QUESTIONNAIRE

UNITED STATES OF AMERICA

David MAIMON, PhD

Associate Professor in the department of Criminology and Criminal Justice,
Georgia State University

1. Introduction

Please read carefully before answering the questionnaire

The RAYUELA project is aimed at protecting children in their online interactions. For this purpose, the project will develop a "game", which will present the children with realistic scenarios relating to the following cybercrimes/cyber-facilitated crimes:

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.
- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behaviour online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.
- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.
- ***Human trafficking with a cyber component*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.
The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.
A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.
One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.
The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?
- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?

- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

Importantly, we want to know both the legal rules and policies which are implemented in practice, and their effect on the **real enforcement situation**. If you have knowledge about the effects of current policies on crime rates by minors and on the crime rates for OG, CB, MD and HT, this would be of interest.

We are specifically interested in **case law** that illustrates the "why and how" of certain legal rules, principles and policies in practice. Case law will help us illustrate the similarities and differences between jurisdictions and is therefore *essential***.** Please ensure to have a good amount of case law processed in your answers.

In addition, we want input on **international legal instruments and international cooperation** relevant for cybercrime, and in particular for cybercrime perpetrated by minors. What happens when cybercrimes is perpetrated in a cross-border context? What are the legal rules in place for cooperation with authorities from other countries, and how does this work out in practice (issues, problems, etc.)?

Lastly, we are interested in some **statistical information on cybercrime** in your country and cybercrime by minors specifically.

The purpose of this questionnaire is to help you provide this information for your jurisdiction.

2. Questions relating to OG, CB, HT and MD with minors as victims

Question 1: Is online grooming punishable by law in your country?

Answer: Both Federal and state legislation has been created in the USA to allow child sexual grooming to be punishable as a standalone criminal offense, even if contact sexual abuse does not take place (Pollack and Maclver2015). The federal enticement statute under 18 U.S.C. § 2422 of the U.S. Criminal Code reads as follows:

> (a) Whoever knowingly persuades, induces, entices, or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both.
>
> (b) Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

In United States v. Gagliardi, Frank Gagliardi was charged with attempt to entice, induce, or persuade a minor to engage in illegal sexual activity, in violation of 18 U.S.C. § 2422 (b). On July 7, 2005, Gagliardi, then sixty-two years old, entered an Internet chat room called "I Love Older Men" and initiated an instant-message conversation with "Lorie," an adult government informant posing as a thirteen-year-old girl under the screen name "Teen2HoT4u." During this initial conversation, Gagliardi tried to verify that Lorie was in fact thirteen years old and broached the topic of sex. On August 29, 2005 Gagliardi contacted “Lorie” again and had the first of many online conversations in which he expressed his desire to have sex with her. On September 1, 2005, Lorie indicated that she was "scared" to meet Gagliardi alone and suggested that he contact her thirteen-year-old friend Julie. "Julie" was in fact FBI Special Agent, who was working in collaboration with the informant. Gagliardi suggested that the two girls come together to meet him, and arranged to meet with them in lower Manhattan on the morning of October 5, 2005. FBI agents placed the pre-arranged meeting place under surveillance and arrested Gagliardi as he waited in his car. On May 16, 2006, Gagliardi was convicted by a jury in violation of 18 U.S.C. § 2422 (b), and was sentenced to imprisonment term of sixty months.

In addition to the federal statute, 42 states have enacted their own anti-grooming legislation (Chetosky, 2019), while other states do not have legislation specific to sexual grooming. Those 42 states are: Indiana, Kansas, Louisiana, Maine, Maryland, Massachusetts. Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Verminy, Virginia, Washington DC, West Virginia, and Wyoming (Kaylor, et al 2022). In several states, including Alabama, Alaska, Connecticut, Florida, Idaho, Illinois, Louisiana, Minnesota, Missouri. Nebraska, New Hampshire, New Mexico, North Carolina, Texas, Utah, and West Virginia the enticement, solicitation, or luring, must involve the use of an electronic device, computer, Internet, or text messaging (Kaylor et al 2022).

The varying definitions of sexual grooming across jurisdictions pose a serious challenge to the application of grooming laws and can lead to discrepancies in prosecution and sentencing. This is further complicated by the fact that many identified sexual grooming behaviors in and of themselves (e.g. hugging, buying gifts, giving attention) can present as normal adult/child interactions. Moreover, proving intent is especially evident in cases of online child sexual grooming. For example, some offenders may seek to engage in sexualized online chats with minors with no intention of moving the online interactions to criminal acts such as sending or receiving sexual material or in-person sexual contact (Gilden, 2016). Therefore, several experts argue that engaging in fantasy-driven sexualized

conversation online may not constitute a preparatory action for in-person sexual contact, and consequently, shouldn't be prosecuted under sexual grooming legislation.

For example, thirty-four-year-old Patrick Naughton, had sexual correspondence for over nine months with KRISLA over online platforms. At some point Naughton, traveled from Seattle to meet with KRISLA which was an undercover FBI agent in Santa Monica. The FBI arrested Naughton and charged him (along other crimes) with the intent to have sex with a minor and using the Internet to try to arrange to have sex with a minor. In his trial, Naughton argued that he thought the person he was about to meet was a grown woman who shared his "daddy/daughter" fantasy and was "playing the part" of a young girl." The jury believed his "fantasy defense" and acquitted him of these charges (Yamagami 2000).

References:

Chetosky, K. K. (2019). Minnesota v. Muccio: The Constitutionality of Minnesota's Sexual Grooming Law. *Nw. UL Rev. Online*, *114*, 1.

Gilden, A. (2016). Punishing sexual fantasy. *Wm. & Mary L. Rev.*, *58*, 419.

Kaylor, L. E., Winters, G. M., Jeglic, E. L., & Cilli, J. (2022). An analysis of child sexual grooming legislation in the United States. *Psychology, Crime & Law*, 1-19.

Pollack, D., & MacIver, A. (2015). Understanding sexual grooming in child abuse cases. Child L. Prac., 34, 161.

United States v. Gagliardi, 506 F.3d 140, 147

Yamagami, D. (2000). Comment, Prosecuting Cyber-Pedophiles: How Can Intent Be Shown in a Virtual World in Light of the Fantasy Defense?, 41 Santa Clara L. Rev. 547.

Question 2: Is cyberbullying punishable by law in your country? Please take into account a broad understanding of cyberbullying (cyber/online stalking, harassment, sexual harassment)?

Answer: There are no federal statutes criminalizing cyber bullying, cyber stalking or cyber harassment in the United States (Bossler 2020). However, several federal laws prohibit sending abusive or harassing messages. For example, 18 U.S.C § 875 (Interstate Communications) prohibits the use of communication devices via interstate or foreign communication to (1) demand a ransom for the release of a kidnapped person; (2) send a message with the intent to extort money; (3) threaten to injure a person; or (4) threaten to damage property. The statute can be used to prosecute an offender who lives in the same state as the victim if the Internet was used. Penalties for violation of this statue range from a fine and up to 2 years in prison for threats to damage property and extortion and up to 20 years in prison for demanding ransoms and threatening physical injury.

Similarly, Title 47 U.S.C § 223 (Obscene or Harassing Telephone Calls in the District of Columbia or in Interstate or Foreign Communications) forbids the use of telecommunication devices to carry out harassing behaviors (Brenner 2011). Specifically, individuals are not allowed to use telecommunication devices in order to make, create, solicit, or initiate requests that are obscene or that involve child sexual exploitation materials with the intent to annoy, threaten, abuse, or harass others. It is also prohibited to withhold one's identity and use these devices to annoy, abuse, threaten, or harass someone (Bossler 2020). Punishment for violation of this title could vary from a fine to two years imprisonment.

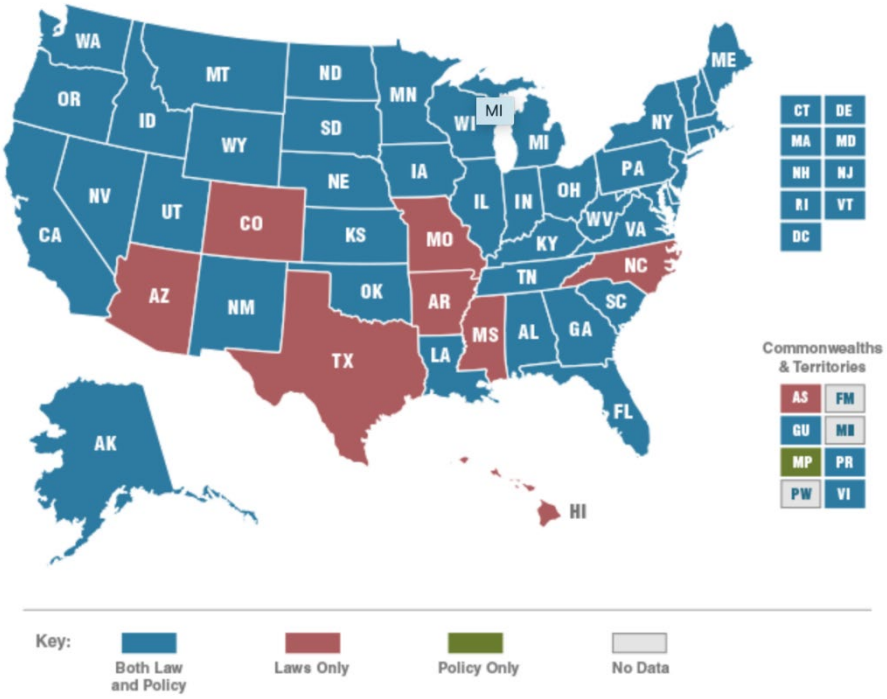
Similarly, 18 U.S.C. § 2261A details how interactive computer services cannot be used for any activities that cause a person to feel substantial emotional distress or places that person or their family in reasonable fear of death or serious bodily injury (Bossler 2020). This statute also criminalizes interstate travel with the intent to kill, injure, threaten, or harass another person and place them or their family in fear of death or serious bodily harm. Penalties for these offenses may range from 5 years in prison if

only a threat is made, up to 10 years if serious bodily injury occurred as a result of a weapon, 20 years if the victim was permanently disfigured or received a life-threatening injury, and up to a life sentence if the victim died in relation to the threat (Brenner 2011).

