Le chiffrement, le gardien

Sharayah Lane - Internet Society: Merci à tous de nous rejoindre pour le panel d'aujourd'hui, The Guardian. Aujourd'hui, nous allons parler du chiffrement et de ses impacts sur la sécurité des enfants en ligne. Je m'appelle Sharayah Lane. Je suis conseillère principale à l'Internet Society et également membre de notre équipe de chiffrement.

Une grande partie de mon travail avec l'équipe de chiffrement s'est concentrée sur la sécurité des enfants en ligne, et c'est un domaine relativement nouveau que beaucoup d'entre nous examinent. Ce sera une bonne discussion aujourd'hui. Nous avons des intervenants formidables. En ce qui concerne le sujet du chiffrement et de la sécurité des enfants en ligne, la discussion s'est principalement concentrée sur les auteurs d'abus et d'exploitation des enfants en ligne.

Ce dont on entend moins parler, cependant, c'est du rôle que joue le chiffrement dans la protection des enfants en ligne. Aujourd'hui, nous allons aborder ce sujet avec notre panel d'experts. Nos panélistes travaillent dans des domaines qui se concentrent sur l'utilisation sécurisée d'Internet par les enfants. Ce sont des universitaires menant des recherches dans ce domaine, et l'objectif de la session d'aujourd'hui est que nos participants comprennent mieux comment le chiffrement contribue à la sécurité des enfants en ligne, afin de vous aider, vous, nos participants, à devenir de meilleurs défenseurs du chiffrement avec plus d'informations à ajouter à vos propres domaines de travail.

Et en plus de la conversation d'aujourd'hui, trois de nos panélistes ont également contribué à un document de groupe de travail collaboratif qui explore ce sujet plus en profondeur. Si vous êtes intéressé par la lecture de ce document, vous pouvez le trouver ici, et je vais juste le poster dans le chat pour que vous puissiez le trouver ici si vous souhaitez en savoir plus.

Mais d'abord, je vais présenter nos panélistes. Tout d'abord, nous avons Jessica Dickinson Goodman. Jessica fait le lien entre les mondes de la technologie et de la politique. Elle a été présidente du conseil d'administration de l'Internet Society de la région de la baie de San Francisco et soutient le travail exceptionnel de son équipe sur les politiques technologiques, l'éducation et l'aide aux communautés défavorisées pour un meilleur accès à Internet. Elle est également l'auteure du livre de 2023, Encryption for Babies.

Ensuite, nous avons Larry Magid. Larry est docteur en éducation et également PDG de ConnectSafely.org. C'est un journaliste technologique chevronné. Il écrit une chronique hebdomadaire pour le San Jose Mercury News et anime le ConnectSafely Report deux fois par semaine pour CBS News Radio aux États-Unis. Il est fréquemment invité dans des émissions de télévision et de radio nationales et locales, aux États-Unis et au

Royaume-Uni. Il a été analyste technologique à l'antenne pour CBS News pendant 20 ans et anime l'émission populaire de CBS, Eye on Tech.

Ensuite, nous avons Dr. Sabine Witting. Dr. Witting est professeure adjointe en droit et technologies numériques à l'Université de Leiden. Ses recherches se concentrent sur l'intersection des droits de l'homme, y compris les droits des enfants, avec la technologie numérique. Elle est également cofondatrice de TechLegality, une société de conseil spécialisée dans les droits de l'homme et les technologies numériques. Sabine est chercheuse non résidente au Center for Democracy and Technology.

Ensuite, nous avons le Dr Ezequiel Passeron. Le Dr Passeron est titulaire d'un doctorat en Éducation et Société de l'Université de Barcelone et d'un diplôme en Sciences de la Communication de l'Université de Buenos Aires. Il possède également un Master en Environnements d'Enseignement et d'Apprentissage Médiatisés par les Technologies Numériques. Il est de l'Université de Barcelone. Il est le directeur de l'éducommunication chez Faro Digital, une ONG qui étudie et développe des projets en éducation aux médias. Il est également professeur associé à l'Université de Barcelone, coordinateur du réseau Conectados al CERN et chercheur au sein du groupe de recherche ESBRINA. Ses intérêts portent sur l'étude et l'analyse des intersections entre l'éducation, la communication, les plateformes numériques et les environnements d'intelligence artificielle.

