Children's Online Privacy Protection Act and the Cisco Security Portfolio

Understanding COPPA

The Children's Online Privacy Protection Act (COPPA) is a U.S. federal law enacted in 1998 designed to protect the privacy and personal information of children under the age of 13 who use the internet. It requires operators of websites and online services that are directed to children or that knowingly collect personal information from children to obtain verifiable parental consent before collecting, using, or disclosing such information.

COPPA applies to a wide range of online entities that may interact with or collect data from children online, either intentionally or inadvertently. The types of businesses typically affected by COPPA:

- **Websites and Online Services for Children**
  Websites, apps, and online services specifically designed for or targeted at children under 13.
- **General Audience Platforms**
  General audience websites and services that have sections or features specifically directed at children.
- **Educational Technology Companies**
  Companies providing online educational tools and resources for use in schools or by children at home.
- **Gaming Platforms**
  Online gaming sites and apps that are either directed at children or have a significant number of users under 13.
- **Social Media and Community Platforms**
  Social media sites and community forums that allow children under 13 to register and participate.
- **E-commerce Sites**
  Online stores and marketplaces that collect personal information from children under 13.

COPPA mandates that these operators provide clear privacy notices, implement reasonable data security measures, and offer parents the opportunity to review and delete their children's information. The law aims to give parents control over the information collected from their young children online.

2025 Revisions

In 2023, the Federal Trade Commission (FTC) proposed revisions to the COPPA Rule to respond to changes in technology and online practices. The FTC finalized these changes in January of 2025; the new rules to go into effect 60 days after the publication in the Federal Register. Revisions will include:

- Requiring opt-in consent for targeted advertising to children.
- Expanding definitions of personal information to include biometric identifiers.
- Increasing transparency from COPPA Safe Harbor Programs.
- Prohibiting the use of push notifications to encourage prolonged use by children without parental consent.
- Operators must obtain separate verifiable parental consent for disclosing children's personal information to third parties.
- Enhanced data security, retention, and deletion practices.
- Banning targeted advertising to individuals under 17.
- Requiring consent for data collection from users under 17.
- Providing tools for parents and kids to delete personal information online.
- Establishing a Youth Marketing and Privacy Division at the FTC.
- Implementing a duty of care for online platforms to protect minors.

The Children's Online Privacy Protection Act (COPPA) is a U.S. federal law enacted in 1998, designed to protect the privacy of children under the age of 13 online.

COPPA Requirements for Computer Security Safeguards

COPPA requires operators of websites and online services directed to children under 13, or those collecting personal information from children, to implement robust computer security safeguards. These safeguards are intended to protect the confidentiality, integrity, and security of the personal information collected. Operators must establish and maintain reasonable procedures to prevent unauthorized access, use, or disclosure of children's data.

Additionally, they are required to minimize data collection to only what is necessary for the service and ensure secure data storage and transmission. The law also mandates that operators provide mechanisms for parents to access and delete their child's information, ensuring ongoing oversight and protection of the child's online privacy.

COPPA Security Requirements Deep Dive

Data Security and Minimization

Collect only the personal information necessary for the activity.

Data minimization is a key principle of COPPA that requires operators to limit the collection of personal information from children to only what is necessary for the specific activity or service being provided. This means that websites and online services should not collect more data than is required to fulfill the intended purpose of the interaction.

By adhering to this principle, operators can reduce the risk of misuse or unauthorized access to children's personal information, thereby enhancing privacy and security. COPPA also requires operators to implement reasonable procedures to protect the confidentiality, security, and integrity of children's data. This includes safeguarding against unauthorized access or breaches and ensuring that third parties handling such data provide similar protections.

Implementing data minimization involves assessing what data is essential for the functionality of the service and ensuring that no additional, unnecessary information is gathered. This approach not only helps in complying with COPPA but also fosters trust with users by respecting their privacy.

Parental Consent

Obtain verifiable parental consent before collecting personal data from children.

Provide parents with access to their child's personal information and the ability to delete it upon request.

Parental consent is a fundamental requirement of COPPA, which mandates that operators of websites and online services directed at children under 13, or those collecting personal information from them, must obtain verifiable parental consent before collecting, using, or disclosing such information. This process ensures that parents are fully informed about what data is being collected from their children and how it will be used.

To obtain verifiable parential consent; operators can use serveral methods, such as:

- **Consent Forms**
  - Sending a consent form to be signed and returned by the parent via mail, fax, or electronic scan.
- **Credit Card Verification**
  - Collecting a credit card number along with a transaction to verify parental identity and consent.
- **Phone or Video Verification**
  - Engaging in a phone or video call with the parent to confirm consent.
- **Government ID Verification**
  - Using a government-issued ID to verify parental identity, provided it is checked and then promptly deleted to protect privacy.

