Global Encryption Day – October 21 2024 - Encrypt Today to Safeguard Tomorrow: The Encryption Summit

Encriptación, el Guardián

Sharayah Lane - Internet Society: Gracias a todos por unirse a nosotros en el panel de hoy, The Guardian. Hoy vamos a hablar sobre la encriptación y los impactos que tiene en la seguridad de los niños en línea. Mi nombre es Sharayah Lane. Soy Asesora Principal en la Internet Society y también miembro de nuestro equipo de encriptación.

Gran parte de mi trabajo con el equipo de cifrado se ha centrado en la seguridad infantil en línea, y esta es un área relativamente nueva que muchos de nosotros estamos explorando. Será una buena discusión hoy. Tenemos algunos oradores maravillosos. Cuando se trata del tema del cifrado y la seguridad infantil en línea, la discusión principalmente se ha centrado en los perpetradores de abusos y explotación de niños en línea.

Lo que no escuchamos tanto, sin embargo, es el papel que juega la encriptación en mantener a los niños seguros en línea. Hoy abordaremos este tema con nuestro panel de expertos. Nuestros panelistas trabajan en áreas que se centran en el uso seguro de Internet por parte de los niños. Son académicos que realizan investigaciones en este campo, y el objetivo de la sesión de hoy es que nuestros asistentes obtengan una mejor comprensión de cómo la encriptación contribuye a la seguridad de los niños en línea, para apoyar a cada uno de ustedes, nuestros asistentes, en ser mejores defensores de la encriptación con más información que puedan añadir a sus propias áreas de trabajo.

Y además de la conversación de hoy, tres de nuestros panelistas también contribuyeron a un documento de trabajo colaborativo que profundiza más en este

tema. Si estás interesado en leer ese documento, puedes encontrarlo aquí, y lo publicaré en el chat para que puedas encontrarlo si te interesa leer más.

Pero primero presentaré a nuestros panelistas. Primero, tenemos a Jessica Dickinson Goodman. Jessica une los mundos de la tecnología y la política. Se desempeña como ex presidenta de la junta directiva de la Internet Society del Área de la Bahía de San Francisco y apoya el trabajo excepcional de su equipo en políticas tecnológicas, educación y ayuda a comunidades desatendidas para obtener mejor acceso a Internet.

También es autora del libro de 2023, "Encriptación para bebés". A continuación, tenemos a Larry Magid. Larry es Doctor en Educación y también es CEO de ConnectSafely.org. Es un veterano periodista de tecnología. Escribe una columna semanal para el San Jose Mercury News y es el presentador del informe ConnectSafely, que se emite dos veces por semana en CBS News Radio en los EE. UU. Frecuentemente es invitado en programas de televisión y radio nacionales y locales, tanto en los EE. UU. como en el Reino Unido. Durante 20 años fue analista de tecnología en el aire para CBS News y es el presentador del popular programa de CBS "Eye on Tech". A continuación, tenemos a la Dra. Sabine Witting. La Dra. Witting es profesora asistente de derecho y tecnologías digitales en la Universidad de Leiden.

Su investigación se centra en la intersección de los derechos humanos, incluidos los derechos de los niños, con la tecnología digital. También es cofundadora de TechLegality, una firma de consultoría especializada en derechos humanos y tecnologías digitales. Sabine es investigadora no residente en el Centro para la Democracia y la Tecnología.

A continuación, tenemos al Dr. Ezequiel Passeron. El Dr. Passeron tiene un Doctorado en Educación y Sociedad por la Universidad de Barcelona y es licenciado en Ciencias de la Comunicación por la Universidad de Buenos Aires. También tiene una Maestría en Entornos de Enseñanza y Aprendizaje Mediados por Tecnologías Digitales. Es de la Universidad de Barcelona.

Es el Director de Educomunicación en Faro Digital, una ONG que estudia y desarrolla proyectos en alfabetización mediática. También es Profesor Asociado en la Universidad de Barcelona, Coordinador de la Red Conectados al CERN y Investigador en el Grupo de Investigación ESBRINA. Sus intereses se centran en el estudio y análisis de las intersecciones entre educación, comunicación, plataformas digitales y entornos de inteligencia artificial.

Por último, tenemos al Dr. Mark Leiser. El Dr. Leiser es un teórico regulador especializado en la regulación digital, legal y de plataformas. Su enfoque está en el derecho y las tecnologías digitales, como los derechos fundamentales, el comercio electrónico, la teoría regulatoria, la regulación de plataformas, los contratos, la seguridad, la privacidad, la libertad de expresión, el cibercrimen y los fenómenos relacionados con el diseño engañoso.

Patrones oscuros, protección al consumidor y el uso y regulación de la IA y las tecnologías digitales. Así que tenemos mucha experiencia en la llamada de hoy. Muchas gracias a todos por estar con nosotros y compartir su tiempo y su experiencia sobre el tema. Lo apreciamos mucho. Con eso, procederemos a nuestra sesión de preguntas y respuestas.

Vamos a tener algunas preguntas específicas para nuestros panelistas. También animamos a todos nuestros asistentes a enviar sus preguntas utilizando la función de preguntas y respuestas. Tendremos tiempo cerca del final de nuestra llamada de hoy para abordar sus preguntas y plantearlas a los panelistas.

Pero con eso, comenzaremos nuestra conversación y empezaremos con Larry Magid. Entonces, Larry, has trabajado significativamente en el ámbito del compromiso en línea de los niños. ¿Puedes darnos una visión general de lo que has aprendido sobre cómo la encriptación juega un papel en el uso de Internet por parte de los jóvenes?

Larry Magid - ConnectSafely.org: Gracias. Primero, quiero reconocer que hay un gran número de personas bien intencionadas que han argumentado que el cifrado es necesario para que las fuerzas del orden puedan prevenir la explotación de niños, y están pensando específicamente en el material de abuso sexual infantil (CSAM).

Hay controversia dentro de la comunidad de protección infantil, y francamente creo que la mayoría de mis amigos y colegas en esta comunidad no estarían de acuerdo conmigo. Y argumentan que la necesidad de prevenir el CSAM, con lo cual, por supuesto, estoy de acuerdo, pero que la necesidad de las fuerzas del orden, que la encriptación se interpone en su camino y, por lo tanto, causa daño.

Y eso probablemente hace que el trabajo de las fuerzas del orden sea más difícil. Todos los problemas tienen ciertos matices y concesiones, y de ninguna manera quiero, de ninguna forma, restar importancia al bloqueo y la prevención del material de abuso sexual infantil, conocido como pornografía infantil, así como la persecución de aquellas personas que trafican de manera que dañan y abusan de los niños.

Dicho esto, también es importante señalar que los niños mismos necesitan protección contra las posibles violaciones de privacidad y seguridad que pueden ocurrir en un mundo sin cifrado. Hay muchos ejemplos que van desde brechas de datos donde la información de los niños ha caído en manos de criminales o posibles criminales, o donde su información ha sido simplemente revelada de maneras que violan su privacidad.

Incluso se podría argumentar que la encriptación protege a los niños contra los depredadores infantiles, porque el poder acceder a la información de los niños facilita a quienes quieren abusar de ellos encontrarlos, alcanzarlos y explotarlos. Así que esto es un arma de doble filo.

Pero yo, al reflexionar mucho sobre esto, creo que, claramente, la capacidad de proteger la privacidad y la seguridad de los niños es un derecho fundamental que debe mantenerse. Y las fuerzas del orden necesitan encontrar otras formas dentro del régimen de un mundo encriptado para poder cumplir con su responsabilidad de combatir el material de abuso sexual infantil.

Pero hay muchos ejemplos donde, nuevamente, mencioné las violaciones de datos, así que recuerdo que el Servicio Nacional de Salud en el Reino Unido tuvo una violación importante hace algunos años con información sobre niños. Hay muchos casos de datos escolares que han sido violados y hay muchos casos de niños que se comunican directamente con otros de una manera que podría haber sido violada o tal vez ha sido violada como resultado de la falta de una plataforma encriptada.

Así que creo que todos merecemos protección. Ya sea en bancos y transacciones financieras, ya sea para activistas en varios países, y por cierto, los niños pueden estar entre los activistas. Cuando pensamos en personas que están involucradas en actividades que los gobiernos quieren suprimir, en muchos casos, estos son menores de edad, adolescentes, ciertamente, que están involucrados en actividades alrededor del mundo, donde tener la capacidad de mantener comunicaciones privadas y confidenciales es esencial no solo para su misión de intentar reformar cosas, sino también para la protección de sus propias vidas, porque a menudo hay un gran peligro asociado con ser parte de un movimiento, sin importar la edad que tengas.