In United States v Elonis (2016), Anthony Elonis posted threating messages with either the purpose of threatening his ex-wife, or with knowledge that she would interpret the posts as threats. The case started with Elonis's wife leaving their home with their children. Elonis had trouble at work, leaving early and crying at his desk. Days later, Elonis began posting statements about "sinister plans for all my friends," and, concerning his wife. Followed by issuance of a protective order, Elonis posted statements concerning shooting at his wife's house, using explosives, and "I'm checking out and making a name for myself." After being visited by federal agents, he posted statements about blowing up SWAT members. Anthony Elonis was convicted of violating 18 U.S.C. § 875(c), which prohibits transmitting in interstate commerce a communication containing a threat to injure the person of another

Although there are no specific Federal Cyber bullying laws, almost every state has legislation addressing cyberbullying and the roles of schools to prevent bullying (https://www.stopbullying.gov/resources/laws). Figure 1 presents a map with all the USA states and their adoption of anti-bullying laws and policies. Hinduja and Patchin (2018) report that forty-eight states recognize the terms "cyberbullying" or "electronic harassment" in their state bullying legislation, and that forty- four states provide criminal sanctions for electronic harassment. Moreover, forty-five states require schools to punish bullying behaviors. In seventeen states there are also statutes which indicate that off-campus bullying can also be sanctioned (Hinduja and Patchin 2018). This provides an avenue for states to punish cyberbullying which often happens off-campus. Although some opponents of these statutes argue that schools should not have jurisdiction over behavior that does not occur on their physical property, proponents argue that bullying victimization greatly affects students' academic performance and attendance because of its impact on students' mental health and emotional state.

Figure 1. USA States Anti-Bullying Laws and Policies (source https://www. stopbullying.gov/resources/laws)



Similarly to state-level practices pertaining to cyber bullying, most US states have statutes criminalizing cyberstalking, online harassment, or both (see https://www.haltabuse.org/resources/laws/index.shtml). These statutes allow for the prosecution of cyberstalking or harassment in which the offender used electronic communications to stalk or engage in a pattern of threatening behaviors Forty states have

statutes which criminalize the use of CMCs to annoy or harass the victim; these do not require a credible threat. The violations of these offenses are considered either misdemeanors or felonies depending on the seriousness of the offense.

The major challenge in applying these statues is the with the requirement to prove that a credible threat has been made either to a person or property. In the United States v. Alkhabaz (1997), the court ruled that the communication needed to generate actual fear or concern for safety. According to Bossler (2020) In this case "Abraham Jacob Alkhabaz, also known as Jake Baker, wrote graphic stories describing fictional rapes, tortures, and murders and posted them on Usernet. In one of the stories, he described the raping and killing of a female character who shared the same name as one of his fellow classmates. The female classmate complained to the University of Michigan police department who investigated the offense and brought in the FBI because of the interstate aspect of the online communication. Baker was arrested on six counts of communicating threats to kidnap and injure a person under § 875. His case was dismissed, however, by a judge stating that there was insufficient evidence that Baker would act out his fantasies. The government appealed the decision, but the decision was upheld (p.19)".

Another major challenge to the application of these laws, is that their enforcement must comply with the First Amendment. Specifically, the First Amendment imposes two key limitations on threats and harassment law. The "true threat" doctrine teaches that the government cannot punish threats that in context are mere advocacy or political hyperbole, as these are protected speech under the First Amendment. Threats can be punished only if they are "true threats." A second First Amendment limit on these laws considers incitement of illegal conduct- speech that encourages other to act, rather than suggest the speaker intent to take action (Kerr 2018).

In United States v. Carmichael (2004), Leon Carmichael was arrested after informants told Drug Enforcement Administration Task Force agents that they were employed by Carmichael to assist in his marijuana and money-laundering operation. After his arrest, Carmichael posted a website asking for information that he could use in his defense. The final version of the website had pictures of the informants and agents under the word "wanted" in big red letters. Beneath the pictures, the website had contact information for Carmichael's attorneys. At the bottom of the page, there was statement suggesting that the website "is definitely not an attempt to intimidate or harass any informants or agents, but is simply an attempt to seek information. The Carmichael Case will not be a 'closed door' case." The government sought a protective order against the website, arguing that Carmichael's website made unlawful threats against informants and agents. The court held that Carmichael's website was not a true threat and was protected by the First Amendment.

References:

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (Ed.), Cybercrime: The investigation, prosecution, and defense of a computer-related crime (3rd ed., pp. 15–104). Raleigh: Carolina Academic Press.

Hinduja, S., & Patchin, J. W. (2018). State bullying laws. Cyberbullying Research Center. Accessed 22/5/2022 at: https://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf

Kerr, Orin S. (2018). *Computer crime law*. Thomson/West.

Question 3: When would misinformation and deception online constitute a criminal offence in your country? In other words, what potential qualifications could apply to willful misinformation and deception on the internet?

Answer: The First Amendment guarantees freedoms concerning religion, expression, assembly, and the right to petition. As such it protects Americans' rights to freely exchange ideas—even false or controversial ones. This poses a serious challenge to any attempt to prevent the spread of misinformation in the USA. Therefore, the main legal recourse against the spread of fake news is to file a defamation lawsuit. Defamation is a tort that encompasses false statements of fact that harms another's reputation. Defamation could be classified as libel (written defamation) or slander (oral defamation). Since tort law is mainly a state law in the USA, it differs to some extent throughout the fifty states and the District of Columbia. Importantly though, when filing a defamation suit in tin the USA the falsity of the charge must be proved by the plaintiff (Johnson 2016).

Acknowledging the role of the internet and websites in serving as potential platforms for misinformation, the United States, section 230 of the Communications Decency Act of 1996 (47 U.S.C.S. § 230(1)(c)(1) (2016) reads as follows: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." According to Johnson (2016), this provision has been broadly interpreted as banning defamation claims against Internet services and website operators. For example, in Schneider v. Amazon.com, Inc., the court ruled that an online bookseller was not responsible for libelous comments posted about an author's (plaintiff Rhawn Joseph) books.

Moreover, American courts have held that the immunity awarded by the Act is not lost neither if a website operator edited some of the information that has been posted, nor if the person who posted the information could not be identified. For example, in Batzel v. Smith,
the United States Court of Appeals for the Ninth Circuit held that the operator of an anti-art-theft website, who posted an allegedly defamatory e-mail authored by a third party, and made only minor alterations to the e-mail, could not be considered a content provider who was subject to liability (Johnson 2016).

Finally, under section 230 of the Communications Decency Act, website operators do not have legal incentive to remove defamatory posts which were posted by a third party on their websites. In fact, "whether a website operator can be forced to disclose the identity of anonymous posters depends on the application of tests developed by the courts to determine whether disclosure will be judicially ordered. In many cases, disclosure is denied because there is a constitutional right to speak anonymously, and that right is not lightly abridged Johnson 2016, p.61)"

In addition to misinformation and fake news, online deception could also be manifested as online fraud. As of today, there is no designated federal statute in the United States which focuses on online fraud. Instead, tradition mail and wire fraud statutes are used to prosecute offenders who commit Internet-based fraud. 18 U.S.C. § 1341 specifics that mail fraud involves:

> "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed".

18 U.S.C. § 1343, makes it illegal to commit similar fraudulent activities by "wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." The penalties for wire and mail fraud are similar and range from a fine and/or imprisonment of up to 20 years (the sentence can be increased up to 30 years if a financial institution was involved).

Conspirators of online fraud can also be charged under 18 U.S.C. § 371, which reads as follows: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

Historically, the wire fraud statute has been used more often than the mail fraud statute when prosecuting online fraud (Bossler 2020; Brenner 2011). For example In USA v. Olaniyi, Olayinka Olaniyi_was convicted in federal court of conspiracy to commit wire fraud. This fraudster led a phishing scheme (along with other Nigeran nationals) that tricked employees at several American universities into sharing their computer log-in and password. Once he had that information, he used it to deposit payroll checks into bank accounts he controlled. Olaniyi also gained access to W2 forms and used them to file fraudulent tax returns. Similarly in United States v. Asri, plaintiff Himanshu Asri was prosecuted under the wire fraud, and conspiracy to commit wire fraud statutes. Asari admitted taking active part in a conspiracy to route American callers calls to call centers in India where call center operators falsely reasserted to victims that malware had been detected on their computers, and offered the victims purported computer protection services in exchange for payment.