These methods are designed to ensure that consent is obtained from an adult legally authorized to make decisions on behalf of the child, thereby safeguarding the child's personal information. The consent process must be clear and straightforward, providing parents with information about what data will be collected, how it will be used, and with whom it may be shared. This empowers parents to make informed decisions about their child's online interactions.

Notice

Under COPPA, the notice requirement mandates that operators of websites and online services directed at children under 13, or those collecting personal information from them, must clearly and comprehensively disclose their information practices. This notice aims to inform parents about the data collection, use, and sharing practices, enabling them to make informed decisions regarding their child's online activities.

Key Elements of Notice

- **Content of the Notice**
  - The notice must include details about the types of personal information being collected from children, such as name, address, email, or any other information that can be used to identify the child.
  - It should explain how the information will be used, for example, to provide services, improve user experience, or for marketing purposes.
  - The notice must also outline with whom the information may be shared, such as third-party service providers or partners, and under what circumstances.
- **Direct Notice to Parents**
  - Before collecting personal information from a child, operators must provide parents with a direct notice of their information practices. This notice should be clear and understandable, allowing parents to provide informed consent.
- **Online Privacy Policy**
  - Operators are required to maintain a publicly accessible privacy policy on their website or service that reflects their data practices. This policy should be easy to locate and understand, providing transparency about how children's information is handled.

By providing a clear and detailed notice, operators help ensure that parents are aware of and can consent to the data practices affecting their children. This transparency is crucial for complying with COPPA and building trust with users by demonstrating a commitment to protecting children's privacy.

Cisco Security Portfolio and COPPA Compliance

The Cisco® Security portfolio offers a comprehensive suite of solutions that can assist educational institutions and online service providers in achieving COPPA compliance. By implementing robust security measures, Cisco's offerings help protect the confidentiality, integrity, and security of children's personal information.

The portfolio includes tools that enable secure data collection and storage. These tools significantly aid in gathering only the necessary information and in protecting it against unauthorized access or breaches. With advanced access controls and threat detection capabilities, Cisco solutions provide a secure environment for online activities directed at children.

Additionally, these solutions facilitate parental involvement by supporting mechanisms for verifiable parental consent and providing options for data access and deletion. Through these features, the Cisco Security portfolio aids in maintaining transparency and compliance with COPPA's stringent privacy requirements, ultimately fostering a safer online experience for children.

The Cisco Security Portfolio Complies with COPPA Safeguards

Data Security

Cisco solutions offer robust security measures such as encryption, threat detection, and access controls to protect children's personal data.

Cisco solutions incorporate a range of robust security measures that help safeguard children's personal data in compliance with COPPA's data security requirements:

- **Encryption**
  Cisco solutions employ advanced encryption technologies to protect data both at rest and in transit. By encrypting personal information, these solutions ensure that even if data is intercepted or accessed without authorization, it remains unreadable and secure. This helps prevent unauthorized disclosure of children's sensitive information.
- **Zero Trust**
  Cisco Zero Trust helps safeguard children's personal data by implementing strict access controls and continuous monitoring, ensuring that only authorized users can access sensitive information. Additionally, it employs advanced encryption and data protection measures to comply with COPPA's data security requirements, providing a secure environment for personal data management.
- **Threat Detection and Prevention**
  Cisco provides sophisticated threat detection tools that continuously monitor for potential security threats, such as malware, phishing attacks, and unauthorized access attempts. These tools use machine learning and behavioral analytics to identify and mitigate threats in real time, thereby reducing the risk of data breaches that could compromise children's personal information.

- **Access Controls**
  Cisco solutions offer comprehensive access control mechanisms that restrict data access to authorized users only. This includes features such as multi-factor authentication, role-based access control, and user activity monitoring. By ensuring that only verified individuals can access sensitive data, Cisco solutions help prevent unauthorized use or exposure of children's personal data.

  Through these security measures, Cisco solutions not only support compliance with COPPA's data security requirements but also enhance the overall protection of children's online privacy, providing a safer digital environment for young users.

- **Parental Controls**
  Features can be integrated to allow parental oversight and control over their child's data and activity.

  Cisco solutions can be integrated with features that empower parents to oversee and control their child's data and online activities, aligning with COPPA's emphasis on parental involvement and consent. Here's how these parental control features work:

Parental Consent Management

Cisco solutions can support systems that facilitate obtaining verifiable parental consent before collecting or using a child's personal information. This includes secure platforms where parents can review consent requests and authorize data collection activities.