Y hay tantos ejemplos que necesitamos señalar. Y supongo que lo que estoy tratando de hacer dentro de la comunidad en la que opero es hacer que la gente piense más allá del simple deseo de las fuerzas del orden de proteger, sino en el tema más amplio de proteger toda nuestra seguridad y privacidad. Y finalmente, y esto no fue una idea original mía, sino de uno de mis colegas que ayudó a trabajar en este documento que mencionaste antes, hizo el punto de que la encriptación a menudo puede usarse para ayudar a detectar y procesar crímenes, pero en, lo siento, la falta de encriptación podría hacer más fácil procesar crímenes, pero la encriptación ayuda a prevenir crímenes.

Y dado a elegir entre procesar y prevenir, elegiría la prevención cada vez. Sería genial dejar sin trabajo a los fiscales porque eliminamos el crimen. Probablemente nunca lo logremos. Pero si podemos reducir el crimen protegiendo la seguridad de las personas, eso significa menos casos que los fiscales tienen que perseguir.

Sharayah Lane - Internet Society: Eso es genial. Gracias, Larry. Y quería pasar a Jessica. Sé que Jessica tendrá que dejar la llamada temprano, así que gracias por estar con nosotros. Y mi pregunta para ti es, ¿qué te motivó a escribir el libro "Cifrado para bebés"? ¿Cuál era tu esperanza de que los lectores se llevaran después de terminar ese libro?

Jessica Dickinson Goodman - SF Bay ISOC: He estado interesado en la encriptación desde que hice una pasantía en la Electronic Frontier Foundation cuando estaba en la

escuela secundaria, porque soy ese tipo de persona y ese tipo de nerd. Pero en ese momento, estaba en casa con mi hijo, que cumplirá dos años en tres semanas. Y le estaba leyendo muchos libros sobre cosas como la astrofísica para bebés.

Hay una serie de libros de cartón que muchos niños pequeños tienen en los Estados Unidos sobre estadísticas para bebés y astrofísica para bebés. Y yo quería explicarle la encriptación. Pensé que sería un desafío interesante y él es un chico inteligente. Y siempre es complejo, ¿verdad? ¿Cómo explicas algo que no es físico, que es técnico?

Pero pensé que si podíamos leer astrofísica para bebés, podríamos encontrar una manera de hablar sobre la encriptación. Así que cuando lo escribí y lo probé con él, y luego hice que mis amigos lo probaran con sus hijos, y luego organicé un evento emergente en el centro de Mountain View, pasé siete horas pidiendo a cada persona técnica que pasaba que intentara desafiar las metáforas que usé allí, y no encontraron errores técnicos, lo cual fue maravilloso.

Y luego ponerlo en línea a la venta para beneficiar a mi capítulo en San Francisco, mi objetivo principal era ayudar tanto a los niños como a los padres que les leen a sentirse más cómodos con la encriptación. A veces, cuando dices que te importa la encriptación, como yo actualmente en Georgetown haciendo estudios de posgrado en la Escuela de Servicio Exterior, y deseé a todos un feliz Día Global de la Encriptación para aquellos que lo celebran.

Y no todos se sentirán inmediatamente cómodos con la idea. Ahora hay un estigma asociado a querer mantener la privacidad de tus hijos en algunos espacios, como mencionaba el Sr. Vedgett, particularmente en el área en la que ambos trabajamos en Silicon Valley, donde existe una narrativa muy fuerte de las fuerzas del orden sobre intentar facilitar su trabajo en la persecución de delitos.

Y solía trabajar para el Departamento de Justicia de California. Me importa ese trabajo también. Pero esta es una herramienta esencial para que los padres puedan mantener a su familia segura, y entenderla lo suficientemente bien como para explicársela a un niño pequeño es valioso, en lugar de enfrentar la avalancha de tácticas de miedo, tratando de dar a los padres un poco de cuerda para salir de toda esa presión de estar en contra del cifrado.

Porque creo que es algo bueno querer proteger la ubicación, la privacidad y las fotos de tu hijo. Y puedo entrar en detalles técnicos con otros adultos, pero mi pequeño no necesita saber sobre todas esas cosas. Diré que no estaba seguro de si iba a incluir la frase E2EE en el libro, y resulta que es la parte favorita de mi pequeño.

Él dice, ¡E2EE! Piensa que es muy divertido decir esa parte y me pide que la repita una y otra vez. Así que a veces podemos ponernos un poco técnicos incluso con nuestras audiencias más jóvenes y podrán seguirnos el ritmo, al menos si es divertido decirlo en voz alta.

Sharayah Lane - Internet Society: Me encanta eso. Me encanta esa historia. Y también estoy deseando leer el libro.

Tengo un pequeño que tiene aproximadamente la misma edad, así que será divertido. Antes de que te desconectes, Jessica, quería hacerte una última pregunta mientras aún te tenemos aquí. Has trabajado extensamente en el papel de la encriptación para proteger los derechos reproductivos de las mujeres en los EE. UU. ¿Puedes compartir más sobre este trabajo y cómo se conecta con la seguridad de los niños a través de la encriptación?

Jessica Dickinson Goodman - SF Bay ISOC: Absolutamente. Después de que se filtró la decisión de Dobbs, fui a mi junta directiva. Para aquellos que no están familiarizados, la mayoría de los capítulos son completamente voluntarios, así que comenzamos a hablar, sabíamos que era un tema sensible, pero queríamos empoderar a las personas con información para mantener sus datos seguros. Durante todo el año en que se filtró la decisión de Dobbs, y cuando se hizo pública, nuestro capítulo realizó mensualmente lo que yo llamo entrenamientos de soporte técnico táctico, abiertos a cualquier persona en el mundo.

Creo que tuvimos representación de media docena de países. Muchas personas de estados como Texas, donde el gobierno está activamente buscando recopilar información privada. Y nos enfocamos en dos estudios de caso. Uno era una joven que estaba tratando de buscar atención para un aborto desde Texas y necesitaba salir y recopilar esa información sin, como ha sido el caso, ser demandada por una pareja o arrestada por la policía, o que sus amigos o familiares fueran demandados, arrestados o multados, lo cual es actualmente la ley vigente que está siendo impugnada en Texas y que muchas personas que buscan atención para un aborto están enfrentando.

El otro estudio de caso fue de una persona joven que estaba en Alabama y que buscaba atención de afirmación de género fuera del estado y tenía una preocupación en casa. Así que esos son los dos estudios de caso. Atención de salud reproductiva donde tienes una preocupación sobre el estado husmeando en tu información y usándola para perjudicarte. Y el otro era preocuparse por los miembros de la familia husmeando y potencialmente siendo violentos debido a esa información.

Así que trabajamos en cuáles son los problemas logísticos, cuáles son las herramientas técnicas. Mucho de esto fue inspirado por ser una persona queer, una madre y una mujer. Y necesito esas herramientas. Para poder ser libre en el mundo de la misma manera que las personas sin úteros son libres en el mundo, y de la misma manera que las personas heterosexuales son libres en el mundo, y necesito poder tener privacidad porque mi gobierno, aunque aspiro a trabajar para él algún día y he trabajado para él en el pasado, no representa a todos los estadounidenses, no solo a los estadounidenses que están de acuerdo conmigo y que quieren que esté segura y feliz.

Y esa serie de entrenamientos fue importante para mí, importante para nuestro capítulo e importante para las personas que asistieron, porque guiaba a la gente sobre cómo configurar WhatsApp, cómo usar Tor Browser, ¿qué es esto? Y la mayoría de las preguntas surgían de ese miedo del que hablaba el Sr. Magic, de que la gente no estaba segura de si estas herramientas eran para ellos.

Y si estas herramientas eran seguras para que las usaran. Y una vez que hablamos de ello, la mayoría de las personas se sintieron cómodas avanzando y usando más herramientas de cifrado. Pero creo que recordar que las personas en el gobierno son solo personas y los miembros de la familia son solo familias y van a ser buenos y malos y feos y maravillosos, como cualquier otra persona, y no merecen acceso especial a la ubicación.

imágenes o comunicaciones, pueden obtener una orden judicial como lo habrían hecho hace cien años y conseguir esa información. No necesitan tener acceso especial solo porque es 2024. Así que eso fue lo que hicimos y la información de capacitación sigue en línea. La Electronic Frontier Foundation tiene un maravilloso marco de defensa digital que utilizamos.

También el sitio web Plan C, lo usamos para encontrar información sobre el cuidado del aborto, lo cual era importante, y se está volviendo aún más importante a medida que más estados están aprobando leyes para criminalizar el acceso a la atención de afirmación de género y la atención de salud reproductiva.