Another relevant fraud statute is 18 U.S.C. § 1029. This statue makes it illegal to knowingly have the intent to defraud others using counterfeit or unauthorized access devices. According to the statute, "the term 'access device' means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)" (e) (1). Depending on the severity of the offense (e.g., number of access devices and economic costs), the penalty for a conviction can range up to 15 years; a previous conviction increases the penalty up to 20 years (Bossler 2020).

18 U.S.C. § 1029 was one of the statues used in *United States v. Ivanov* to prosecute a Russian national hacker who targeted USA companies and individuals. The government alleged that Aleksey Ivanov hacked into OIB's computer system and obtained key passwords (OIB collected and maintained customer credit card information). He then sent OIB a series of unsolicited emails demanding for money to make their systems secure. The government contends that Ivanovs extortionate communications originated from an email account at Lightrealm.com and Internet Service Provider based in Washington. It contends that while he was in Russia Ivanov gained access to the Lightrealm computer network and that he used that system to communicate with OIB also while he was in Russia. Ivanov was sentenced to 48 months in prison.

References:

Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003)

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (Ed.), Cybercrime: The investigation, prosecution, and defense of a computer-related crime (3rd ed., pp. 15–104). Raleigh: Carolina Academic Press.

Johnson, V. R. (2016). Comparative defamation law: England and the United States. *U. Miami Int'l & Comp. L. Rev.*, *24*, 1.

Joseph v. Amazon.com, Inc., 46 F. Supp. 3d 1095, 1106 (W.D. Wash. 2014

USA v. Olayinka Olaniyi, No. 18-14622 (11th Cir. 2019)

UNITED STATES v. ASRI Case No. 20-mj-70041-SK-1.

Question 4: What constitutes human trafficking and how is human trafficking facilitated by electronic means punished in your country? Are online grooming activities to find victims (e.g. lover boys) before the actual human trafficking punishable in itself? In addition, are these activities punishable as a separate crime if human trafficking does take place afterward?

Answer:

The Victims of Trafficking and Violence Protection Act of 2000 (TVPA) defines sex trafficking and clarifies that minors induced into prostitution are victims of sex trafficking regardless of the presence of force, fraud, or coercion. The TVPA also enhanced penalties for existing offenses such as slavery, peonage, and involuntary servitude, and established protections for trafficking victims and allowing non- citizen trafficking victims to remain in the U.S (Farrell and Cronin 2015). Section 1590 in the act pertains to trafficking with respect to peonage, slavery, involuntary servitude, or forced labor and reads as follows:

> `Whoever knowingly recruits, harbors, transports, provides, or obtains by any means, any person for labor or services in violation of this chapter shall be fined under this title or imprisoned not more than 20 years, or both. If death results from the violation of this section, or if the violation includes kidnapping or an attempt to kidnap, aggravated sexual abuse, or the attempt to commit aggravated sexual abuse, or an attempt to kill, the defendant shall be fined under this title or imprisoned for any term of years or life, or both.

Section 1591 pertains to sex trafficking of children or by force, fraud or coercion and reads as follows:

> (a) Whoever knowingly--
>
> > `(1) in or affecting interstate commerce, recruits, entices, harbors, transports, provides, or obtains by any means a person; or
> > `(2) benefits, financially or by receiving anything of value, from participation in a venture which has engaged in an act described in violation of paragraph (1), knowing that force, fraud, or coercion described in subsection (c)(2) will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act, shall be punished as provided in subsection (b).
>
> `(b) The punishment for an offense under subsection (a) is--
> > `(1) if the offense was effected by force, fraud, or coercion or if the person transported had not attained the age of 14 years at the time of such offense, by a fine under this title or imprisonment for any term of years or for life, or both; or

> `(2) if the offense was not so effected, and the person transported had attained the age of 14 years but had not attained the age of 18 years at the time of such offense, by a fine under this title or imprisonment for not more than 20 years, or both.

In addition to this federal act, every state (since 2003) has enacted laws establishing criminal penalties for human traffickers who seek to profit from forced labor or sexual servitude (see https://ndaa.org/wp-content/uploads/Human-Trafficking-3-3-2015.pdf)

Some traffickers contact their potential victims online (mainly over social networking sites such as Facebook). The techniques used by the traffickers and their assistants to gain trust vary widely, and include expressing love and admiration of the victim, promising to make the victim a star, and providing a ticket to a new location away from the victim's home (i.e. online grooming). The federal enticement statute under 18 U.S.C. § 2422 of the U.S. Criminal Code prohibits such activities (as discussed in Answer 1 above). The activities prohibited in this act are punishable independent of whether human trafficking was followed. Statue 18 U.S.C. § 2422 has been used in USA v. Evans to prosecute Justin Evans for his role in recruiting minors online and enticing them to engage in prostitution. The defendants arranged dates and supplied the underage girls with condoms for use on dates. Evans admitted using both a cellular telephone and a land-line telephone to entice Jane Doe to engage in prostitution,

18 U.S.C § 875 (Interstate Communications) is additional statues which criminalizes the use of communication devices via interstate or foreign communication to (1) demand a ransom for the release of a kidnapped person; (2) send a message with the intent to extort money; (3) threaten to injure a person; or (4) threaten to damage property. The statute can be used to prosecute an offender who lives in the same state as the victim if the Internet was used (Bossler 2020). The punishments for these offenses range from a fine and up to 2 years in prison for threats to damage property and extortion and up to 20 years in prison for demanding ransoms and threatening physical injury.

References:

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

Farrell, A., & Cronin, S. (2015). Policing prostitution in an era of human trafficking enforcement. *Crime, Law and Social Change*, *64*(4), 211-228.

UNITED STATES of America, v. Justin EVANS, 06-10907.

3. Questions regarding cybercrime or cyber-facilitated crime committed by minors

This section is aimed at understanding how cybercrime or cyber-facilitated crime committed by minors is dealt with in your jurisdiction. In particular we are trying to assess to what extent the rules and policies in place create leeway for minors who may not always be aware of when their behaviour is crossing a line. We are also interested to know the real enforcement situation. In addition to the general rules on the juvenile justice system and the punishment of minors, the 4 crimes of focus of RAYUELA are addressed, as well as two particularly relevant crimes committed by minors online: online piracy and hacking.

Question 5: How is crime committed by minors dealt with in your country, in general? Is there a specific juvenile justice system? If yes, please explain in detail how this works.

Answer: The underlying doctrine guiding the USA treatment of juveniles is of *parents patriae*, meaning that the state is the ultimate parent of the child. This means that as long as parents take care for at least the basic needs of their children, they are theirs to keep. However, when children are physically or

emotionally neglected or abused by the parents, the juvenile court may intervene and remove the children from the problematic environment. Under these circumstances, the doctrine of *in loco parentis* (which means that the state act in place of the parent) kicks in.

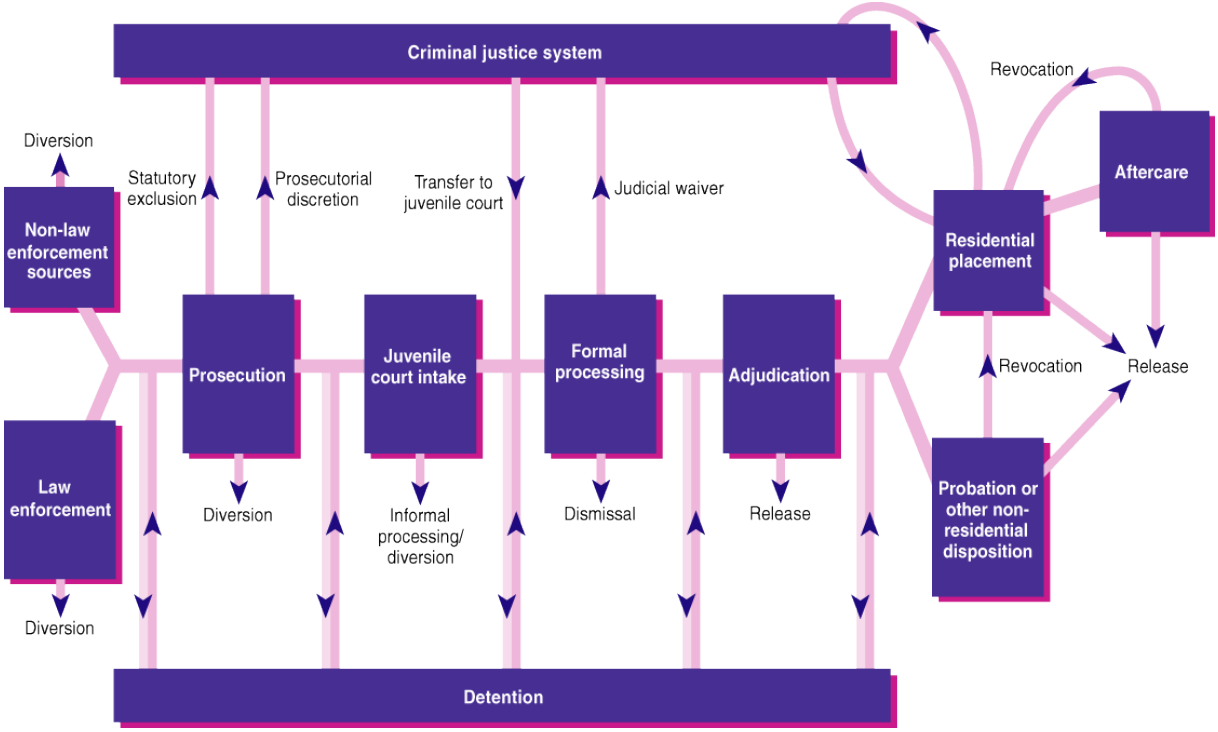
All in all, the prevailing philosophy of the USA criminal justice system toward juveniles is very different from its philosophy towards adults. Table 1 below describes the idealistic contrast between juvenile and adult criminal justice processes. Still, in situations where a juvenile commits a crime which is so heinous, he/she may not be eligible to the more lenient philosophy and jurisdiction of the juvenile court, and will be remanded to the custody of the appropriate adult court.