Enfin, nous avons le Dr. Mark Leiser. Le Dr. Leiser est un théoricien de la régulation spécialisé dans la régulation numérique, juridique et des plateformes. Son domaine d'expertise inclut le droit et les technologies numériques, tels que les droits fondamentaux, le commerce électronique, la théorie de la régulation, la régulation des plateformes, les contrats, la sécurité, la vie privée, la liberté d'expression, la cybercriminalité et les phénomènes liés aux conceptions trompeuses, les schémas trompeurs, la protection des consommateurs, et l'utilisation et la régulation de l'IA et des technologies numériques. Cela représente beaucoup d'expertise pour l'appel d'aujourd'hui.

Merci à tous d'être avec nous et de partager votre temps et votre expertise sur ce sujet. Nous vous en sommes vraiment reconnaissants. Sur ce, nous allons passer à notre session de questions-réponses.

Nous allons poser des questions spécifiques à nos panélistes. Nous encourageons tous nos participants à soumettre également leurs questions en utilisant la fonctionnalité de questions-réponses. Nous aurons du temps vers la fin de notre appel aujourd'hui pour aborder vos questions et les soumettre aux panélistes.

Mais sur ce, nous allons commencer notre conversation et nous allons débuter avec Larry Magid. Alors Larry, vous avez beaucoup travaillé dans le domaine de l'engagement en ligne des enfants. Pouvez-vous nous donner un aperçu de ce que vous avez appris sur le rôle du chiffrement dans l'utilisation d'Internet par les jeunes ?

Larry Magid - ConnectSafely.org: Merci. Tout d'abord, je tiens à reconnaître qu'il y a certainement un grand nombre de personnes bien intentionnées qui ont soutenu que le chiffrement est nécessaire pour que les forces de l'ordre puissent prévenir l'exploitation des enfants, et ils pensent spécifiquement au CSAM, matériel d'abus sexuel sur enfants.

Il y a une controverse au sein de la communauté de protection de l'enfance, et je pense franchement que la plupart de mes amis et collègues dans cette communauté ne seraient pas d'accord avec moi. Ils soutiendraient que la nécessité de prévenir le CSAM, ce avec quoi je suis bien sûr d'accord, mais que le besoin des forces de l'ordre, que le chiffrement les gêne et cause donc du tort.

Et cela rend probablement le travail des forces de l'ordre plus difficile. Toutes les questions ont certains types de nuances et de compromis, et en aucun cas je ne veux, d'une manière ou d'une autre, diminuer l'importance du blocage et de la prévention de la pornographie infantile, du matériel d'abus sexuel sur enfants, ainsi que la poursuite de ceux qui trafiquent de manière à nuire et abuser des enfants.

Cela dit, il est également important de souligner que les enfants eux-mêmes ont besoin de protection contre les violations potentielles de la vie privée et de la sécurité qui peuvent survenir dans un monde sans cryptage. Il existe de nombreux exemples allant des violations de données où les informations des enfants sont tombées entre les mains de criminels ou de criminels potentiels, ou encore où leurs informations ont été simplement révélées de manière à violer leur vie privée.

On pourrait même avancer l'argument que le chiffrement protège les enfants contre les prédateurs d'enfants, car le fait de pouvoir accéder aux informations des enfants facilite la tâche de ceux qui veulent les abuser, les trouver, les atteindre et les exploiter. C'est donc une arme à double tranchant.

Mais en y réfléchissant beaucoup, je pense que, clairement, la capacité de protéger la vie privée et la sécurité des enfants est un droit fondamental qui doit être maintenu. Et les forces de l'ordre doivent trouver d'autres moyens dans un monde chiffré pour pouvoir exercer leur responsabilité de lutte contre le matériel d'abus sexuel sur enfants.