Sharayah Lane - Internet Society: Gracias por eso, y gracias por todo el excelente trabajo que haces.

Voy a pasar a Sabine. Y gracias por estar con nosotros hoy. Entonces, tuviste un rol con la ONU trabajando en Namibia y Zimbabue en temas de reforma de leyes y políticas sobre ciberdelincuencia, responsabilidad del sector privado y tecnologías digitales. ¿Cuáles fueron algunos de los hallazgos clave que surgieron en este trabajo con respecto a la seguridad de los niños en línea y, o con el papel del cifrado?

Dr Sabine K Witting - Leiden University: Sí, muchas gracias. Gracias por invitarme. Como decía, trabajé específicamente con UNICEF durante muchos años en el sur de África, pero también en la región de Asia Oriental y el Pacífico. Y una cosa que está surgiendo en muchos países del sur global es la conectividad y el acceso a las tecnologías digitales.

Y, por supuesto, eso también significa un mayor acceso y conectividad para los niños. Y aunque las tecnologías digitales pueden ser muy útiles para que los niños realicen sus derechos, también existen ciertos riesgos para los derechos de los niños. Y en particular, creo que el que recibe más atención es el derecho a la protección contra todas las formas de violencia, abuso y explotación.

Y creo que cuando estamos, cuando estábamos trabajando en estos temas aquí en la región, una de las cosas a las que siempre llevábamos a los legisladores y responsables de políticas era decirles: miren, por supuesto, es un tema emergente que parece algo nuevo, pero las dinámicas subyacentes de estas formas de violencia, abuso y explotación son exactamente las mismas que hemos visto en el entorno físico.

Entonces, cuando piensas en cómo prevenir y responder a este tipo de delitos, realmente necesitas pensar de manera más amplia y no solo en el espacio digital, sino en todo el sistema de protección infantil y cómo puedes fortalecer esos sistemas de protección para también poder responder a estos casos facilitados por la tecnología.

Reconocer esta conexión entre la violencia física y la facilitada por la tecnología fue realmente muy importante para desarrollar un enfoque holístico y no recurrir al solucionismo técnico, algo que todavía vemos mucho, no solo en el Sur Global, sino también en el Norte Global.

Así que creo que en la misma línea, cuando estamos discutiendo este tipo de intervenciones políticas y específicamente mirando el lado de la aplicación de la ley. Ciertamente también hay una falta de apreciación por la comunicación privada y la encriptación. Y creo que también es porque no valoramos de manera similar la privacidad y la seguridad en la comunicación para los niños.

Simplemente no parece ser algo en lo que la gente piense mucho. Por supuesto, la protección contra la violencia es muy importante, pero al mismo tiempo, realmente necesitamos considerar todo el espectro de los derechos de los niños. Y creo que una de las cosas que realmente me llamó la atención fue cuando estábamos trabajando con niños en Zimbabue en el desarrollo de la Política de Protección Infantil en Línea de Zimbabue.

Les preguntamos a los niños, ¿cuál es su experiencia en línea? ¿Qué cosas encuentran? Y, por supuesto, muchos niños dijeron que experimentaron varias formas de violencia, incluida la violencia sexual. Pero también hubo niños que nos dijeron que estaban usando una VPN para protegerse. Y cuando llevamos estos hallazgos a los legisladores en Harare, se podía ver que muchas personas en la sala, los legisladores, no sabían qué era una VPN.

Y creo que este es un aspecto bastante interesante del debate: las experiencias de los niños y su enfoque en lo que es importante para ellos en relación con las tecnologías digitales a menudo difiere de lo que los adultos consideran realmente importante. También vimos esto en la región del sur de Asia, donde les preguntamos a los niños qué quieren de las empresas tecnológicas para hacer que los productos y servicios digitales sean más amigables para los niños.

Y nuevamente, en la lista de deseos, muy alto en la lista de deseos, estaba una mayor protección de datos y privacidad. Y creo que esto es para nosotros y realmente para los

legisladores y creadores de políticas una buena llamada a la acción en términos de consultar a los niños, no solo sobre la declaración del problema. Entonces, ¿en qué medida experimentas A, B, C, D, sino también qué piensas de las soluciones que estamos proponiendo?

Y creo que es aquí donde faltan mucho las voces de los niños y, en realidad, no solo las voces de los niños, sino las voces de todos los grupos vulnerables que se ven afectados por, digamos, la encriptación, como dijo Jessica. Mujeres, personas queer, pero también defensores de los derechos humanos, todos ellos verían sus derechos considerablemente disminuidos.

Y creo que esto es algo en lo que simplemente no estamos tomando en cuenta las opiniones de las personas afectadas, lo que también incluye a los niños. Gracias.

Sharayah Lane - Internet Society: Gracias. Y sí, continuaremos esa conversación un poco más tarde con Larry, porque sé que Connect Safely tiene un Consejo Asesor Juvenil sobre el cual me encantaría aprender más.

Pero primero, quiero llegar a todos nuestros panelistas, ya que luego volveremos y saltaremos entre diferentes preguntas para nuestros distintos panelistas. La siguiente pregunta es para Ezequiel. Y esto en realidad continúa un poco con la pregunta de Sabine. Tu organización trabaja significativamente con jóvenes y sus familias.

¿Qué suelen hacer los padres sin darse cuenta que puede estar exponiendo a sus hijos? ¿Qué podrían estar haciendo mejor? ¿Y cuál es el papel de la encriptación en todo esto?

Ezequiel Passeron - University of Barcelona: Genial. Gracias, antes que nada, por la oportunidad de compartir con estas personas maravillosas.

Creo que debemos celebrar estos espacios para tener tiempo y diálogo.

Creo que el primer problema que vemos en las familias es la falta de diálogo intergeneracional. En Argentina y Sudamérica, los niños y jóvenes están muy solos en el mundo digital. Los adultos desconocen sus prácticas y la cultura digital. Así que cuando surge un problema, no son las personas a las que los jóvenes recurren para dialogar.

En Faro, los principales problemas que estamos viendo cuando hablamos y escuchamos a los estudiantes, a los niños y jóvenes son la violencia digital, la desinformación y la mala información, una creciente personalización de la experiencia, las burbujas de filtro, la falta de contexto con la diferencia, todos los problemas que estas cosas están causando a la convivencia social y la democracia, y también la hipersexualización y la monetización de los imaginarios y subjetividades juveniles. Por eso, en nuestra ONG promovemos compartir momentos de conexión que fomenten el

diálogo, las conversaciones, tratando de no juzgar sobre temas que interesan a los jóvenes para entender el cuidado que necesitan. Creo que el cuidado es un gran concepto que debemos poner al frente. Más allá de eso, surgen prácticas adultas como, no sé, la crianza, por ejemplo, que implica compartir imágenes personales de niños y jóvenes y ellos ven que es un gran problema y no les gusta.

Muchos niños están comenzando a tener una identidad digital sin siquiera haber dado su consentimiento. En cuanto al papel del cifrado, creemos que es un gran aliado para las familias porque es algo que generalmente se desconoce en nuestro país. Estudiamos la guía de cifrado de ISOC que acabas de compartir y vemos una gran oportunidad de entregarla en las escuelas.

Creemos que este tipo de herramientas, sumadas a talleres educativos y, nuevamente, teniendo tiempo y espacio para dialogar y construir reflexión, podrían ser un enfoque integral para alcanzar a estos aliados clave en la protección y cuidado de los jóvenes. La familia a menudo habla sobre controles parentales, contraseñas o tiempo de pantalla seguro.

Como dijo Sabine anteriormente, queremos un botón para resolver todos nuestros problemas. Y pensamos que la encriptación podría ser una técnica realmente buena para ponerla por encima de los cuidados que debemos tener. Con los niños y jóvenes.

Sharayah Lane - Internet Society: Sí, gracias. Es muy interesante este tipo de cambio en la dinámica que ha ocurrido incluso con cosas como la regulación.

Entonces, siempre ha sido responsabilidad de los adultos mantener a los niños seguros en varias áreas. Pero cuando se trata de espacios en línea y tecnología, a menudo los jóvenes están más informados, tienen más conocimientos y experiencia que algunas personas mayores. Así que realmente cambia la conversación y la dinámica de cómo llevar a cabo ese trabajo.

Sí, eso es realmente importante. Voy a pasar a Mark para nuestra próxima pregunta. Otro recordatorio, si tienen preguntas, asistentes en la audiencia, por favor colóquenlas en la función de Preguntas y Respuestas. Ya tenemos algunas que han llegado y las abordaremos en unos minutos, así que por favor sigan enviando sus preguntas para nuestros panelistas y tendremos tiempo para responderlas.