Table 1. the Ideals of Juvenile and Adult Criminal Justice Process (adopted from Peak and Everett 2017)

ADULT	JUVENILE
Adversarial procedure	Relatively amiable procedure
Individual responsibility to crime	Societal/family factors involved
Punishment is typically the goal	Rehabilitation is the goal
Arrest process	Petition
Trial-public	Hearing-private
Guilt or innocence	Guilt not the sole issue
Public record	Confidential record
Verdict	Decision
Sentence	Disposition

The four primary goals of the USA juvenile justice system are separation from adults, youth confidentiality, community based corrections, and individualized justice of minors. Most USA states' juvenile courts decisions are driven by the presumption of innocence, the presumption of the least amount of involvement with the system, and the presumption of the best interest of the minor. Figure 1 below presents the case flow diagram of the USA juvenile justice process.

Figure 1. Case Flow Diagram of the Juvenile Justice Process (source https://www.ojjdp.gov/ojstatbb/structure_process/case.html)



At the Federal level the Juvenile Justice and Delinquency Prevention Act (the "Act"), codified at 18 U.S.C. §§ 5031 to 5042 of Title 18, is used to governs both the criminal prosecution or the delinquent adjudication of minors in federal court. According to this act, a "juvenile" is a person who has not yet reached the age of eighteen at the time of the commission of the offense and is under twenty-one as of the time of the filing of formal juvenile charges. Therefore, a person who committed the offense before his eighteenth birthday but is over twenty one on the date formal charges are filed may be prosecuted as an adult (DeMarco 2001). Under the Act, there are three situations under which federal delinquency jurisdiction over a juvenile is assumed. First, where the state court lacks jurisdiction, or refuses to assume jurisdiction. Second, where the state does not have available programs and services adequate for the needs of juveniles. And third, where the crime is a federal felony crime of violence or one of several enumerated federal offenses, and there exists a sufficient federal interest to warrant exercise of federal jurisdiction.

Table 2 below presents data on the civil age of majority, the age of criminal responsibility, and the age in which a juvenile case can be transferred to adult court in the 50 USA states (source https://www.juvenilecompact.org/age-matrix. Each state has its own rules about mitigating/attenuating circumstances, and jurisdictional aspects in cross-border cases.

Table 2. Age matrix for 50 USA States

state	Civil Age of Majority	Age of Criminal Responsibility/Majority	Age Juvenile Case Can Be Transferred to Adult Court
Alabama	19	18	14 with a juvenile court hearing; 16 direct file for class A felonies
Alaska	18	18	16
Arizona	18		
Arkansas	18	18	14
California	18	16	16
Colorado	18	18	15
Connecticut	18	18	15
Delaware	18	ranges between ages 14-16 depending on the specific charge	14
District of Columbia	18	18	16
Florida	18	16	The juvenile offender must be at least 14 years old.
Georgia	18	17	13-17 for certain offenses
Hawaii	18	18	On/after 16 and alleged to have committed act that would constitute felony if committed by adult under certain circumstances. Minimum age on/after 14 & alleged to have committed act that constitutes a felony if committed by adult. See HRS 571-22.
Idaho	18	18	Generally 14 but for certain offenses in Idaho Code 20-509 (murder, rape, arson, etc.) there is no minimum age

Illinois	18		
Indiana	18	18 for all criminal offenses; 16 for certain felony offenses (see IC 31-30-1-4)	Upon waiver motion by prosecutor and finding of juvenile court: 12-16 for certain major felony offenses; no minimum age for felony offense and previous felony or non-traffic misdemeanor conviction (see IC 31-30-3)
Iowa	18	18	14
Kansas	18	10	14
Kentucky	The Juvenile Code does not contemplate a minimal age of criminality. Ten (10) is the minimal age for secure detention of a juvenile unless it is a capital offense. Must be at least thirteen (13) years of age in order to be declared as a JSO.	The age of 18 triggers adult court jurisdiction.	Must be at least fourteen (14) years of age., under circumstances outlined in KRS 640.010. Contact ICJ Office for more information.
Louisiana	18		
Maine	18	18	No minimum age for a bind over to adult court.
Maryland	21	14 for 1st Degree Murder and Rape, but normally 16	14 for 1st Degree Murder and Rape, but normally 16
Massachusetts	18	18	14
Michigan	18	18	14
Minnesota	18	18	14
Mississippi	18	18	13
Missouri	18	18	14
Montana	18	18	12
Nebraska	19	18	14
Nevada	18	18	13

New Hampshire	18	18	15
New Jersey	18	18	A discretionary and presumptive waiver can be used for youth age 15 and older that meet statutorily-delineated offense criteria set forth in NJ SA 2A:4A-26.1
New Mexico	18	18	14
New York	18	18	13
North Carolina	18	18	13
North Dakota	18	10	14 or older for serious offenses (Murder, Attempted Murder, Gross Sexual Imposition by force or threat of force, or kidnapping). A juvenile can ask for a voluntary transfer to adult court if both the juvenile and the parents agree.
Ohio	18	18	14
Oklahoma	18	18	13 to 15 (for Murder I)*some age 13-14 can become Youthful Offender Cases
Oregon	18	18	15
Pennsylvania	18	18	Automatic certification to adult court if murder. 15+ with the commission of certain crimes with a deadly weapon. 15+ charged with certain crimes and who have previously been adjudicated delinquent of certain crimes. Prosecutor can file motion to certify.
Rhode Island	18	18	No age limit if charge punishable by life imprisonment. 16 if charge is another felony. If under 16 with felony charge, youth may be certified to serve sentence in juvenile facility until age of majority & may transfer to adult facility or adult probation
South Carolina	18		
South Dakota	18	18	16
Tennessee	18	18	Depends on offense
Texas	18	17	14 for capital murder, agg controlled substance felony, or first degree felony; 15 for 2nd degree, 3rd degree, or state jail felony
Utah	18	18	14 and charged with murder, or attempted murder, or aggravated murder, or attempted aggravated murder
Vermont	18	14 - but only on certain offenses	16

Virgin Islands	18	18	14
Virginia	18	18	14
Washington	18	18	12
West Virginia	18	no minimum	14, unless other factors are present
Wisconsin	18	17	Any state criminal law violation age 15; certain offenses or circumstances age 14.
Wyoming	18		

As noted above, under certain circumstances, a juvenile's case may be transferred to adult status and the juvenile can be tried as an adult. In these situations, the case proceeds as any criminal case would with the exception that *a juvenile under eighteen who is transferred to adult status may never be housed with adults, either pretrial or to serve a sentence*. For example in *Breed v. Jones* the U.S. Supreme Court reviewed the lower court's decision to transfer a juvenile defendant to be tried as an adult. In this case, Gary Jones, who was seventeen-year-old at the time, first appeared in a Juvenile Court in California for committing an act that, if committed by an adult, would have constituted the crime of robbery. After a hearing, the Juvenile Court determined that Jones should be tried as an adult in California Superior Court. Jones filed a writ of habeas corpus and argued that the adult criminal trial was an exercise of double jeopardy in violation of his due process rights under the Fifth Amendment, applied to the states through the Fourteenth Amendment. Jones's writ was successively denied by the Superior Court, the Court of Appeals, and the California Supreme Court. Jones was tried as an adult and found guilty of first-degree robbery.

References:

Breed v. Jones, 421 U.S. 519, 523 (1975) https://supreme.justia.com/cases/federal/us/421/519/

DeMarco, Joseph V. "It's Not Just Fun and War Games-Juveniles and Computer Crime." *US Att'ys Bull.* 49 (2001): 48.

Doyle, Charles. (2018) Juvenile Delinquents and Federal Criminal Law: The Federal Juvenile Delinquency Act and Related Matters. Congressional Research Services.https://sgp.fas.org/crs/misc/RL30822.pdf

Question 6: Are there specific rules or is there a specific policy that deals with cybercrime by minors as a special topic, acknowledging the special characteristics of crime by minors in the cyber environment, and the fact that minors may not knowingly or intentionally break rules (issues with criminal intent)? Even absent a written policy, are minors prosecuted for cybercrime in practice?