Mais il y a de nombreux exemples où, encore une fois, j'ai mentionné les violations de données, donc je me souviens que le Service national de santé au Royaume-Uni a subi une violation majeure il y a quelques années avec des informations sur les enfants. Il y a de nombreux cas de données scolaires qui ont été violées et de nombreux cas où les enfants eux-mêmes communiquent directement avec d'autres d'une manière qui aurait pu être violée ou peut-être a été violée en raison de l'absence d'une plateforme cryptée.

Je pense donc que nous méritons tous d'être protégés. Que ce soit les banques et les transactions financières, que ce soit les activistes dans divers pays, et d'ailleurs, les enfants peuvent être parmi les activistes. Quand nous pensons aux personnes

impliquées dans des activités que les gouvernements veulent réprimer, dans de nombreux cas, ce sont des mineurs qui sont engagés, des adolescents, certainement, qui sont engagés dans des activités à travers le monde, où la capacité d'avoir des communications privées et confidentielles est essentielle non seulement pour leur mission de réforme, mais aussi pour la protection de leur propre vie, car il y a souvent un grand danger associé au fait de faire partie d'un mouvement, quel que soit votre âge.

Et donc, il y a tellement d'exemples que nous devons souligner. Et je suppose que ce que j'essaie de faire au sein de la communauté dans laquelle j'opère, c'est d'amener les gens à penser au-delà du simple désir des forces de l'ordre de protéger, mais à la question plus large de protéger toute notre sécurité et notre vie privée. Et enfin, et ce n'était pas une pensée originale de ma part, mais l'un de mes collègues qui a aidé à travailler sur ce document que vous avez mentionné plus tôt a fait remarquer que le chiffrement peut souvent être utilisé pour aider à détecter et à poursuivre les crimes, mais en, je suis désolé, l'absence de chiffrement pourrait rendre plus facile la poursuite des crimes, mais le chiffrement aide à prévenir les crimes.

Et étant donné le choix entre la poursuite et la prévention, je choisirais la prévention à chaque fois. Ce serait formidable de mettre les procureurs au chômage parce que nous avons éliminé le crime. Nous n'y arriverons probablement jamais. Mais si nous pouvons réduire la criminalité en protégeant la sécurité des gens, cela signifie moins de cas à poursuivre pour les procureurs.

Sharayah Lane - Internet Society: C'est super. Merci, Larry. Et je voulais passer à Jessica. Je sais que Jessica va devoir quitter l'appel plus tôt, alors merci d'être avec nous. Et ma question pour vous est, qu'est-ce qui vous a poussé à écrire le livre "Le chiffrement pour les bébés" ? Qu'espériez-vous que les lecteurs retiennent après avoir terminé ce livre ?

Jessica Dickinson Goodman - SF Bay ISOC: Je m'intéresse au chiffrement depuis que j'ai fait un stage à la Electronic Frontier Foundation quand j'étais au lycée, parce que je suis ce genre de personne et ce genre de nerd. Mais à l'époque, je restais à la maison avec mon enfant, qui aura deux ans dans trois semaines. Et je lui lisais beaucoup de livres sur des sujets comme l'astrophysique pour les bébés.

Il existe une série de livres cartonnés que beaucoup de petits enfants ont aux États-Unis, avec des statistiques pour bébés et de l'astrophysique pour bébés. Et je voulais lui expliquer le chiffrement. Je pensais que ce serait un défi intéressant et c'est un garçon intelligent. Et c'est toujours complexe, n'est-ce pas ? Comment expliquer quelque chose de non physique, de technique ?

Mais je me suis dit que si nous pouvions lire l'astrophysique pour les bébés, nous pourrions trouver un moyen de parler de l'encryption. Alors, quand je l'ai écrit et testé sur lui, puis que mes amis l'ont testé sur leurs enfants, et ensuite que j'ai organisé un

événement éphémère au centre-ville de Mountain View, j'ai passé sept heures à demander à chaque personne technique qui passait de remettre en question les métaphores que j'avais utilisées, et ils n'ont trouvé aucune erreur technique, ce qui était formidable.