La academia desempeña un papel importante en la investigación y en el estudio de cómo los niños interactúan en línea. ¿Cuáles han sido algunos de los hallazgos clave de su investigación a lo largo de los años en relación con la encriptación?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Entonces, tal vez haga un poco de trampa y comience con una gran pregunta que estaba en la sesión de

preguntas y respuestas, la cual accidentalmente voy a responder en parte con mi propia respuesta a esa pregunta, así que solo quería destacar eso.

Diría que a lo largo de los años, ha habido innumerables incidentes en los que la encriptación ha proporcionado seguridad a los niños en sus interacciones digitales, pero también ha habido una falta de comprensión de su importancia, lo que los deja vulnerables. En la investigación que he realizado, y obviamente también el Dr. Witting, hemos encontrado que las plataformas no encriptadas exponen a los niños a riesgos. Desde el rastreo de ubicación, pasando por los metadatos, hasta el ciberacoso en aplicaciones de mensajería no protegidas. En contraste, el uso de sistemas encriptados reduce drásticamente estas amenazas. Por ejemplo, un caso involucraba a un niño que compartió su ubicación sin saberlo a través de una publicación en redes sociales, lo que llevó a que extraños aparecieran en su casa.

Y así, este incidente y otros similares destacan cómo la encriptación puede servir como un escudo, protegiendo los datos sensibles que no querríamos que cayeran en manos equivocadas. Pero, los niños y los padres aún carecen de la educación para reconocer su valor, lo que los hace susceptibles a amenazas digitales. Y la micro narrativa es tratar de observar estos incidentes específicos donde la encriptación habría mantenido a un niño seguro en un contexto determinado.

Pero a una escala más amplia, la integración de la encriptación en plataformas, escuelas y entornos de juegos ha tenido un impacto positivo sustancial en la seguridad infantil. La encriptación previene el acceso no autorizado a datos personales. Reduce el robo de identidad. Disminuye el ciberacoso y el acecho, y durante la pandemia, el cambio al aprendizaje en línea subraya aún más la importancia de la encriptación.

Cuando las escuelas hicieron la transición a sistemas de videoconferencia encriptados, se mitigaron los riesgos, como el Zoom bombing y las intrusiones digitales en las aulas virtuales. Persiste una brecha en la concienciación sobre el papel de la encriptación en la protección de los niños en línea. Como se ha dicho antes, la investigación y las políticas deben converger para abordar estas vulnerabilidades promoviendo la encriptación y expandiendo su implementación en las plataformas frecuentadas por los niños.

Y finalmente, esta especie de mega narrativa es que la encriptación está vinculada a los principios fundamentales de privacidad y seguridad. Y tiene profundas implicaciones para los derechos y libertades digitales. Mientras que el RGPD de la UE fomenta fuertemente la encriptación como un método para proteger los datos personales, el panorama global muestra diferencias marcadas en cómo se trata realmente la encriptación.

En los regímenes autoritarios, las restricciones a la encriptación permiten la vigilancia masiva, lo que socava la privacidad y los derechos humanos. Y la relación entre privacidad y seguridad se vuelve innegable. No son dos cosas separadas, son dos caras

de la misma moneda. La encriptación mantiene a las personas seguras. Sirve como un pilar clave para proteger a los individuos, especialmente a los niños y otros miembros vulnerables de la sociedad, de la explotación y el daño que los padres intentan desesperadamente evitar para sus hijos.

A medida que las sociedades se vuelven más dependientes de este tipo de infraestructuras digitales, leyes como el GDPR y las leyes que promueven la protección de datos y la privacidad por diseño son realmente vitales para garantizar la seguridad y la dignidad de las poblaciones vulnerables en todo el mundo. Gracias.

Sharayah Lane - Internet Society: Vaya, eso fue un excelente resumen.

Gracias, Mark. Y gracias por responder una de nuestras preguntas. Tenemos algunas más que están llegando. Así que, nuevamente, un recordatorio para nuestros asistentes: siéntanse libres de escribir sus preguntas a los panelistas en la función de Preguntas y Respuestas y tendremos tiempo para abordarlas un poco más tarde en nuestra llamada. Nuestra próxima pregunta es para Larry, y esto puede informar parte de lo que hemos estado hablando sobre incluir a los jóvenes en la conversación y, en última instancia, incluirlos en la solución.

Entonces, ConnectSafely tiene un Consejo Asesor de Jóvenes Adultos. ¿Cómo ha influido en su trabajo el hecho de trabajar directamente con jóvenes, y cuáles son algunas de las cosas clave que están escuchando de ellos ahora?

Larry Magid - ConnectSafely.org: Tener un consejo asesor juvenil realmente nos ancla de muchas maneras, y nos enseña algunas de las cosas a las que aspiran los jóvenes, y también nos muestra algunas de sus preocupaciones. Debo decirte que, en algunos aspectos, los jóvenes son un poco más conservadores que yo en ciertos temas.

A veces me sorprende lo preocupados que están por tantos peligros en Internet y lo ansiosos que están por ver más controles implementados. No hemos tenido conversaciones extensas sobre la encriptación. Planeamos hacerlo en el futuro como parte de nuestra agenda, pero me imagino que tendríamos una diferencia de opinión.

Eso parece ser, una de las cosas que aprendes al hablar con personas de cualquier demografía es que no puedes encasillar a ninguna demografía, ya sea por género, raza, orientación sexual, edad o cualquier otra cosa. Las personas son personas con diferentes opiniones. Pero en general, creo que ciertamente algunos de los jóvenes con los que he hablado tienen un deseo muy fuerte de ver un Internet que sea seguro y privado y realmente entienden la necesidad de la encriptación de manera similar a como lo mencionó Mark y otros, como una forma de protegerse de posibles abusos en línea.

Hay otros que podrían estar preocupados por las limitaciones o los desafíos que presenta para las fuerzas del orden, y eso es algo que sería parte de un programa educativo para tratar de que la gente entienda mejor por qué la encriptación es tan importante y cómo las fuerzas del orden aún pueden hacer su trabajo a pesar de tener herramientas, al igual que hacen su trabajo a pesar de las diversas protecciones legales que han estado en vigor en los Estados Unidos y otros países no autoritarios, en la medida en que Estados Unidos, con suerte, siga siendo un país no autoritario.

Pero sí, es muy importante para aquellos de nosotros en el mundo de las políticas hablar con los jóvenes. Y de nuevo, no hacer suposiciones sobre lo que podrían decir, sino darles un lugar en la mesa. De hecho, este año, como algunos de Connect Safely son los anfitriones en EE. UU. del Día de Internet Seguro.

Y este año vamos a tener una conversación sobre políticas en Sacramento, el gobierno estatal donde está la capital del estado en California, para tratar de proporcionar a los jóvenes un papel en la mesa, de modo que cuando los legisladores estén aprobando leyes, ya sea sobre encriptación, control parental, verificación de edad, redes sociales, o las llamadas leyes anti-adicción, o cualquier otra cosa, los jóvenes sean parte de esa conversación.

Queremos ver un aumento en el número. Nos gustaría ver más educación para los jóvenes sobre la encriptación. Una de las razones por las que Connect Safely ha hecho varios artículos y ha tenido el honor de ser el anfitrión del documento que este grupo ha elaborado, es porque queremos asegurarnos de que cada vez más jóvenes entiendan la encriptación.

Mi sensación es que para la mayoría de las personas, es un tema que realmente no han abordado. Así que hay una gran necesidad de tener muchas conversaciones educativas con personas de todas las edades, pero especialmente con adolescentes.

Sharayah Lane - Internet Society: Sí, gracias. Y compartí un enlace al Día de Internet Segura en el chat por si alguien está interesado en aprender más.

Larry Magid - ConnectSafely.org: Ah, por cierto, este año estamos otorgando subvenciones, como lo hemos hecho en los últimos años, a educadores y organizaciones sin fines de lucro. Así que si alguien quiere hacer un programa sobre encriptación en su comunidad o en sus escuelas, tenemos subvenciones de hasta 1,000 dólares para maestros y organizaciones sin fines de lucro para ayudarlos a realizar educación comunitaria en torno al Día de Internet Seguro este próximo febrero.

Así que por favor revisen en un par de semanas cuando se lancen las solicitudes.

Sharayah Lane - Internet Society: Sí, gracias por ese recurso. Es una excelente manera de dar seguimiento a la llamada de hoy también. Así que quería, con eso, pasar

a Ezequiel para continuar esta conversación porque Ezequiel, tú también trabajas muy de cerca con niños, jóvenes y sus familias.