Answer: As far as I am aware, there are no specific rules and policies that deal with cybercrime by minors as a special topic in the USA. However, the same provisions in the criminal code which apply for the prosecution of juvenile delinquency are relevant also in the context of juvenile online crime (see answer 5). Importantly though, according to DeMarco (2001), in the context of typical computer crimes committed by juveniles, several factors will play in favor of transferring juvenile cases to adult status. Specifically, at the Federal level, the court should consider six factors to determine whether to grant a transfer a juvenile offender from a status of juvenile to adult:

(1) the age and social background of the juvenile
(2) the nature of the alleged offense, including the juvenile's leadership role in a criminal organization
(3) the nature and extent of the juvenile's prior delinquency record
(4) the juvenile's present intellectual development and psychological maturity

(5) the juvenile's response to past treatment efforts and the nature of those efforts
(6) the availability of programs to treat the juvenile's behavioral problems.

Since many computer delinquents come from middle-class or affluent backgrounds, commit their exploits with the assistance of other delinquents; and are extremely intelligent, there is a high probability of these cases to be trialed as adults. Moreover, some sophisticated computer criminals are barely under the age of eighteen, and may merit punishment as adults.

References:

DeMarco, Joseph V. "It's Not Just Fun and War Games-Juveniles and Computer Crime." *US Att'ys Bull.* 49 (2001): 48.

Question 7: Can minors be punished for online grooming in your country? I.e. the situation of a minor capable of providing sexual consent (e.g. 17 year-old) grooming a minor who has not reached the age of sexual consent (e.g. 13 years old) to meet up with the intent to perform sexual activities? Please focus not only on the specific crime of online grooming (which, if present as a separate crime in your jurisdiction, often requires an adult perpetrator), but also on other crimes that would punish the activities that constitute online grooming (i.e. the use of different strategies to force a meeting with the minor victim with the intent to perform sexual activities). If criminal sanctions could apply, are minors prosecuted in practice?

Answer: Minors are subjected to the same states' relevant statutes I described in Answer 1.

Question 8: Can minors be punished for purely online behaviour with a sexual intent when other minors are the victim? E.g. the situation where a minor perpetrator obtains sexually explicit material from the minor victim in order to sell this or to force the victim to do something. If criminal sanctions could apply, are minors prosecuted in practice?

Answer: The creation, distribution, possession, and viewing of pornography is legal in the United States, as long as the participants in the work and the consumer are of legal age (i.e., 18). Some content is considered illegal regardless of the age of the consumer if the pornographic content depicts minors, sex between humans and animals, or true-life rape or physical harm (as opposed to performing) (Bossler 2020). As such, sexting (which could be defined as, "the practice of sending or posting sexually suggestive text messages and images, including nude or semi-nude, photographs via cellular telephones or over the Internet" (Sweeny 2011, p. 952), could be viewed as the creation and distribution of self-made pornography is generally legal, unless it violates two conditions: either it involves sexual harassment, or the distributor and/ or receiver is a minor.

In some cases, the receivers of the sexual photos betray the trust of the original sender and disseminate the photos or videos in order to cause emotional harm to the original sender. This behavior became known as "revenge pornography". Finally, in other cases, the recovers of the sexual material could engage in sextortion, which employs non-physical forms of coercion to extort sexual favors from the victim (Greenberg 2019). Still there is no national Federal law in the United States that specifically addresses sexting, revenge porn, or sextortion (Bossler 2020). This is unfortunate since although some sextortion cases potentially can be prosecuted under general extortion, harassment or child pornography laws, courts have dismissed strong cases because criminal statutes do not specifically address these specific online behaviors. Still, the most common federal statute applied to prosecute sextortion cases is 18 U.S.C. § 2251, which prohibits the sexual exploitation of children. According to § 2251(a), "Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct" is subject to a mandatory minimum sentence of 15 years in prison.

Although no legislation exist at the Federal level, Greenberg (2019) reports that state legislatures in 46 states and Washington DC have already began enacting legislation prohibiting the nonconsensual

dissemination of intimate images in 2013. The laws vary considerably from state to state (e.g., some provide for misdemeanor offenses, some felonies; some are part of cyber harassment or voyeurism codes; others are standalone provisions). Additional growing trend is legislation which is aimed to provide for civil remedies for victims of these acts. About a dozen state laws currently allow for a private right of action against those who disclose intimate images without consent (see here for a list of states https://www.uniformlaws.org/committees/community-home?CommunityKey=668f6afa-f7b5-444b-9f0a-6873fb617ebb). In July 2018, the Uniform Law Commission approved the Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act, which aims to provide a "uniform, clear, fair and constitutionally sound definition of this harmful conduct and remedies for the harm it causes." Moreover, at least 26 states and D.C. now have laws addressing sextortion (for example Georgia, North Dakota, and Nebraska).

References:

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

Greenberg, P.(2019). Fighting Revenge Porn and 'Sextortion'**.** Legisbrief Vol . 27, No. 29 Available at: *https://www.ncsl.org/research/telecommunications-and-information-technology/fighting-revenge-porn-and-sextortion.aspx*

Sweeny, J. (2011). Do sexting prosecutions violate teenagers' constitutional rights. *San Diego L. Rev.*, *48*, 951.

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?

Answer: Minors are subjected to the same states' relevant statutes I described in Answer 2.

Question 10: Can minors be punished for wilful misinformation or deception online (sharing false news, false information, pretending to be someone else, pretending to be an expert, etc.)? Which crimes/qualifications could possibly apply? If criminal sanctions could apply, are minors prosecuted in practice?

Answer: Minors are subjected to the same states' relevant statutes I described in answer 3.

Question 11: Can minors be punished for online actions facilitating human trafficking? Typically this includes the selection and grooming of victims (e.g. lover boy phenomenon). If criminal sanctions could apply, are minors prosecuted in practice?

Answer: Minors are subject to the same statues I elaborated on answer 4 in the context of human trafficking related crimes. In terms of actions (both online and offline) facilitating human trafficking, most state laws include a wide variety of activities under their definitions of trafficking, which include actions that facilitate human trafficking. Still, in recent years, some jurisdictions have expanded their definitions of trafficking to include facilitators of human trafficking. For example Hawaii's sex trafficking law criminalizes aiding or facilitating sex trafficking of a child and a convicted facilitator can face up to 20 years in prison and a fine of up to $50,000. The Missouri House of Representative's Human Trafficking Task Force advised the General Assembly to amend the definition of trafficking for the purposes of sexual exploitation to include the act of "advertising the availability," which means those who advertise on posters, websites and apps can be prosecuted in the same manner as those perpetrators actually trafficking. Oklahoma has a similar law. In any event, minors are subject to the same statues and penalties for online actions which facilitate human trafficking behaviors.

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?

Answer: The Copyright Act of 1976 (17 U.S.C. § 506(a)) is the most important copyright law in the United States that protects intellectual property from being reproduced and distributed without authorization (Bossler 2020).This Act makes it a federal crime to willfully infringe on an existing copyright for commercial advantage, private gain, or by reproducing or distributing one or more copies of copyrighted work with a value of more than $1000 over a 180- day period. Individuals are charged with a felony if they reproduce or distribute at least 10 copies of one or more copyrighted works with a total value of more than $2500 over a period of 180 days. The Copyright Felony Act of 1992 extended copyright protection to computer software and other works written, stored or transmitted in a digital format, if the other elements of the statute are satisfied (Brenner 2011). Felony penalties are attached to violations of a victim's rights of reproduction or distribution in the quantity stated. A misdemeanor applies if the defendant does not meet the numerical and monetary thresholds, or if the defendant is involved in the infringement of the other rights bestowed upon the copyright holder, including the right to prepare derivative works, or the right to publicly perform a copyrighted work. According to the US Department of Justice "In order to sustain a conviction under section 506(a), the government must demonstrate: (1) that a valid copyright; (2) was infringed by the defendant; (3) willfully; and (4) for purposes of commercial advantage or private financial gain. Attempts to infringe are prohibited to the same extent as the completed act. Conspiracies to violate the Act can be prosecuted under 18 U.S.C. § 371."

The No Electronic Theft Act of 1997 recognized infringement of copyrighted material even when the person who received or expected to receive copyrighted work did not profit through commercial or personal gain. This makes it illegal to even attempt to acquire pirated media through file sharing rather than paying for the intellectual property (Bossler 2020). These revisions make music piracy illegal by sanctioning the reproduction or distribution of one or more copies of phonorecords. These acts also increased the penalties for piracy up to 5 years in prison and $250,000 in fines while also increasing statutory damages.

Finally, the Digital Millennium Copyright Act (DMCA), further address concerns by online media piracy (Brenner 2011). The second section of the act under the title added § 1201 makes it illegal to circumvent any protective technologies placed on copyrighted materials, and § 1202 makes it illegal to tamper with copyright management software or protections. The DMCA also contained Title II (titled the Online Copyright Infringement Liability Limitation Act), which extendes protections to Internet Service Providers from liability if ISPs blocked infringing material or removed infringing materials if a complaint was received from a copy- right holder or owner (Bossler 2020). This title also allows copyright holders to subpoena ISPs for the ISP addresses, names, and home addresses of customers who had engaged in the distribution of copyrighted materials and pursue civil and criminal charges.