Et ensuite, en le mettant en ligne à vendre pour bénéficier à mon chapitre de San Francisco, mon objectif principal était d'aider à la fois les enfants et les parents qui leur lisent à se sentir plus à l'aise avec le chiffrement. Parfois, quand vous dites que vous vous souciez du chiffrement, comme moi actuellement à Georgetown en train de faire des études supérieures à l'École de service extérieur, et j'ai souhaité à tout le monde une joyeuse Journée mondiale du chiffrement pour ceux qui la célèbrent.

Et tout le monde ne se sentira pas immédiatement à l'aise avec cette idée. Il y a maintenant une stigmatisation attachée au désir de préserver la vie privée de vos enfants dans certains espaces, comme M. Vedgett en parlait, en particulier dans la région où nous avons tous deux travaillé, la Silicon Valley, où il y a cette forte narration des forces de l'ordre visant à faciliter leur travail en matière de poursuites.

Et je travaillais pour le Département de la Justice de Californie. Ce travail me tient également à cœur. Mais c'est un outil essentiel pour que les parents puissent garder leur famille en sécurité, et le comprendre suffisamment bien pour l'expliquer à un petit enfant est précieux, plutôt que de faire face à la vague de tactiques de peur en essayant de donner aux parents un peu de marge pour échapper à toute cette pression d'être anti-chiffrement.

Parce que je pense que c'est une bonne chose de vouloir protéger l'emplacement, la vie privée et les photos de votre enfant. Et je peux entrer dans les détails techniques avec d'autres adultes, mais mon petit n'a pas besoin de connaître tous ces éléments. Je dirai que je n'étais pas sûr d'inclure la phrase E2EE, et c'est la partie préférée de mon petit dans le livre.

Il dit, E2EE ! Il trouve ça très amusant à dire et il me demande de le répéter encore et encore. Donc parfois, on peut être un peu technique même avec nos plus jeunes auditeurs et ils pourront nous suivre, au moins si c'est amusant à dire à voix haute.

Sharayah Lane - Internet Society: J'adore ça. J'adore cette histoire. Et j'ai hâte de découvrir le livre.

J'ai un petit qui a à peu près le même âge, donc ça va être amusant. Avant que vous ne vous déconnectiez, Jessica, je voulais vous poser une dernière question tant que nous vous avons encore. Vous avez travaillé intensivement sur le rôle du chiffrement dans la protection des droits reproductifs des femmes aux États-Unis. Pouvez-vous nous en dire plus sur ce travail et comment cela se connecte à la sécurité des enfants grâce au chiffrement ?

Jessica Dickinson Goodman - SF Bay ISOC: Absolument. Après la fuite de la décision Dobbs, je suis allé voir mon conseil d'administration pour ceux qui ne sont pas familiers, la plupart des chapitres sont entièrement basés sur le bénévolat, donc nous avons commencé à en parler, nous savions que c'était un sujet sensible mais nous voulions donner aux gens les moyens de protéger leurs données. Pendant toute l'année où la décision Dobbs a été divulguée, et lorsqu'elle est sortie, notre chapitre a organisé des formations mensuelles que j'appelle des formations de soutien technique tactique, ouvertes à tous dans le monde.

Je pense que nous avions une demi-douzaine de pays représentés. Beaucoup de gens venaient d'États comme le Texas où le gouvernement cherche activement à recueillir des informations privées. Et nous nous sommes concentrés sur deux études de cas. L'une concernait une jeune femme qui cherchait à obtenir des soins d'avortement. Elle venait du Texas et devait partir et recueillir ces informations sans, comme cela a été le cas, être poursuivie par un partenaire ou arrêtée par les forces de l'ordre, ou que ses amis ou sa famille soient poursuivis, arrêtés ou condamnés à une amende, ce qui est actuellement la loi en vigueur au Texas et qui est contestée, une situation à laquelle de nombreuses personnes cherchant des soins d'avortement sont confrontées.