Y espero poder hacerte la gran pregunta y que podamos hablar del elefante en la habitación: materiales de abuso sexual infantil, materiales CSAM. También he visto un comentario sobre esto en el chat. Entonces, ¿cómo nos protegemos de eso? ¿Y qué hay en esa caja de herramientas? ¿Y cuál es parte del trabajo que han estado haciendo en FonoDigital sobre esto?

Ezequiel Passeron - University of Barcelona (2): Como te mencioné antes, la hipersexualización de la sociedad, y también de los niños, es un tema importante que debemos enfrentar, y la forma en que interactuamos con las plataformas digitales tiene algo que ver en ese contexto. No creemos en la determinación de los medios de comunicación masivos sobre nuestras prácticas, pero sin duda tiene una fuerte influencia.

En Argentina, tenemos un trabajo significativo realizado por fiscales especializados en ciberdelincuencia. Sabemos que hay una amplia cooperación internacional, especialmente con la red NMAC, que facilita el intercambio de información sobre casos y el progreso de las investigaciones en cada instancia. El hecho es que este tipo de casos, lo llamamos en español, masi, siempre tenemos este malentendido de pornografía infantil.

Es material de explotación sexual infantil y tenemos que. Tenemos que decirlo en voz alta para entender el gran problema. Está emergiendo cada vez más. Tenemos muchos casos de niños y escuelas que no saben cómo, qué hacer. Así que, hay un papel clave ahí para involucrarse con los fiscales.

Y las comisarías de policía que están trabajando en este tipo de casos. También estamos viendo en nuestros talleres que tecnologías como la IA se están utilizando para generar imágenes de niños que violan sus derechos y privacidad. La semana pasada tuvimos un caso reciente que estuvo en la cima de las noticias y los medios.

¿Y cómo podemos protegernos de esto? ¿Y con qué herramientas? Creo que esas son las preguntas clave que debemos hacernos. Una vez más, enfatizamos en la educación, en la ciudadanía digital y en la creación de espacios de diálogo. Creo que este tipo de temas sexuales a veces son un poco tabú en nuestras sociedades.

Pero cuando los niños están en Internet y entre plataformas digitales, no hay tabú. Aprendemos haciendo. Y la mayoría de las veces, antes de tener un espacio para cuestionar, descubrimos nuestra sexualidad con nuestros padres o con un adulto de confianza. Creemos en la educación, creemos en el diálogo y en crear espacios seguros para que los niños expresen sus curiosidades y todas las cosas que necesitan aprender paso a paso. Estas son las principales cosas que debemos promover y defender.

Sharayah Lane - Internet Society: Sí, y realmente hay muchas maneras diferentes de ver esto. No hay una respuesta clara y creo que eso es realmente el núcleo de nuestra llamada hoy, abordar el problema. Cuando se trata de la encriptación y el impacto en la seguridad de los niños en línea, gran parte del enfoque ha estado en los perpetradores de abuso y en los adultos y la comunidad.

Las implicaciones de la encriptación para los jóvenes en línea se pierden realmente en esa conversación. Entonces, ¿cómo mantener una salvaguarda para los jóvenes en línea a través de la encriptación mientras se persigue y aborda el problema de los materiales de abuso sexual infantil? Es una pregunta abierta en este momento, y es algo en lo que muchas personas están trabajando y reflexionando.

Y realmente es uno de los grandes desafíos del momento porque, como hemos escuchado de nuestros ponentes anteriores, la cantidad de formas en que la encriptación juega un papel para los jóvenes. Así que simplemente eliminarla también tiene un efecto. Así que gracias por un poco más de contexto sobre eso. Sé que siempre es una pregunta difícil.

Y Sabine, quería volver contigo. Has trabajado extensamente asesorando a los responsables de políticas en todo el mundo sobre tecnología. ¿Cuál es una de las cosas clave que aconsejas a los responsables de políticas en cuanto a la seguridad de los niños en línea?

Dr Sabine K Witting - Leiden University: Sí, muchas gracias por esa pregunta. Por supuesto, siempre partimos de un enfoque basado en los derechos humanos y los derechos del niño.

Nuestro consejo clave es realmente que no podemos aislar la seguridad de los niños y su derecho a la protección de otros derechos de los niños. Y según la Convención de las Naciones Unidas sobre los Derechos del Niño, todos estos diferentes derechos de los niños son interdependientes, indivisibles y están interrelacionados.

Esto significa que no podemos avanzar en un derecho sin considerar el impacto adverso o los impactos positivos de otros derechos en la convención. Y cómo se traduce esto en términos de asesoramiento, lo que los legisladores deberían hacer concretamente cuando se encuentran en una situación en la que piensan en leyes y políticas.

El primer paso para la seguridad en línea de los niños es realizar una evaluación del impacto en los derechos humanos, incluyendo un enfoque específico en los derechos de los niños. Y lo que eso significa es utilizar realmente la metodología propuesta por los Principios Rectores de la ONU sobre Empresas y Derechos Humanos, para pensar, de acuerdo, cuáles son los derechos humanos afectados en general, no solo para los adultos, sino específicamente para la población vulnerable y los niños.

Y luego, un segundo paso es pensar, bien, hasta qué punto. ¿Hasta qué punto se ven afectados estos derechos? ¿Cuál es la escala? ¿Cuál es el alcance en varias jurisdicciones? Y creo que esto es algo que siempre destacamos, que incluso si eres la UE y estás considerando políticas que afectan el cifrado de extremo a extremo, debes saber que esto tiene un impacto en las leyes y políticas de todo el mundo.

Y como dijiste, trabajamos en estas decisiones políticas en todo el mundo, y no puedo decirte cuántas veces hemos visto disposiciones, por ejemplo, del Acta de Seguridad en Línea del Reino Unido, copiadas y pegadas en nuevas leyes de ciberseguridad donde el contexto obviamente es muy diferente en países donde el estado de derecho podría no ser igualmente respetado, y eso, por supuesto, es una gran preocupación.

Entonces, una vez que se ha realizado esta evaluación del impacto en los derechos humanos, realmente necesitamos pensar en, bien, ¿qué medida podemos implementar ahora que considere todos estos diferentes derechos afectados? Y es aquí donde el término proporcionalidad se vuelve importante, y creo que cuando miramos los debates sobre la seguridad infantil y el cifrado de extremo a extremo.

Todos afirman que sus medidas son proporcionales. Y lo que me llama la atención es que la gente parece pensar que la proporcionalidad no tiene realmente una metodología. Es simplemente algo que sientes, si una cosa u otra es más importante, entonces simplemente afirmas la proporcionalidad de esa medida específica.

Y creo que, por supuesto, viniendo de Alemania y trabajando mucho en la UE, ponemos mucho énfasis en la metodología detrás de las pruebas de proporcionalidad. Y hay dos cosas que me gustaría destacar. La primera es preguntar, ¿es realmente necesaria esa medida? ¿Tenemos alguna medida igualmente efectiva pero menos intrusiva?

Y solo una vez que hayamos agotado estas medidas, entonces podemos pensar en medidas más intrusivas. Y creo que cuando pensamos en medidas menos intrusivas, como estos enfoques sistemáticos para fortalecer el sistema de protección infantil, creo que todavía estamos fallando considerablemente en todos los ámbitos. Si miras algunas evaluaciones de los sistemas de protección infantil también en los países del Norte global.

La narrativa es casi siempre la misma. No tenemos suficientes trabajadores sociales. No tenemos suficiente personal de la ley especializado en estos temas. Los maestros no están capacitados. Los médicos no están capacitados para identificar casos de abuso y explotación. Entonces, mi pregunta es, incluso si detectáramos todas estas imágenes de abuso sexual infantil, ¿quién va a responder a eso?

Y. Entonces, la respuesta probablemente sea nadie, porque todavía no tenemos un sistema de protección infantil suficientemente equipado. Y creo que aquí es donde realmente necesitamos pensar si esta medida es realmente la mejor manera de abordar este problema. Y el segundo punto es sobre la proporción, la prueba de

proporcionalidad en sí, donde uno de los primeros pasos es realmente evaluar, bien, ¿a qué nivel está un derecho específico? Y ese nivel de infracción tiene una línea roja, y esto es lo que llamamos la esencia del derecho.