Issue in applications of these statutes include the requirement to prove willfulness, estimating the retail value of the stolen IP, and proving the intent to profit. For example, in United States v. Moran, the government filed misdemeanor criminal charges against defendant Dennis Moran, who owned a video store, accusing him in violating federal copyright laws. Defendant contended that he made a copy of copyrighted videotape and retained the original to safeguard it, and that he believed the practice was legal as long as he had purchased the "original" videotape. Defendant therefore argued that he lacked the specific intent to violate the law and should be found not guilty. The court found defendant not guilty, holding that while ignorance of the law was no defense to criminal prosecution in complex statutory schemes, such as the copyright statute and federal criminal tax statutes, the term "**willful**" meant a voluntary, intentional violation of a known legal duty.

In United States v. Armstead , Defendant David Armstead was charged with and convicted of two felony counts of willful copyright infringement for the distribution of bootleg DVDs. Defendant had sold the DVDs at issue to an undercover agent for $500 in the first transaction and for $1,000 in the second. The

only issue at trial and on appeal was how to measure the "retail value" of DVDs sold by the defendant to an undercover agent. Armstead argued that he should only have been convicted of a misdemeanor because "retail value" should be the price a willing buyer would pay a willing seller at the time and in the market in which the infringing DVDs were sold – i.e., the thieves' market. The government argued that "retail value" refers to the higher of what a willing buyer would pay a willing seller for legitimate copies of the DVDs. Stating that it was a "matter of first impression," the Fourth Circuit held that "'retail value' refers to the value of copies of the copyrighted material at the time the defendant committed the violation and sold the copies and that the retail value is determined by taking the highest of the 'face value,' 'par value,' or 'market value' of copies and the copyrighted material in a retail context." The court stated that this definition includes, but is not limited to, the bootleg value. Since, the jury had sufficient evidence from which to conclude that the total retail value of the DVDs exceeded the $2500 threshold, the court upheld defendant's felony conviction.

In line with these statutes, and the general rule that ignorance of the law of mistake of the law is no defense to a criminal prosecution, minors could be prosecuted for acts of online piracy in the USA.

References:

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

United States v. Moran - 757 F. Supp. 1046 (D. Neb. 1991)

United States v. Armstead Fourth Circuit 524 F.3d 442 (2008)

Question 13: Can minors be punished for acts of hacking (i.e. unauthorized access to a computer system)? In particular, would this also apply to various scenarios exploiting vulnerabilities in IoT and connected devices? If criminal sanctions could apply, are minors prosecuted in practice?

Answer: The Computer Fraud and Abuse Act (CFAA) is the most important piece of federal legislation in the United States that deals with cybercrime in general and computer hacking specifically (Bossler 2020). The CFAA is used to prosecute attacks against "protected computers," which can be defined as a computer "(a) exclusively for the use of a financial institution or the United States government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (b) which is used in or affecting interstate or foreign commerce or communication" (18 U.S.C § 1030 (e) (2))."

The CFAA specifies seven applications of hacking that violate federal law including:

(a) (1) Obtaining national security information:
(a) (2) Accessing a computer and obtaining information:
(a) (3) Trespassing in a government computer:
(a) (4) Accessing a computer to defraud and obtain value:
(a) (5) Intentionally, recklessly or negligently damage a computer during by intentional access.
(a) (6) Traffic passwords
(a) (7) Extorting using computers.

Bossler (2020) summarizes the relevant penalties for violation of this act as follows:

"The severity of the punishment associated with the conviction of these offenses is influenced by both the harm caused and the number of prior convictions. Trespassing acts designed to obtain national security information may receive minimum sentences of 10–20 years. The sentence for accessing a computer to obtain information of value may range from a minimum of 1 year in prison and/or a fine up

to 10 years if the offender is charged with multiple charges or committed the offense for commercial or private gain. Similarly, trespassing against government-owned computers may lead to a punishment of up to 1 year in prison and/or a fine or up to 10 years if the offense was connected with another offense.

Offenses covered by (a) (4) have the greatest range of punishments with penalties ranging from up to 5 years "if the object of the fraud and the thing obtained consists only of the use of the computer and the value of that use does not exceed $5,000 in any one-year period"; a minimum of 10 years if the harm exceeded $5000 or affected "more than ten computers, affects medical data, causes physical injury to a person, poses a threat to public health or safety or affects the US government's administration of justice, defense, or national security"; up to 20 years if the computer intrusion causes serious bodily injury; and up to life in prison if the computer hack knowingly or recklessly led to death.

For (a)(5), the punishment can include a fine and a sentence from 2 years all the way to life depending on whether the offense led to death. Offenders convicted of (a) (6) can receive a sentence of a fine and a prison sentence up to 5 years depending on whether the violator gained financially or if the data was valued at over $5000. The convicted offender may receive a sentence up to 10 years if they are found guilty of multiple counts or if the value of the data exceeded $5000. Finally, violations of (a) (7) can be fined and/or imprisoned up to 10 years if the offender had prior convictions (p.5)."

18 U.S.C. § 2701 (Unlawful Access to Stored Communications) is additional Federal statute which could be used for the prosecution of hacking. This statute makes it illegal to either "intentionally access[es] without authorization a facility through which an electronic communication service is provided" or "intentionally exceed[s] authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." Penalties for violators of this statue ranges from up to 1 year for a conviction of one count to up to 5 years for subsequent offenses. These punishments, however, were increased under the Homeland Security Act of 2002 if the offense was committed for "purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or any State" (Brenner 2011). An offender may receive a fine and up to 5 years in prison for the first offense and up to 10 years if convicted of multiple offenses (Bossler 2020).

Computer hacking and the use of code for unauthorized access are criminalized at the state level as well. Today, all US states have passed computer crime legislation with most laws addressing computer hacking or unauthorized access (National Conference of State Legislation 2022). Most states use a two-tiered system to prohibit hacking behaviors with simple hacking (unauthorized access but no damage to the system or further criminal behavior) being considered a misdemeanor and aggravated hacking, unauthorized access leading to further criminal behavior in the form of copying or destroying of data, being treated as a felony (Brenner 2011). However, other states use a single statute to criminalize unauthorized access regardless of whether further criminal activity occurs. States also differ on whether they criminalized these behaviors under existing statutes relating to burglary and theft or whether new statutes were enacted to establish the unique characteristics of computer hacking (Brenner 2011) more clearly.

Known issues in the application of these statues evolves around the court interpretation of the word "access", as well as the interpretation of "authorized access." In the context of "access," courts may interpret access to a computer as either virtual or physical. Under the "virtual access" interpretation, access hinges on whether the user has made a virtual entrance into the computer. Using this interpretation one can imagine a user tring to use a password-protected computer network and is confronted by a screen that requires a valid username and password to proceed. The screen requiring the logging credentials is akin to a lock on a front door, and entering a username and password is like using a key to open the lock (Kerr 2018). In contrast, under the "physical access" interpretation, we recognize that computers are simply machines that communicate with each other by sending and receiving information. Under this approach, one can interpret access by looking to whether a user has sent communications that have physically entered the computer (Kerr 2018).

In State v. Riley, the court adopts the view that access can be pretty much anything that interacts with a computer. In this case, defendant Joseph Riley was accused of calling the general number of Northwest Telco Corporation (which provided long-distance telephone service) and entering random numbers every 40 seconds to try to discover access codes, which then could be used to place long distance calls. Joseph Riley was convicted of three counts of computer trespass and four counts of possession of a stolen access device after he used his home computer to obtain long-distance telephone access codes from telephone company computers. In contrast, in State v. Allen, the court adopted more of a virtual view that the user has to virtually "enter" the machine to access it. In this case, Allen used his computer to dial up access numbers of Southwestern Bell, and he then faced the prompts that asked him for a password that would enable him to make free long-distance telephone calls. The access numbers were only supposed to be known to Southwestern Bell employees. There was no direct evidence that Allen had responded to the password prompt. The Kansas Supreme Court held that Allen had not accessed Southwestern Bell's computer (Kerr 2018).

Another issue in the application of these computer access statues pertains to the question of what is authorization? Kerr (2018) suggests that there are three basic ways to set computer users privileges on a computer: by code, by contract, or by social norms. When an owner regulates privileges by code, the owner or her agent designs and programs the computer's hardware and software so that the code limits each users' privileges. Perhaps every user must have an account, and access to that account is protected by a password. For a user to exceed privileges imposed by code, the user must somehow "trick" the computer into giving the user greater privileges. The code creates a barrier designed to limit privileges. *United States v. Morris* is a classic case on code-based restrictions. In this case, defendant Robert Morris was convicted under the Computer Fraud and Abuse Act for releasing a worm which caused computers at various educational and military sites to cease functioning. He appealed his conviction and argued the government had to prove not only that he intended the unauthorized access of a federal interest computer, but that he also intended to prevent others from using it. The Second Circuit concluded that Morrison could be convicted so long as the evidence showed that he intentionally accessed a Federal interest computer without authorization and that damage was caused by this access. Since the worm was designed to invade computers at which he had no authority, express or implied, Morris's conviction was affirmed.