L'autre étude de cas concernait une jeune personne en Alabama. Elle cherchait des soins de confirmation de genre en dehors de l'État et avait une préoccupation à domicile. Ce sont donc les deux études de cas. Les soins de santé reproductive où vous craignez que l'État espionne vos informations et les utilise contre vous. Et l'autre était l'inquiétude que des membres de la famille espionnent et soient potentiellement violents à cause de ces informations.

Nous avons donc examiné les problèmes logistiques, les outils techniques. Une grande partie de cela a été inspirée par le fait d'être une personne queer, une mère et une femme. Et j'ai besoin de ces outils. Pour que je puisse être libre dans le monde de la même manière que les personnes sans utérus sont libres dans le monde, et de la même manière que les personnes hétérosexuelles sont libres dans le monde, et j'ai besoin de pouvoir avoir de la confidentialité parce que mon gouvernement, bien que j'aspire à y travailler un jour et y ai travaillé par le passé, ne représente pas tous les Américains, pas seulement ceux qui sont d'accord avec moi et qui veulent que je sois en sécurité et heureuse.

Et cette série de formations était importante pour moi, importante pour notre chapitre, et importante pour les personnes qui y ont participé, car elle guidait les gens sur la façon de configurer WhatsApp, d'utiliser Tor Browser, qu'est-ce que c'est ? Et la plupart des questions provenaient de cette peur dont parlait M. Magic, que les gens n'étaient pas sûrs que ces outils étaient pour eux.

Et si ces outils étaient sûrs pour eux à utiliser. Et donc, une fois que nous en avons parlé, la plupart des gens étaient à l'aise pour aller de l'avant et utiliser davantage d'outils de cryptage. Mais je pense qu'il est important de se rappeler que les personnes

au gouvernement sont juste des gens et que les membres de la famille sont juste des familles et qu'ils vont être bons, mauvais, laids et merveilleux, comme n'importe quelle autre personne, et qu'ils ne méritent pas un accès spécial à la localisation.

des images ou des communications, ils peuvent obtenir un mandat comme ils l'auraient fait il y a cent ans et obtenir ces informations. Ils n'ont pas besoin d'un accès spécial juste parce que c'est 2024. Donc, c'est ce que nous avons fait et les informations de formation sont toujours en ligne. La Fondation Electronic Frontier a un excellent cadre de défense numérique que nous avons utilisé.

Nous utilisons également le site web Plan C pour trouver des informations sur les soins liés à l'avortement, ce qui était important, et cela devient de plus en plus crucial à mesure que de plus en plus d'États adoptent des lois criminalisant l'accès aux soins de santé reproductive et aux soins affirmant le genre.

Sharayah Lane - Internet Society: Merci pour cela, et merci pour tout le formidable travail que vous faites.

Je vais passer à Sabine. Et merci d'être avec nous aujourd'hui. Vous avez occupé un poste à l'ONU travaillant en Namibie et au Zimbabwe sur des questions de réforme législative et politique concernant la cybercriminalité, la responsabilité du secteur privé et les technologies numériques. Quelles ont été certaines des principales conclusions de votre travail concernant la sécurité des enfants en ligne et, ou le rôle du chiffrement ?

Dr Sabine K Witting - Leiden University: Oui, merci beaucoup. Merci de m'avoir invitée. Donc oui, comme je le disais, j'ai travaillé spécifiquement avec l'UNICEF pendant de nombreuses années en Afrique australe, mais aussi dans la région Asie de l'Est et Pacifique. Et une chose qui émerge dans de nombreux pays du Sud global est la connectivité et l'accès aux technologies numériques.

Et bien sûr, cela signifie également pour les enfants un accès et une connectivité accrus. Et autant les technologies numériques peuvent être très utiles pour permettre aux enfants de réaliser leurs droits, il y a bien sûr aussi certains risques pour les droits des enfants. Et en particulier, je pense que celui qui attire le plus l'attention est le droit à la protection contre toutes les formes de violence, d'abus et d'exploitation.

Et je pense que lorsque nous travaillions sur ces sujets ici dans la région, l'une des choses que nous rappelions toujours aux législateurs et aux décideurs politiques était de dire : regardez, bien sûr, c'est un sujet émergent qui semble nouveau, mais les dynamiques sous-jacentes de ces formes de violence, d'abus et d'exploitation sont exactement les mêmes que celles que nous avons observées dans l'environnement physique.