Y una vez que hemos alcanzado esa esencia de un derecho específico, entonces esa es una línea roja. Y luego, no importa realmente lo que esté en el otro lado de la balanza, por así decirlo, entonces este derecho está infringido. no puede ser infringido. Y creo que esta línea roja es algo en lo que realmente necesitamos pensar cuando hablamos de abolir o debilitar el cifrado de extremo a extremo en el contexto de las comunicaciones privadas, porque yo argumentaría que probablemente se ha alcanzado esa línea roja.

Esto es algo que creo que no se discute lo suficiente, y donde realmente necesitamos volver a los fundamentos del derecho de los derechos humanos, y evaluar desde una perspectiva holística lo que esta medida significa para los derechos humanos y los derechos de los niños en general. Gracias.

Sharayah Lane - Internet Society: No, gracias.

Y gracias por mencionar la convención de tener una forma de medir. Tener algo con lo que comparar es realmente útil y he leído la convención sobre los derechos del niño y creo que hay muchas cosas allí que son relevantes y que se alinean directamente con la encriptación y el acceso de los niños a la encriptación en línea.

Pero nuevamente, es una conversación en curso, así que quería pasar a Mark. Has realizado una cantidad significativa de investigación sobre el aspecto legal de la tecnología. ¿Existen actualmente leyes que apoyen la encriptación que deberíamos conocer? Si es así, ¿cuál podría ser su impacto? Si no, ¿por qué crees que es así?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Hay muy pocas leyes que realmente digan que debes tener, no creo que haya ninguna ley como la Ley de Cifrado o algo así, pero sí tenemos varias leyes que, en efecto, apoyan el cifrado. Como académico europeo que trabaja junto al Dr. Witting y en los Países Bajos y en el Reino Unido.

El RGPD obviamente tiene una especie de ley fundamental de privacidad de datos y protección de datos para la UE con efecto extraterritorial y algunos incluso podrían argumentar el efecto Bruselas, en el que otros países tienen que adoptarlo para cumplir con nuestras reglas y tener acceso a nuestro mercado.

Hay dos o tres cosas diferentes dentro de eso. Primero, la obligación del Artículo 25 de protección de datos desde el diseño y por defecto. Así que, si estás construyendo una tecnología donde podrías proteger la protección de datos, o tienes que proteger los datos, entonces al integrar la encriptación en la etapa de inicio no es una obligación

obligatoria hacerlo, pero ayuda a que las empresas piensen en los riesgos y tomen medidas para asegurar que los datos estén seguros y protegidos.

Ahora, ¿por qué es esto importante? Porque, según el Artículo 32, los responsables y encargados del tratamiento de datos están obligados a implementar medidas técnicas y organizativas adecuadas para asegurar los datos personales. Y una de las cosas que se destaca para garantizar la seguridad de los datos es la encriptación. Ahora, ¿cuál es el impacto de eso? El impacto es que, bajo el RGPD, si los datos encriptados se ven comprometidos en una brecha, pero permanecen inaccesibles debido a una encriptación fuerte, las sanciones para la empresa podrían reducirse significativamente.

Entonces se convierte en un gran incentivo para que las empresas implementen protocolos de encriptación. El hecho, la segunda cosa es, como insinué antes, es que el GDPR tiene un efecto dominó en las leyes de privacidad y protección de datos en todo el mundo. Muchas empresas, incluso aquellas fuera de la UE, adoptan la encriptación como una mejor práctica para el cumplimiento.

Gigantes tecnológicos globales como Apple, WhatsApp y Google han adoptado la encriptación de extremo a extremo en parte para alinearse con los estándares del GDPR. Y la encriptación de extremo a extremo de WhatsApp asegura que solo las partes que se comunican, en teoría, puedan leer los mensajes, incluso impidiendo que la propia empresa acceda al contenido.

Ahora en los EE. UU., la CCPA, la Ley de Privacidad del Consumidor de California, que a menudo se ve como el equivalente estadounidense del GDPR, enfatiza la importancia de asegurar los datos personales. No es obligatorio, pero se trata como un factor atenuante al evaluar las sanciones por violaciones de datos, al igual que el GDPR. Si una empresa sufre una violación pero puede demostrar que los datos comprometidos estaban encriptados, la responsabilidad y los daños pueden reducirse. La CCPA se ha convertido en un catalizador para las leyes de privacidad federales y estatales.

Si construyes leyes siguiendo el modelo de la CCPA, incorporar la encriptación se convierte en una medida de seguridad recomendada. La ley menos conocida sobre privacidad y protección de datos en la UE es la Directiva de Privacidad Electrónica. A menudo se la conoce como la ley de las cookies y regula la confidencialidad de las comunicaciones dentro de la UE.

La idea aquí es que esta ley y la regulación propuesta que la reemplazará, se espera que fortalezcan el papel de la encriptación para garantizar la confidencialidad de las comunicaciones electrónicas. Estas leyes en sí mismas, puedes ir a Brasil y ver la encriptación como una práctica de seguridad estándar para las empresas que operan en Brasil.

Ayuda a la encriptación a demostrar que han cumplido con la LGPD y también a mantenerse competitivos en los mercados globales. Y luego tienes otros sectores

específicos, como HIPAA en los EE. UU., la Ley de Portabilidad y Responsabilidad de Seguros de Salud. Nuevamente, no obliga a la encriptación, pero sí proporciona a los proveedores de atención médica, planes de salud y sus asociados comerciales la implementación de salvaguardas técnicas para proteger la información de salud.

Y así, es una salvaguardia direccionable, lo que significa que, aunque no es obligatorio, debe implementarse o documentar por qué una medida alternativa es suficiente. Entonces, incluso los sectores como HIPAA, la expansión de la encriptación en la tecnología de la salud, mientras construimos sistemas completos para compartir datos de salud de un proveedor a otro, para trabajar con médicos, hospitales y compañías de seguros, y demás, para transferir datos de salud de manera fluida y sin problemas de un lugar a otro, la encriptación se considera la herramienta para proteger la privacidad de esas comunicaciones.

Hay algunas enmiendas en la legislación de telecomunicaciones y otras en Australia bajo la Ley de Asistencia y Acceso. Hay otro ejemplo de intentar hacer obligatoria la encriptación. El último punto es por qué no hay más leyes que obliguen la encriptación. En algunas áreas, se trata de equilibrar la seguridad nacional y la privacidad.

Tocamos ese tema en mi discusión anterior. Los gobiernos son reacios a imponerlo porque podría interferir con las operaciones de seguridad nacional y de las fuerzas del orden. En otros países en desarrollo, parece que la infraestructura legal para apoyar la encriptación no ha evolucionado completamente, y por lo tanto no existen leyes de privacidad, y la encriptación no siempre ha sido una prioridad.

Y el tercero es la presión real de los regímenes autoritarios. Así que la encriptación se ve como una herramienta que puede permitir la disidencia, debilitando así el control estatal sobre la información. Como resultado, algunos regímenes están desalentando activamente el uso de la encriptación o están imponiendo restricciones legales sobre ella. Así que puedes ver la especie de dicotomía entre privacidad y seguridad y autoritarismo versus democracia.

Y creo que sé de qué lado quiero estar y lo dejaré así. Muchas gracias.

Sharayah Lane - Internet Society: Sí, gracias por ese resumen. Y creo que probablemente continuaremos parte de esa conversación en nuestro próximo panel, ya que será un tema importante. Y lo que es tan interesante sobre el aspecto legal de la encriptación es que se ve una gran diferencia, donde algunos lugares están trabajando para proteger legalmente este derecho a la privacidad y algunos países están trabajando para desmantelarlo por completo.

Y es interesante ver que hay una gran diferencia entre los dos y observar estas diferentes tendencias en todo el mundo. Esa es una parte importante de nuestro trabajo de defensa en ISOC: analizar las leyes de cifrado o las leyes que podrían socavar el cifrado en todo el mundo y realizar labores de defensa a nivel global.

Así que esa fue una gran visión general. Gracias por eso. Creo que tenemos tiempo para una más. Voy a proceder y hacer nuestra pregunta individual antes de pasar a la sesión de preguntas y respuestas. Última oportunidad, nos moveremos a la parte de preguntas y respuestas, así que si tienen preguntas para nuestros panelistas, por favor colóquenlas en la función de preguntas y respuestas en Zoom, que se encuentra junto al botón de chat y el botón de participantes en su pantalla.

Última pregunta, quería volver a Ezequiel. Y quería preguntar, ¿cuál es algo importante, y solo diré algo porque estoy seguro de que hay muchas cosas, pero cuál es algo importante que has aprendido al iniciar una organización como Faro Digital sobre las experiencias de los jóvenes en línea y cómo podemos trabajar para mejorar esas experiencias para ellos en el futuro?