Alternatively, a computer owner or operator may regulate computer privileges by contract. Access to the computer can be conditioned on the user's promise to abide by a set of terms such as Terms of Service for an e-mail account or Terms of Use for a website. In *United States v. Nosal*, Defendant David Nosal convinced some of his former colleagues who were working for Korn/Ferry (an executive search firm the defendant used to work for as well) to use their log-in credentials to Korn/Ferry computers and download source lists, names and contact information from a confidential database on the company's computer, and then transferred that information to Nosal. The employees were authorized to access the database, but Korn/Ferry had a policy that prohibited disclosing confidential information. The government indicted Nosal on twenty counts, including trade secret theft, mail fraud, conspiracy and violations of the Computer Fraud and Abuse Act (CFAA). Nosal filed a motion to dismiss the CFAA counts, arguing that the statute only targeted hackers and not individuals who accessed a computer with authorization and then later misused information they obtained by means of such access. A federal appellate court affirmed the judgment arguing that a violation for exceeding authorized access occurs where initial access is permitted but the access of certain information is not permitted.

Finally, computer use might be unauthorized if it violates a social norm on computer use. Social norms are widely shared attitudes that specify what behaviors an actor ought to exhibit. In the context of computer misuse, access might violate a social norm if most computer users would understand that they are not supposed to access the computer in that way even if it does not circumvent a code-based restriction or breach an explicit contract-based restriction.

Since minors in the USA are subject to the same statutes as adults, they could be prosecuted for acts of hacking. Indeed, Goldberg (1998) reported a 1997 case in which prosecutors brought Federal computer

crime charges against a Massachusetts teenager whose modem mischief temporarily knocked out phone service to about 600 homes and a small airport's control tower. The teenager signed a plea barging in which he faced two years of probation, 250 hours of community service and $5,000 in restitution, which he needed to pay to Bell Atlantic, the telephone company he attacked. He was also forbidden to use a modem or other remote-access device for two years.

References:

Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. In R. D. Clifford (Ed.), Cybercrime: The investigation, prosecution, and defense of a computer-related crime (3rd ed., pp. 15–104). Raleigh: Carolina Academic Press.

Goldberg, C. 1998. *Federal Charges for Juvenile In a Case of Computer Crime. The New York Times. Available at:* https://www.nytimes.com/1998/03/19/us/federal-charges-for-juvenile-in-a-case-of-computer-crime.html

Kerr, Orin S. (2018). *Computer crime law*. Thomson/West.

National Conference on State Legislatures. 2022. Computer Crime Statutes. Available at: https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

Question 14: Can minors be punished for acts of using any instance of Cybercrime as a Service? If yes, under what qualification? If criminal sanctions could apply, are minors prosecuted in practice?

Answer: This question is very broad since cybercrime-as-a-service operations involves many types of cybercrime including botnets, distributed denial of service attacks (DDoS), credit card fraud, malware, hacking, spam, and phishing attacks (Hyslip 2020). These services are often sold through hacker forums, direct web sales, and on the dark web using cryptocurrency. Since many of the crimes that falls under the definition of cybercrime-as -a-service may be prosecuted using the CFAA, subsection 1030(b) of the act, which makes it a crime to attempt or conspire to commit any of these offenses, could be used in this context. Since minors are subject to CFFA, they could be punished for these acts as well.

References:

Hyslip T.S. (2020) Cybercrime-as-a-Service Operations. In: Holt T., Bossler A. (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham

4. **General questions regarding cross border cybercrime, international legal instruments applicable to fighting cybercrime and regarding international cooperation**

Question 15: How does your country deal with the cross-border nature of many cybercrimes? When is jurisdiction established? Can judgements have extra-territorial effect?

Answer: The relatively clear borders and turf lines within the physical world are not replicated in the virtual realm. As such, in contrast to the vast majority of offline crimes, their offender, the victim and the criminal act are not all situated in the same jurisdiction (Grabosky et al 2004). In the context of cybercrime, countries may assert jurisdiction over behaviors that impacted their national interest or their citizens (Finklea 2011).

In the USA, the Computer Fraud and Abuse Act seems to be will equip to deal with this issue. Specifically, upon comping to decide whether a U.S. statute could be applied extraterritorially, USA courts look to two potential foundations for jurisdiction: first, the jurisdictional basis, "territoriality, nationality, passive personality, universality, or the protective principle"(Podger 2002); and second, legislative intent (Kane and Mikail 2020). Thus, while rhe first foundation encompasses passive personality and protective basis for international jurisdiction, the second relies upon the legislative to include any computer 'which is used in interstate *or foreign* commerce or communication. Computer crimes in this sense, could arguably be applied extraterritorially on either foundation. Kane and Mikail argue that although case law is sparse, in *United States v. Ivanov* a Connecticut district court concluded that it had jurisdiction to hear a claim against a Russian national under the Computer Fraud and Abuse Act. Accordingly, the court found ". . . first, because the intended and actual detrimental effects of [the defendant's] actions in Russia occurred within the United States, and second, because each of the statutes under which [he] was charged with a substantive offense were intended by Congress to apply extraterritorially." In sum, *The CFAA's reach goes beyond U.S. borders and packs a jurisdictional reach that allows American law enforcement to bring a foreign party into an American court.*

Kane and Mikail (2020) also argue that the Patriot Act form additional statute which may provide extraterritorial jurisdiction for the Computer Fraud and Abuse act (CFAA). Accordingly, The Patriot Act modified a "protected computer" to include "a computer which is used in interstate or foreign commerce or communication" and the words "including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." By doing that, The Patriot Act expanded the definition of "protected computer" to "include computers located outside the United States."

References:

Finklea, K. M. (2011, July). The interplay of borders, turf, cyberspace, and jurisdiction: Issues confronting US law enforcement. Congressional Research Service, Library of Congress. *Available at https://sgp.fas.org/crs/misc/R41927.pdf*

Grabosky, P., Russell G.. Smith, & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Kane W. and Mikail M. (2020). Extraterritorial Application of the Computer Fraud and Abuse Act. The National Law Review Volume XII, Number 146. Available at: https://www.natlawreview.com/article/extraterritorial-application-computer-fraud-and-abuse-act

Podgor, E. (2002). *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. Davis L. Rev. 267, 282.

United States v. Ivanov, 175 F. Supp. 2d 367, 370 (D. Conn. 2001)

Question 16: What international legal instruments (bi-lateral, multi-lateral) apply in your country to the fight against (cross-border) cybercrime and how have they been implemented in national law (if implementation is necessary)?

Answer: The United States is signed on both regional and/or global agreements (i.e. multilateral agreements), as well as one-on-one agreements with other countries (i.e. bilateral agreements). The purpose of signing these agreements is the facilitation of US cooperation with those governments in cybercrime investigations and prosecutions, including by allowing for the collection and sharing of evidence across borders. Peters and Hindoch (2020) provide a list of those agreements including:

Convention on Cybercrime of the Council of Europe (Multilateral Treaty): the convention on cybercrime articulates a set of principles that member states agree to adopt in their domestic law and ,

is currently the only legally binding international treaty on cybercrime. The Convention sets common standards on investigations and facilitates criminal justice cooperation in cybercrime cases for its 65 member countries. The treaty has been ratified by many non-Council of Europe members, including by the United States (which even though is not a member in the council of Europe, holds observer status in the Council). The treaty is important since it provides a guidepost for nations to create and harmonize their own comprehensive national legislation on cybercrime. On the substantive side, the agreement includes articles relevant to illegal access, illegal interception, data interference, computer related forgery, computer related fraud, offenses related to child pornography, and offences related to infringements of copyright and related rights (to name few). On the procedural site, the treaty includes articles relevant to the scope of procedural provisions, preservation of stored computer data, search and seizure of stored computer data, and real time collection of traffic data (to name few). Importantly, The Budapest Convention is not a static treaty and can be updated to meet evolving needs, as is currently being done for a new protocol dealing with electronic evidence.

UN Convention against Transnational Organized Crime (Multilateral Treaty): This UN Convention is the main international instrument in the fight against transnational organized crime (See https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf). The Convention is further supplemented by three Protocols, which target specific areas and manifestations of organized crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. The United States is a party to this agreement (along with 190 other countries) ever since its ratification in 2005. Although this Convention is aimed at preventing and combatting transnational organized crime, the US government has noted that its provisions are sometimes used to facilitate cooperation in cybercrime cases.

Inter-American Convention on Mutual Legal Assistance of the Organization of American States (Multilateral Treaty): The Charter of this treaty between American states is "to seek the solution of political, juridical, and economic problems that may arise among them". The adoption of common rules in the field of mutual assistance in criminal matters is perceived to support this goal. Although this Convention is not specific to cybercrime, its provisions allow for the United States to request from and provide legal assistance to OAS members, which could help facilitate regional cooperation in cybercrime cases.

Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs) (Bilateral): As of 2018, the United States had entered into MLATs with 65 other nations and the EU. The United States also has an MLAA with China, as well as one with the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office (Peters and Hindoch 2020).

CLOUD Act Agreements (Bilateral): The United States is one of a small number of countries where the most data is collected and stored, which means each year the US Department of Justice fields an enormous number of requests from foreign governments who seek access to electronic evidence stored in this country for cybercrime and other criminal cases. In 2018, Congress passed the "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act, P.L. 115-141) to allow the United States to negotiate for executive agreements with other nations who can meet certain privacy and civil liberties standards in order to facilitate cross-border data sharing directly between US companies and foreign governments. So far, the United States has entered into such an agreement with the United Kingdom and is negotiating another with Australia (Peters and Hindoch 2020).