Donc, lorsque vous réfléchissez à la manière de prévenir et de répondre à ce type d'infractions, vous devez vraiment penser plus largement et ne pas vous limiter à l'espace numérique, mais vraiment considérer l'ensemble du système de protection de l'enfance et comment vous pouvez renforcer ces systèmes de protection pour pouvoir également répondre à ces cas facilités par la technologie.

Ainsi, reconnaître ce lien entre la violence physique et celle facilitée par la technologie était vraiment très important pour élaborer une approche holistique et ne pas se limiter à des solutions techniques, ce que l'on observe encore beaucoup aujourd'hui, non seulement dans le Sud global, mais aussi dans le Nord global.

Donc, je pense que dans le même ordre d'idées, lorsque nous discutons de ce type d'interventions politiques et que nous examinons spécifiquement le côté de l'application de la loi. Il y a certainement aussi un manque de reconnaissance pour la communication privée et le chiffrement. Et je pense que c'est aussi parce que nous ne valorisons pas de la même manière la confidentialité et la sécurité des communications pour les enfants.

Cela ne semble tout simplement pas être une priorité pour les gens. Bien sûr, la protection contre la violence est primordiale, mais en même temps, nous devons vraiment penser à l'ensemble des droits des enfants. Et je pense que l'une des choses qui m'a vraiment marqué, c'est lorsque nous travaillions avec des enfants au Zimbabwe sur l'élaboration de la Politique de protection des enfants en ligne du Zimbabwe.

Nous avons demandé aux enfants, quelle est votre expérience en ligne ? Quelles sont les choses auxquelles vous êtes confrontés ? Et bien sûr, beaucoup d'enfants ont dit qu'ils avaient vécu diverses formes de violence, y compris la violence sexuelle. Mais il y avait aussi des enfants qui nous ont dit qu'ils utilisaient un VPN pour protéger leur Et quand nous avons rapporté ces conclusions aux législateurs à Harare, on pouvait voir que beaucoup de personnes dans la salle, les législateurs, ne savaient pas ce qu'était un VPN.

Et je pense que c'est un aspect très intéressant du débat : les expériences des enfants et leur focalisation sur ce qui est important pour eux en relation avec les technologies numériques diffèrent souvent de ce que les adultes considèrent comme vraiment important. Nous avons également constaté cela dans la région de l'Asie du Sud, où nous demandions aux enfants ce qu'ils attendent des entreprises technologiques pour rendre les produits et services numériques plus adaptés aux enfants.

Et encore une fois, en haut de la liste de souhaits, il y avait une meilleure protection des données et de la vie privée. Et donc, je pense que c'est pour nous et vraiment pour les législateurs et les décideurs politiques un bon appel à l'action en termes de consultation des enfants, non seulement sur l'énoncé du problème. Donc, dans quelle mesure ressentez-vous A, B, C, D, mais aussi que pensez-vous des solutions que nous proposons ?

Et je pense que c'est là que les voix des enfants manquent cruellement et en fait, pas seulement les voix des enfants, mais aussi celles de tous les groupes vulnérables affectés par, disons, le chiffrement, comme l'a dit Jessica. Les femmes, les personnes queer, mais aussi les défenseurs des droits de l'homme, leurs droits disparaîtraient considérablement.

Et je pense que c'est quelque chose où nous ne prenons tout simplement pas en compte les points de vue des personnes concernées, y compris les enfants. Merci.

Sharayah Lane - Internet Society: Merci. Et oui, nous continuerons cette conversation un peu plus tard. Avec Larry, car je sais que Connect Safely a un Conseil consultatif des jeunes dont j'aimerais en savoir plus.

Mais d'abord, je veux m'adresser à tous nos panélistes, puis nous reviendrons et passerons d'une question à l'autre pour nos différents panélistes. La prochaine question est pour Ezequiel. Et cela fait en fait suite à la question de Sabine. Votre organisation travaille beaucoup avec les jeunes et leurs familles.