- **Activity Monitoring**
  These solutions can provide parents with tools to monitor their child's online activity, ensuring transparency and control over the digital content their child interacts with. Parents can receive reports or alerts about their child's online behavior, helping them make informed decisions about their child's internet use.

- **Content Filtering**
  Cisco can offer content filtering features that allow parents to set restrictions on the type of content accessible to their children. By blocking inappropriate or unsafe websites and applications, these filters help create a safer online environment for children.

- **Data Access and Control**
  Parents can be given access to review the personal information collected from their children and request modifications or deletions as necessary. This control ensures that parents can manage their child's data privacy effectively.

- **Customizable User Profiles**
  Solutions can enable the creation of user profiles that reflect parental preferences and restrictions, allowing for tailored online experiences that align with family values and safety requirements.

  By integrating these features, Cisco solutions help ensure that parents remain informed and in control of their child's online presence, thereby supporting compliance with COPPA's parental oversight requirements and enhancing overall child safety online.

- **Compliance Tools**
  Cisco provides tools and services to help educational institutions manage compliance with privacy regulations like COPPA through secure network infrastructure and policies.

  Cisco offers a variety of tools and services designed to help educational institutions manage compliance with privacy regulations like COPPA by building a secure and reliable network infrastructure.

Secure Network Infrastructure

Cisco provides robust network solutions that create a secure foundation for protecting sensitive data. This includes firewalls, secure routers, and switches that help safeguard data in transit across educational networks, preventing unauthorized access and ensuring data integrity.

- **Policy Management**
  Cisco solutions offer centralized policy management tools that allow institutions to define, implement, and enforce security policies across their networks. These policies help ensure that data handling practices comply with COPPA requirements, such as data minimization and secure data storage.
- **User Authentication and Access Control**
  With Cisco's identity and access management solutions, educational institutions can implement strong authentication measures to verify user identities and control access to sensitive data. This helps ensure that only authorized personnel can access children's personal information, aligning with COPPA's security requirements.
- **Monitoring and Reporting**
  Cisco provides advanced monitoring and reporting tools that offer visibility into network activity, helping institutions detect and respond to potential security incidents. These tools also generate compliance reports that document adherence to COPPA requirements, assisting institutions in demonstrating their compliance efforts.
- **Training and Support Services**
  Cisco offers training programs and support services to help educational institutions understand and implement best practices for privacy and data protection. These resources ensure that staff are equipped to manage and maintain compliance with COPPA effectively.

By leveraging these tools and services, educational institutions can create a secure environment that protects children's privacy and aligns with COPPA's stringent requirements, ultimately fostering a safe and compliant educational setting.

Cisco Security Solutions designed for COPPA

Cisco Next Generation Firewall

Cisco Next-Generation Firewall (NGFW) can help meet COPPA requirements by providing robust security features that protect sensitive data, including children's personal information. The NGFW offers advanced threat protection through features like Advanced Malware Protection (AMP), which provides real-time malware blocking and continuous analysis of file activity across the network. It also includes the SNORT Next-Generation Intrusion Prevention System (NGIPS) for traffic analysis and protocol inspection, leveraging threat intelligence from Cisco Talos® to protect against emerging threats. These capabilities ensure that organizations handling children's data can maintain compliance with COPPA by preventing unauthorized access and data breaches.

Cisco XDR

Cisco Extended Detection and Response (XDR) can significantly aid in meeting COPPA by providing comprehensive threat detection and response capabilities. Cisco XDR integrates data from multiple security layers, offering a unified view of an organization's security posture, which is crucial for protecting sensitive data, including children's personal information. It leverages extensive integration with Cisco and third-party security tools, providing visibility across the entire IT infrastructure, and employs robust threat intelligence from Cisco Talos to ensure protection against emerging threats. This comprehensive approach helps educational institutions and other organizations handling children's data to maintain compliance with COPPA by safeguarding personal data from unauthorized access and breaches.

Cisco Umbrella

Cisco Umbrella® can assist in meeting COPPA by providing a comprehensive cloud-native security solution. It offers DNS-layer security, which blocks requests to malicious domains before they reach your network or endpoints, thereby preventing unauthorized access to children's data. Additionally, Umbrella's secure web gateway and cloud-delivered firewall provide robust protection against phishing, malware, and ransomware, ensuring that children's online activities are safeguarded. By integrating threat intelligence and security services into a single platform, Cisco Umbrella helps organizations maintain compliance with privacy regulations like COPPA, protecting children's data from breaches and unauthorized access.