Ezequiel Passeron - University of Barcelona (2): Genial. Gracias por la última pregunta. En los últimos años, debido a la economía de la atención y la forma en que operan las plataformas, hemos notado un creciente interés y una fuerte influencia en la subjetividad de los jóvenes respecto a lo que llamamos monetización. Esto se refiere a la búsqueda de gratificación y recompensas en cada acción, una característica común de cualquier red social.

Eso crea una dinámica donde Internet o el espacio digital se percibe como una fuente de ingresos desde casa sin aparentemente poco esfuerzo. Prácticas como el juego en línea, donde los adultos estamos muy preocupados, pero cuando vamos a talleres y escuchamos a los jóvenes, ellos no lo ven como una concepción vergonzosa.

Entonces, hay una brecha muy grande que necesitamos llenar. La venta de imágenes íntimas, las inversiones han surgido en Argentina. Hace unas semanas se implementó una regulación que permite a personas mayores de 13 años ingresar al mercado financiero. Y esa regulación no es algo aislado. Gracias.

Se refiere a una práctica que tienen en sus actividades en línea. Entonces, lo que vemos como un problema o más bien como un desafío es el tema de la confianza. Lo que los lleva a ser víctimas de estafas digitales, por ejemplo. En Argentina, hablamos de Poncidemia, un problema que es alimentado por la aparición de estos jóvenes influencers a los que llaman Poncipros.

Están todo el tiempo como, hermano, tienes que invertir en esto, tienes que tomar este curso, son supuestos influencers que animan a otros jóvenes a convertirse en sus propios jefes, tener tiempo libre, ganar mucho dinero cada mes desde sus sofás. Por supuesto, son las viejas estafas Ponzi que existían antes de Internet, pero que ahora han encontrado en las plataformas digitales vehículos para reclutar y atraer a más personas, especialmente en contextos económicamente desfavorecidos.

En el mundo digital, vivimos en un territorio donde nuestra atención es explotada, donde nuestras emociones y deseos están en el centro del negocio de las grandes

empresas tecnológicas. Por eso necesitamos crear, por eso hablo de crear tiempo y espacios, solo como una metáfora.

Necesitamos proteger, necesitamos cuidar, necesitamos crear estos espacios donde los niños y jóvenes puedan desarrollarse junto a otros. Donde puedan estudiar y practicar asuntos mundiales sin un objetivo, una meta o utilidad. Simplemente tratando de entender el mundo y renovarlo, como nos dijo Hannah Arendt hace medio siglo.

Nuestro tiempo es el tiempo de este gran problema, Wilson. CODIS, tenemos emociones paleolíticas, instituciones de la Edad Media y tecnologías divinas. Nos encanta esa frase. Creemos que estamos en una época en la que necesitamos recuperar el sentido de la frase de Descartes, Cogito Ergo Sum. Cuando pensamos en esa frase, la traducimos como, pienso, luego existo.

Pero cuando estudiamos la etimología de la palabra cogito, descubrimos que se refiere tanto a "pienso" como a "me importa". Así que les dejo una pregunta. ¿Quiénes son los encargados de la práctica del cuidado en nuestra sociedad? Creo que hay un gran y rebelde asunto revolucionario que debemos luchar y defender para poner los cuidados en otro lugar en nuestra sociedad.

Gracias.

Sharayah Lane - Internet Society: No, es un recordatorio excelente de que gran parte del desafío o el problema radica en la forma en que lo estamos viendo. Y la manera en que estamos abordando las cosas. Creo que mucho de cómo hemos abordado estos problemas hasta ahora ha sido desde una perspectiva y comprensión algo desactualizadas, y la necesidad de pensar profundamente sobre estas cuestiones y de realmente entender lo que los jóvenes están enfrentando y por lo que están pasando, y tomarse el tiempo para comprender eso.

Todas estas cosas son tan importantes en nuestra conversación más amplia. Gracias por mencionar el aspecto filosófico de esto, porque creo que es una pieza faltante. Una pieza faltante de la conversación. Así que vamos a, nos quedan solo unos minutos. Vamos a pasar a nuestra sesión de preguntas y respuestas del público.

Tengo una pregunta traducida aquí. Dice, y esto es para cualquiera de los panelistas, así que siéntanse libres de intervenir y responder. Encontré interesante la encriptación de imágenes de niños. Como un factor de protección contra el uso de imágenes de este usuario o perfil de no usuario, dependiendo de la edad del niño, ¿podría la encriptación usarse para buscar, seleccionar y eliminar imágenes de niños que no tienen autonomía para expresar su voluntad?

Larry Magid - ConnectSafely.org: Ciertamente podría usarse para ocultar esas imágenes y asegurarse de que no se compartan sin el consentimiento de un niño o de

sus padres. No estoy seguro de que pueda usarse de manera independiente para buscarlas. Tal vez algunos de los expertos técnicos tengan una respuesta para eso.

Pero ciertamente puede proteger la privacidad de esas imágenes para asegurarse de que solo lleguen a las personas con las que desean compartirlas.

Sharayah Lane - Internet Society: Sí, entonces, como una especie de medida retroactiva, o para volver atrás y eliminar y ocultar imágenes, no creo que la encriptación pueda usarse como esa clase de herramienta, sino más bien como una característica preventiva, así que evitaría el uso no autorizado de imágenes desde el principio, pero si,

Larry Magid - ConnectSafely.org: si hay una, al menos en los Estados Unidos, si hay una imagen sexualmente explícita de un niño en línea, puedes ir a, creo que es takeitdown.

org, es un servicio de NECMEC, y pueden eliminarla. Además, hay varios sitios que ayudan a combatir la pornografía vengativa y la distribución de imágenes íntimas de adultos. Así que hay herramientas que puedes usar para eliminarlas, pero no creo, como dijiste, que puedas cifrarlas retroactivamente.

Sharayah Lane - Internet Society: De acuerdo, y estoy obteniendo el enlace a ese recurso. También lo pondré en el chat. Y con eso, sé que creo que Mark respondió un poco a esto en su respuesta, pero también lo plantearé a todo el grupo. Cuando se trata de legislación y políticas sobre la seguridad en línea de los niños, hay una tendencia a propuestas de arriba hacia abajo, en lugar de medidas que podrían empoderar a los padres para tomar decisiones informadas sobre las actividades en línea de sus hijos.

Por ejemplo, una propuesta es restringir legalmente a los menores de usar las redes sociales después de ciertas horas. ¿Existe un equilibrio entre las reglas impuestas por el gobierno, como las leyes de privacidad de datos en los EE. UU., y el empoderamiento de los padres? Y dice, siéntanse libres de desafiar completamente mi planteamiento.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: ¿Puedo añadir algo a mi respuesta?

Sharayah Lane - Internet Society: Sí.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Sabina también levantó la mano. Estoy seguro de que tiene algo que decir al respecto. Creo que es importante que los padres se den cuenta de que los niños también tienen derecho a la privacidad respecto a sus padres. Y que a menudo hablamos de esto como algo que queremos dar a los padres para que tengan más control.

Pero también creo que debemos reconocer que la nueva norma debería ser que los niños tengan un espacio seguro para comunicarse libremente, sin la intervención de los padres. Y les daré un par de ejemplos muy rápidamente para enfatizar este punto. El primero es que hay muchas culturas donde ser LGBT es mal visto dentro del hogar.

Y si vas a explorar tu sexualidad, tu identidad sexual, quieres poder hablar libremente, sin que tus padres husmeen y revisen tus comunicaciones. El segundo, y más obvio para las personas en culturas occidentales, creo, especialmente en esta época, es para aquellos que buscan información sobre salud sexual y su identidad.

Y luego, el tercero es proteger al niño de comunicaciones que puedan ser dañinas, no deseadas o no solicitadas. Si les das un espacio seguro para comunicarse, el niño en realidad está capacitado para mantener alejados a otros niños. Esa es mi adición a la pregunta, pero creo que también es importante reconocer que los padres deben proporcionar al niño un espacio seguro donde pueda comunicarse libremente sin la supervisión de los padres.

Y estoy seguro de que Sabina también tendrá otras opiniones al respecto.

Dr Sabine K Witting - Leiden University: Sí, gracias, Sabine. Sí, muchas gracias. Creo que Mark también tocó ese punto. Creo que cuando siempre nos enfocamos en los padres, decimos, oh, no deberíamos hacer esto o no deberíamos infringir en la anti-encriptación. Deberíamos enfocarnos en la alfabetización digital y el papel de los padres.