Que font généralement les parents sans se rendre compte que cela peut exposer leurs enfants ? Que pourraient-ils faire de mieux ? Et quel est le rôle du chiffrement dans tout cela ?

Ezequiel Passeron - University of Barcelona: Super. Merci, tout d'abord, pour l'opportunité de partager avec ces personnes formidables.

Je pense que nous devons célébrer ces espaces pour avoir du temps et pour le dialogue.

Je pense que le premier problème que nous voyons dans les familles est le manque de dialogue intergénérationnel. En Argentine et en Amérique du Sud, les enfants et les jeunes sont souvent seuls dans le monde numérique. Leurs adultes ne sont pas au courant de leurs pratiques et de leur culture numérique. Donc, lorsqu'un problème survient, ce ne sont pas vers eux que les jeunes se tournent pour dialoguer.

À Faro, les principaux problèmes que nous observons lorsque nous parlons et écoutons les étudiants, les enfants et les jeunes sont la violence numérique, la désinformation et la mésinformation, une personnalisation croissante de l'expérience, les bulles de filtres, le manque de contexte avec la différence, tous les problèmes que ces choses causent à la coexistence sociale et à la démocratie, ainsi que l'hypersexualisation et la monétisation des imaginaires et subjectivités des jeunes. C'est pourquoi, dans notre ONG, nous encourageons à partager des moments de connexion qui favorisent le dialogue, les conversations, en essayant de ne pas juger les sujets qui intéressent les jeunes afin de comprendre les soins dont ils ont besoin. Je pense que le soin est un concept important que nous devons mettre en avant. Au-delà de cela, des

pratiques adultes comme, je ne sais pas, la parentalité, par exemple, émergent. Cela inclut le partage d'images personnelles des enfants et des jeunes, et ils voient que c'est un problème majeur et ils n'aiment pas ça.

De nombreux enfants commencent à avoir une identité numérique sans même y avoir consenti. En ce qui concerne le rôle du chiffrement, nous pensons que c'est un grand allié pour les familles car c'est quelque chose de généralement méconnu dans notre pays. Nous avons étudié le guide de chiffrement de l'ISOC que vous venez de partager et nous voyons une grande opportunité de le diffuser dans les écoles.

Nous pensons que ce genre d'outils ajoutés aux ateliers éducatifs et, encore une fois, en ayant du temps et de l'espace pour dialoguer et réfléchir, pourraient constituer une approche intégrale pour atteindre ces alliés clés dans la protection et le soin des jeunes. La famille parle souvent de contrôles parentaux, de mots de passe ou de temps d'écran sécurisé.

Comme Sabine l'a dit précédemment, nous voulons un bouton pour résoudre tous nos problèmes. Et nous pensons que le chiffrement pourrait être une très bonne technique pour surmonter les préoccupations que nous devons avoir. Pour les enfants et les jeunes.

Sharayah Lane - Internet Society: Oui, merci. C'est tellement intéressant ce changement de dynamique qui s'est produit, même avec des choses comme la réglementation.

Il a toujours été de la responsabilité des adultes de protéger les enfants dans divers domaines. Mais en ce qui concerne les espaces en ligne et technologiques, les jeunes sont souvent plus informés, plus compétents et plus expérimentés que certains adultes. Cela change vraiment la conversation et la dynamique sur la manière de mener ce travail.

Oui, c'est vraiment important. Je vais passer à Mark pour notre prochaine question. Un autre rappel, si vous avez des questions, chers participants dans l'audience, veuillez les poser dans la fonctionnalité de questions-réponses. Nous en avons déjà reçu quelques-unes et nous y répondrons dans quelques minutes, alors continuez à envoyer vos questions à nos panélistes et nous aurons le temps d'y répondre.

Le monde académique joue un rôle important dans la recherche et l'étude de la manière dont les enfants interagissent en ligne. Quels ont été certains des principaux résultats de vos recherches au fil des ans concernant le chiffrement ?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Je vais peut-être tricher un peu et commencer par une excellente question qui a été posée lors de la séance de

questions-réponses, à laquelle je vais en partie répondre dans ma propre réponse à cette question, donc je voulais juste le souligner.