Extradition Treaties (Bilateral): Extradition treaties establish a process whereby one country surrenders an individual suspected in crime to another country for prosecution or punishment for the crimes committed by the individual in the requesting country's jurisdiction. As of 2022 the United States has signed extradition treaties with over 100 countries. More recent treaties have also included a "dual criminality" requirement, which requires the charged conduct to be criminalized in both the requesting and requested jurisdictions for an extradition to proceed (Peters and Hindoch 2020). The

United States is also a member state in the INTERPOL, the world's largest police organization. As a member state in the INTERPOL, the United States can send (and respond) to requests for information and assistance in criminal investigations. Those requests are sent through the red notice system which is the closest thing that exists to an international arrest warrant and.

Other Bilateral Cooperation Initiatives: in addition to these aforementioned agreements, the United States is engaged in numerous bilateral cybercrime cooperation initiatives with other nations. The United States also contributes to bilateral and regional capacity building efforts on cybercrime, which can help boost the capability of countries to be able to cooperate in these investigations.

References:

Peters, A. and Hindoch A. 2020. US Global Cybercrime Cooperation: A Brief Explainer. Available at: *http://thirdway.imgix.net/pdfs/us-global-cybercrime-cooperation-a-brief-explainer.pdf*

Question 17: What forms of international cooperation exist in your country to the fight against cross-border cybercrime? Please describe different routes/options/procedures and the measures that can be requested (e.g. asking for investigative actions, exchange of information/evidence, etc.)?

Answer: Peters and Hindoch (2020) outline the following international organizations and forums as platforms which the United States participate in aim to facilitate the exchange of information in criminal cases and sharing of expertise and experience around the issue of cybercrime:

United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ): The UN CCPCJ (See https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html) acts as the principal policymaking body of the United Nations in the field of crime prevention and criminal justice. ECOSOC provided for the CCPCJ's mandates and priorities which include improving international action to combat national and transnational crime and the efficiency and fairness of criminal justice administration systems. The CCPCJ also offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies, and to identify priorities for combating crime. The CCPCJ also governs the work of the UN Office on Drugs and Crime (UNODC), which educates countries on cybercrime and conducts important capacity building programming to help boost the capability of other countries to investigate it. It is also the preparatory body for what is colloquially known as the UN Crime Congress—a high-level meeting of government officials held every five years to discuss important criminal matters where cybercrime has been a primary focus in recent years. The United States is currently an elected member of the Commission, providing the US government with a forum to discuss and exchange expertise and experience on cybercrime issues (Peters and Hindoch 2020).

Organization for Security and Co-operation in Europe (OSCE): OSCE (see https://www.osce.org/), is the world's largest regional security organization and includes 57 countries from North America, Europe, and Asia. The organization has worked to develop confidence-building measures (CBMs) to reduce conflict between countries that arises from the increased use of information and communications technologies (ICTs). These measures encourage countries to put in place national legislation to facilitate the voluntary cooperation between law enforcement agencies to counter the criminal use of ICTs and have a point of contact to facilitate communication (Peters and Hindoch 2020). In the context of cybercrime, OSCE participating States are working to make cyberspace more predictable and offer concrete tools and mechanisms to avoid misunderstandings, including:

- A mechanism to bring together states for consultations over potential cyber/ICT security incidents to de-escalate rising tensions;
- A platform for exchanging views, national cyber/ICT security policies and approaches to allow states to better "read" each other's intentions in cyberspace; and

- Concrete work items, for instance to protect ICT-enabled critical infrastructure, allowing participating States to collectively enhance cyber resilience in the OSCE region for the benefit of all.

OSCE also focuses on tackling cyber/ICT security threats from non-state actors, such as organized criminals and terrorists through promotion of adequate and timely responses by national authorities to these evolving threats. The United States is a participating State in this organization.

Organization of American States (OAS) Inter-American Cooperation Portal on Cyber-Crime and Working Group: the Inter-American Cooperation Portal on Cyber-Crime (See http://www.oas.org/en/sla/dlc/cyber-en/homePortal.asp) was created to facilitate information exchange from government experts with cybercrime responsibilities within OAS member states and streamline cybercrime investigations and extraditions. The OAS' Cyber-Crime Working Group seeks to develop mechanisms to enhance and strengthen cooperation among its regional members in the area of cybercrime. The United States is a participant country in this organization.

Group of Seven (G7)'s 24/7 Cybercrime Network: The G7 is a forum to bring together the leaders of the world's leading industrial nations, including the United States. Its 24/7 Network, which includes more than 70 nations, establishes points of contact to respond to urgent requests from governments to preserve digital evidence, including in cybercrime cases *(Peters and Hindoch 2020*). The Primary purpose of the Network is to preserve data for subsequent transfer through mutual legal assistance channels. The United States is an active member in this network. The United States also participates in the Council of Europe's Network of 24/7 Contact Points and INTERPOL's secure communication network known as I-24/7, which is a tool that allows for intelligence and information sharing during cybercrime investigations.

European Union Agency for Law Enforcement Cooperation (EUROPOL)'s Joint Cybercrime Action Taskforce (J-CAT): As one of 16 member countries in EUROPOL's J-CAT, the United States has liaisons from the FBI and Secret Service to participate in the Taskforce's standing team of cyber liaisons and work with other members to support joint intelligence-led, coordinated action against specific cybercrime threats.

Global Forum on Cyber Expertise (GFCE): The GFCE strengthens international cooperation on cyber capacity building by connecting needs, resources and expertise and by making practical knowledge available to the global community (see https://thegfce.org). Its current focus the coordination of regional and global cyber capacity projects and initiatives; sharing knowledge and expertise by recommending tools and publications; and matching individual needs for cyber capacities to offers of support from the community as a clearing house function. The GFCE is comprised of public and private sector members and works to strengthen international cooperation on cyber capacity building, including by sharing research and expertise on cybercrime and serving as a clearing house for projects. The United States is a member of the GFCE and participates in meetings of its Cybercrime Working Group.

References:

Peters, A. and Hindoch A. 2020. US Global Cybercrime Cooperation: A Brief Explainer. Available at: *http://thirdway.imgix.net/pdfs/us-global-cybercrime-cooperation-a-brief-explainer.pdf*

Question 18: Do the rules (national, international) and policies mentioned in your answers in this section have any particular effect or impact on cybercrime committed by minors?

Answer: I am not aware of any way in which the rules and policies mentioned in this section have particular impact on cybercrime committed by minors. As indicted in the answers provided on section 3, minors are subject to the same cybercrime laws and statues which adults are subjected to in the USA.

5. Other

Question 19: Do you have any information on the rates/statistics of cybercrime in your country and their recent evolution? Of particular interest would be statistics related specifically to the crimes covered in this questionnaire and statistics on cybercrime by minors (ideally also specifically for the crimes covered above)? If there were any (relatively) recent legislative or policy changes, please try to find statistical information on how this has impacted the incidence of cybercrime in practice, and in particular cybercrime by minors.

Answer: Similar to the concept "crime", the term "cybercrime" encompasses various types of illegal online activities. As such, collecting data about cybercrime incidents is challenging; the collection of data about DDoS attacks against a sever requires the use of different tools and research designs than those required for the collection of data about cyber-bullying or identity theft. Moreover, although some cybercrime types could be easily identified and reported by victims (for example online fraud or cyber harassment), other types of cybercrime could go undetected by victims for years (for example hacking and malware infection). As such, data collection efforts around cybercrime incidents varies considerably, and are performed by three types of actors:

Nonprofit organizations – Nonprofit organizations are dedicated to advancing a particular social cause. Several nonprofit organizations gather and measure information on various types of cybercrime in an established systematic fashion that enables them to support their goal. The Privacy Clearning House, for example, believe everyone deserves the opportunity to be informed and be heard. As part of their efforts to provide clarity on complex topics such as cybercrime, they publish educational materials and compile a database around data breaches which could be accessed and downloaded here https://privacyrights.org/
Cybersecurity companies – Cybersecurity companies constantly collect data about cybercrime incidents experienced by their customers in effort to improve their operations and offer better protection to their clients. Those companies use these data to produce annual reports, as well as make some of this data available on their websites. Kaspersky Lab for example, allow users to download statistics and data regarding vulnerabilities they discover here: https://statistics.securelist.com/en/vulnerability-scan/day

Law enforcement agencies- the amount of crime within a specific population is typically estimated though police reporting of crime reported to them. In the United States, police reporting of crimes is standardized by the FBI's Uniform Crime Report system. Unfortunately, this system does not support the collection and report of cybercrime incidents. Instead, the Internet Crime Complaint Center (IC3) is the official USA based portal which accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. IC3 produces annual reports of the volume of cybercrime in the USA which could be found here: https://www.ic3.gov/default.aspx. Most of the reports available through the IC3 are reports submitted by victims of online fraud.
Still, despite these efforts, none of these sources produces reliable and rigorous statistics around cybercrime events in the USA.

Question 20: Do you have any other comments to make that may be relevant to your jurisdiction?

Answer: *N.A.*