Y estoy de acuerdo con eso. Y creo que, hasta cierto punto, hay una idea errónea de que pensamos que los padres siempre actúan en el mejor interés del niño. Y creo que ciertamente no es el caso. Y Mark mencionó algunos ejemplos donde eso en realidad podría no ser así, por lo que poner al padre a cargo no necesariamente hará que el niño esté más seguro, y creo que eso es algo a considerar.

Y también creo que en este debate, hay un poco de, es un, hay un enfoque en la encriptación de extremo a extremo o en la alfabetización digital, y es como si usáramos una medida o la otra. Y creo que eso deja a las empresas tecnológicas fuera del gancho un poco demasiado rápido. Porque aunque no queremos que creen brechas o respalden esta encriptación de extremo a extremo, queremos que las empresas tecnológicas creen un entorno seguro.

Para los niños, y eso debería hacerse a través de esfuerzos legislativos. Mark y yo hemos escrito un capítulo de un libro sobre esto, que creo que saldrá el próximo año, donde analizamos la Ley de Servicios Digitales, por ejemplo, y el tipo de medidas que esta ley impone a los intermediarios para crear activamente un entorno seguro para los niños, como la obligación de reportar material ilegal, crear mecanismos de reporte amigables para los niños y notificaciones.

Y así sucesivamente. Así que creo que ciertamente hay un gran papel para la alfabetización digital, pero no deberíamos poner toda la responsabilidad en los padres o los niños y dejar que las empresas tecnológicas se libren de su responsabilidad. Gracias.

Sharayah Lane - Internet Society: Sí, estoy de acuerdo. Gracias. Y Larry.

Larry Magid - ConnectSafely.org: Sí, varía según el país, pero en los Estados Unidos, hay una, no diría un consenso, pero la cultura se basa en la idea de que los padres controlan a sus hijos y todos los derechos de un niño realmente fluyen a través del padre, mientras que los europeos tienen una actitud algo diferente, creo, y el hecho es, como Mark dijo tan correctamente, que los niños necesitan un cierto grado de autonomía, incluso de sus propios padres, y no solo por las razones que Mark especificó, y todas eran muy buenas, que un padre podría tener una actitud diferente hacia la salud reproductiva, la identidad de género, la orientación sexual, etc.

Pero también, no todos los padres se sienten cómodos o están preparados para interactuar con las autoridades, y hasta las empresas de redes sociales pueden ser vistas como una autoridad. Pueden tener preocupaciones sobre la inmigración, que de alguna manera, al involucrarse en algo en línea por sus hijos, aumenten la posibilidad de meterse en problemas con las autoridades de inmigración.

Es posible que no tengan la alfabetización, ya sea técnica o lingüística. Puede que no estén al tanto, y hay niños que, desafortunadamente, tienen padres que no están preparados, tal vez debido a problemas de salud mental, o simplemente porque sus vidas son demasiado caóticas o están demasiado ocupados, etc.

No todos los niños reciben el apoyo de sus padres y no todos los padres están capacitados para proporcionar el tipo de apoyo y estructura de permisos que algunas de estas leyes requieren de ellos. Así que me preocupa que los niños se queden atrás por diversas razones, y esto antes de que se aprueben cualquiera de estas leyes.

Necesitamos pensar en las consecuencias no deseadas.

Sharayah Lane - Internet Society: Sí, es muy importante. Quiero agradecerles a todos por acompañarnos hoy. Nos quedan unos 6 minutos juntos y, al cerrar, me gustaría pedir a cada uno de nuestros panelistas un pensamiento final, una o dos frases sobre el papel de la encriptación en la seguridad de los niños.

Entonces, la pregunta para ustedes es: ¿por qué es importante la encriptación para ustedes cuando se trata de la seguridad de los niños en línea? Y podemos empezar con Mark.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Yo mismo. Creo que en una o dos frases, a nivel social, la privacidad y la seguridad no solo están vinculadas, sino que son pilares que se refuerzan mutuamente. Gracias. Una democracia en funcionamiento. Así que cuando los niños se sienten empoderados y seguros, sabiendo que su información personal no les causará daño, esto contribuye a una mayor sensación de seguridad infantil y confianza tanto en el entorno digital como en el físico.

Y al debilitar las protecciones de privacidad, se puede llevar a una pérdida de seguridad. Y creo que cuando se prioriza la privacidad y la seguridad del niño, se asegura la protección de sus derechos, sus libertades civiles y su confianza en las tecnologías digitales.

Sharayah Lane - Internet Society: Wow, eso es bueno. Ezequiel, pasamos a ti.

Ezequiel Passeron - University of Barcelona: Es complicado seguir después de Mark.

Gracias por eso. Sí, creo que por un lado realmente necesitamos hacer preguntas más amplias para, como nos dijo Sabine antes, siempre tratamos de pensar en una solución técnica para los problemas que tenemos en nuestra relación con las técnicas. Creo que la naturaleza humana es técnica, ¿verdad?

Sin tener un lenguaje compartido, no podemos entendernos aquí. Por eso creemos que necesitamos empezar a encontrar nuevas formas, caminos y técnicas para salvaguardar nuestros derechos primarios. Creo que el empoderamiento de los niños y jóvenes es vital. Realmente pienso que esta metáfora que se creó en 2001 de Nativos Digitales, creo que surgió como un gran problema para nosotros los adultos al cuidar de los niños porque pensamos que ellos saben todo sobre el mundo digital y que no podemos ayudarlos.

Realmente creo que la encriptación es una forma segura de empoderarse en un territorio donde tenemos muchas empresas tratando de hacer negocios con nuestro tiempo y atención. Y realmente creo que este tipo de técnicas pueden salvar nuestros derechos y crear entornos poderosos para que vivamos y disfrutemos sin ser explotados. Eso es, en pocas palabras.

Sharayah Lane - Internet Society: Sí, no, eso es genial. Gracias. ¿Sabine?

Dr Sabine K Witting - Leiden University: Sí, creo que si seguimos polarizando la discusión como está en este momento, estamos creando una distracción perfecta para los dos actores que realmente deberían invertir en prevención y respuesta, que son los gobiernos, invirtiendo realmente en el sistema de protección infantil, pero también las empresas tecnológicas, creando productos seguros y que respeten los derechos.

Así que creo que mi llamado sería realmente dar un paso atrás y preguntar Cui Bono, y eso ciertamente incluye a los gobiernos y las empresas tecnológicas. Gracias.

Sharayah Lane - Internet Society: Eso es muy importante. Gracias. Y por último, Larry.

Larry Magid - ConnectSafely.org: Creo que todas las personas, independientemente de su edad, tienen derecho a la privacidad y la seguridad, y a tener comunicaciones que sean solo entre ellas y otros.

Y creo que, después de escuchar a los oradores y reflexionar sobre nuestro papel, necesitamos cambiar el enfoque. En esta noción de protección infantil, no debemos permitir que la gente piense que la protección infantil se logra simplemente empoderando a las fuerzas del orden y dándoles todas las herramientas y herramientas de vigilancia que necesitan, sino también protegiendo a las personas de los criminales, de los miembros de la familia, si es necesario, y de conocidos, de gobiernos que puedan oprimirlos.

O simplemente porque quieren tener comunicaciones privadas. Y finalmente, creo que necesitamos redoblar nuestros esfuerzos en educación. Realmente me hace pensar, al reflexionar sobre el Día de Internet Segura y el trabajo que ConnectSafely está haciendo con los adolescentes, que todos necesitamos proporcionar a los adolescentes, y a los niños en general, todas las herramientas que podamos para ayudarles a proteger su privacidad y su seguridad.

Y eso además de todas las cosas que seguimos haciendo en torno al phishing y las contraseñas, también les enseñamos a usar una encriptación robusta como una forma de protegerse.

Sharayah Lane - Internet Society: Sí, nuevamente, muchas gracias a todos. Tuvimos una gran cantidad de experiencia y conocimiento en la llamada de hoy, así que realmente aprecio que se hayan tomado el tiempo para compartir con todos nosotros hoy.

Tenemos algunos recursos excelentes en el chat, así que no duden en seguir cualquiera de los enlaces que se compartieron hoy. Esperamos que puedan unirse a nuestra próxima sesión, que comenzará en unos 10 minutos, titulada "Encriptación Arrestada: el arresto de Pavel Durov de Telegram por no registrar servicios encriptados".

Entonces, nuevamente, eso parece ser un pequeño seguimiento de nuestra conversación legal sobre cifrado y leyes de hoy. Así que si desean tomar un descanso, tendrán unos 10 minutos antes de nuestra próxima sesión para el Día Global del Cifrado, pero gracias a nuestros ponentes y gracias a todos nuestros asistentes por acompañarnos hoy.

Muy bien. Gracias. Adiós.