Cisco Secure Endpoint

Cisco Secure Endpoint helps meet COPPA mandates by providing comprehensive endpoint protection. It offers advanced Endpoint Detection and Response (EDR) capabilities, which allow for the detection, response, and remediation of threats across multiple domains. This ensures that any malicious activity is quickly identified and contained, reducing the risk of unauthorized access to children's data. Additionally, Cisco Secure Endpoint integrates with Cisco's broader security architecture, providing a unified defense against threats and enhancing compliance with privacy regulations like COPPA.

Cisco Secure Network Analytics (SNA)

SNA helps meet COPPA by providing comprehensive network visibility and threat detection capabilities. It continuously analyzes network activities to establish a baseline of normal behavior, using advanced analytics and machine learning to identify anomalies and potential threats in real time. This includes detecting insider threats, policy violations, and encrypted malware without compromising data privacy. By ensuring that security and compliance policies are enforced, Cisco Secure Network Analytics aids in protecting children's data from unauthorized access and breaches, aligning with COPPA's requirements.

Cisco Secure Access by Duo

Cisco Secure Access by Duo helps meet COPPA by providing robust Multi-Factor Authentication (MFA) and a zero-trust security approach. Duo verifies user identities and establishes device trust before granting access to applications, ensuring that only authorized users and compliant devices can access sensitive data. This aligns with COPPA's requirements to protect children's personal information by preventing unauthorized access and ensuring data security. Additionally, Duo offers detailed logs of access events and granular policy controls, which help organizations manage and restrict access effectively, further supporting compliance with data protection regulations.

Cisco Identity Services Engine (ISE)

ISE helps meet COPPA by implementing a zero-trust architecture that ensures secure access for users and devices across networks and applications. ISE acts as a policy decision point, enabling organizations to authenticate and authorize trusted endpoints and users, thereby preventing unauthorized access to sensitive data. It provides comprehensive Network Access Control (NAC) and supports dynamic policy enforcement, which aligns with COPPA's requirements to protect children's personal information by ensuring that only compliant devices and authorized users can access the network. Additionally, ISE offers extensive visibility and control over network access, which is crucial for maintaining compliance with data protection regulations.

Cisco Secure Email

Cisco Secure Email and Cisco Secure Email Threat Defense help meet COPPA compliance by providing a robust security framework that includes advanced threat protection capabilities that detect, block, and remediate threats faster, preventing data loss and ensuring privacy protection standards. Additionally, the Cisco Secure Email Encryption Service provides enhanced control by securing sensitive information in transit with end-to-end encryption. This is crucial for protecting children's personal information online.

Cisco Web Security Appliance

The Cisco Web Security Appliance (WSA) helps meet COPPA by providing robust web security features that protect against unauthorized access and data breaches. It leverages Cisco Talos for web categorization and reputation, allowing administrators to enforce policies that block or allow web content based on categories, user types, and IP ranges. The WSA also supports advanced malware protection and data loss prevention, which are critical for safeguarding children's personal information online. Additionally, it offers flexible deployment options and integrates seamlessly with existing security infrastructures, ensuring comprehensive protection across all network layers.

Cisco User Protection Suite

The Cisco User Protection Suite can help meet the 2025 Children's Online Privacy Protection Act (COPPA) Computer Security Safeguards by providing comprehensive security measures that protect user data and privacy. This suite offers robust protection against various attack vectors targeting users, such as phishing, malware, and credential compromise, while ensuring seamless and secure access to applications and data. By implementing zero-trust principles and integrating advanced threat detection and response capabilities, the suite helps organizations maintain compliance with privacy regulations like COPPA, ensuring that children's data is safeguarded against unauthorized access and breaches.

Cisco Cloud Protection Suite

Tailored for hybrid and multicloud environments, the Cisco Cloud Protection Suite helps meet COPPA by providing the critical capabilities to prevent unauthorized lateral movement and the ability to protect against application vulnerabilities using surgical compensating controls. The also suite delivers foundational security to stop inbound attacks and data exfiltration, as well as advanced protection against zero day exploits and to block malware in encrypted traffic. The Cloud Protection Suite marries simplicity, flexibility, and investment protection for easy adoption of Cisco's Hybrid Mesh Firewall.

Cisco Breach Protection Suite

The Cisco Breach Protection Suite helps meet COPPA by providing a comprehensive security framework that integrates detection, prevention, and response capabilities. It leverages AI and cross-domain telemetry to deliver intelligent, integrated protection across email, endpoints, network, and cloud environments. The suite empowers security analysts to quickly detect and respond to advanced threats like ransomware and data exfiltration, ensuring compliance with privacy protection standards. Additionally, it enhances threat detection and streamlines security operations, which are essential for maintaining robust security postures in compliance with COPPA.

C07-5057520-00 04/25