  - Do you have any suggestions for us in designing these educational materials?
- Do you have suggestions on promoting the students' empathy toward others, particularly vulnerable populations such as younger children?

Interview script for students

This has been lightly edited for length and privacy.

Introduction

[REDACTED]

Interview questions

- Before we get started, could you tell us a little bit about yourself?
  - Where do you live?
  - What year are you?
  - What type of things do you do for fun?
  - What are you most interested in at school?
- Could you tell us a bit about your high school?
  - Do you know about how many students are there?
  - How many students are usually in your classes?
  - Is it selective enrollment?
  - Does your school offer A.P. courses? Which ones?
  - Would you say it's diverse? How so?

- Do you talk about current events in any of your classes?
  - Could you tell us a bit about what classes do that, and how it goes?
  - How do you and your classmates feel about it?
  - Is it interesting to talk about stuff in the news?
- Have you ever learned anything related to cybersecurity or AI in your classes?
  - (Offer examples if helpful)
  - Could you tell us what was covered, and in what class?
  - How was this material taught? (slideshow, lecture, activity, etc.)
  - Did you have any in-class exercise or home assignment on that topic?
  - How was your experience learning that topic?
  - How did other students' react to the topic?
  - What were the good things about what you learned, and how it was taught?
  - Do you have any suggestions on what could be improved and how?
- Have you ever talked about fake news, disinformation, misinformation, or that sort of thing in any classes?
  - (Offer examples if helpful)
  - How did that go, and how did you feel about it?
- Have you ever learned anything related to ethics/morality in your classes?
  - (Offer examples if helpful - ethical dilemmas like free speech vs. fake news or disinformation, privacy vs. security, etc.)
  - Could you tell us what was covered, and in what class?
  - How was this material taught? (slideshow, lecture, activity, etc.)
  - Did you have any in-class exercise or home assignment on that topic?
- In any of your classes, do you ever talk about how students use social media and cell phones?
  - How did the conversations go?
  - How did you and your classmates react? Was it interesting or engaging?
  - Was it strange talking with teachers about that sort of thing, especially since they're in a different generation?
- Do you think high school students should be introduced to cybersecurity/AI ethics?
  - If so, how early?
  - What do you think are the best ways to learn this sort of thing?

Recruitment materials

These are the recruitment texts we used to recruit the majority of interviewees. The versions presented were rewritten after it appeared our initial text was too narrow. These have been lightly edited for length and privacy.

Recruitment material for teacher interviewees

[PERSONALIZED INTRODUCTION AND PROJECT DESCRIPTION REDACTED]

As part of this project, we are interviewing high school teachers with relevant experience. Most high schools do not have a dedicated curriculum for AI and cybersecurity ethics, so we are interested in reaching high school teachers with experience teaching related topics. A few examples of teachers we've interviewed include (but aren't limited to):

- *Computer science teachers*, whose topics include safe password usage, safe usage of websites and apps, how AI works, how AI is used (self-driving cars, smart speakers, targeted advertising, facial recognition, surveillance), coding skills, etc.
- *Civics teachers*, whose topics include social media's role in recent elections, fake news, disinformation, media bias, ethics of current events, etc.
- *Librarians*, whose topics include using the internet to find reputable information, fake news, disinformation, general computer skills, etc.

If you have relevant experience, we would very much appreciate the opportunity to interview you over Zoom for about 30 minutes at a convenient time.

Recruitment material for student interviewees

[PERSONALIZED INTRODUCTION AND PROJECT DESCRIPTION REDACTED]

As part of this project, we are interviewing high schoolers about their experiences learning these topics. Many high schools don't have a specific curriculum for AI and cybersecurity ethics, so we are also interested in students who've learned related topics including:

- *Computer science*, with topics including safe password usage, safe usage of websites and apps, how AI works, how AI is used (self-driving cars, smart speakers, targeted advertising, facial recognition, surveillance), coding skills, etc.
- *Civics/digital citizenship*, with topics including social media's role in recent elections, fake news, disinformation, media bias, ethics of current events, etc.

If you are a student with relevant experience, we would very much appreciate a 30-60 minute Zoom at a convenient time. As a small thank you for your time, we are offering $15 Amazon gift cards.