Je dirais donc qu'au fil des années, il y a eu d'innombrables incidents où le chiffrement a assuré la sécurité des enfants dans leurs interactions numériques, mais il y a aussi eu un manque de compréhension de son importance, ce qui les rend vulnérables. Dans les recherches que j'ai menées, et évidemment celles du Dr. Witting également, nous avons constaté que les plateformes non chiffrées exposent les enfants à des risques. Du suivi de localisation, des métadonnées, au cyberharcèlement dans les applications de messagerie non protégées. En revanche, l'utilisation de systèmes chiffrés réduit considérablement ces menaces. Par exemple, un cas impliquant un enfant partageant involontairement sa localisation via un post sur les réseaux sociaux, ce qui a conduit des inconnus à se présenter à son domicile.

Et donc cet incident, et d'autres similaires, mettent en évidence comment le chiffrement peut servir de bouclier, protégeant les données sensibles que nous ne voudrions pas voir tomber entre de mauvaises mains. Mais, les enfants et les parents manquent encore d'éducation pour en reconnaître la valeur, ce qui les rend vulnérables aux menaces numériques. Et le micro-narratif consiste à essayer d'examiner ces incidents spécifiques où le chiffrement aurait pu protéger un enfant dans un certain contexte.

Mais à une échelle plus large, l'intégration du chiffrement dans les plateformes, les écoles et les environnements de jeu a eu un impact positif considérable sur la sécurité des enfants. Le chiffrement empêche l'accès non autorisé aux données personnelles. Il freine le vol d'identité. Il réduit le cyberharcèlement et le harcèlement en ligne, et pendant la pandémie, le passage à l'apprentissage en ligne souligne encore plus l'importance du chiffrement.

Lorsque les écoles sont passées à des systèmes de visioconférence cryptés, cela a atténué les risques, comme le Zoom bombing et les intrusions numériques dans les salles de classe virtuelles. Il reste un fossé dans la sensibilisation au rôle du cryptage dans la protection des enfants en ligne. Comme cela a été dit auparavant, la recherche et les politiques doivent converger pour aborder ces vulnérabilités en promouvant le cryptage et en étendant son application sur les plateformes fréquentées par les enfants.

Et enfin, cette sorte de méga-narratif est que le chiffrement est lié aux principes fondamentaux de la vie privée et de la sécurité. Il a des implications profondes pour les droits et libertés numériques. Alors que le RGPD de l'UE encourage fortement le chiffrement comme méthode de protection des données personnelles, le paysage mondial montre des différences marquées dans la manière dont le chiffrement est réellement traité.

Dans les régimes autoritaires, les restrictions sur le chiffrement permettent la surveillance de masse, ce qui porte atteinte à la vie privée et aux droits de l'homme. Et la relation entre la vie privée et la sécurité devient alors indéniable. Ce ne sont pas deux choses distinctes, mais deux faces d'une même médaille. Le chiffrement protège les gens. Il sert de pilier essentiel pour protéger les individus, en particulier les enfants et autres membres vulnérables de la société, contre l'exploitation et les préjudices que les parents cherchent désespérément à éviter pour leurs enfants.

À mesure que les sociétés deviennent de plus en plus dépendantes de ce type d'infrastructures numériques, des lois comme le RGPD, qui promeuvent la protection des données et la confidentialité dès la conception, sont en réalité essentielles pour garantir la sécurité et la dignité des populations vulnérables à travers le monde. Merci.

Sharayah Lane - Internet Society: Wow, c'était un excellent aperçu.

Merci, Mark. Et merci d'avoir répondu à l'une de nos questions. Nous en avons d'autres qui arrivent. Encore une fois, un rappel pour nos participants : n'hésitez pas à taper vos questions aux panélistes dans la fonctionnalité de questions-réponses et nous aurons le temps d'y répondre un peu plus tard lors de notre appel. Notre prochaine question est pour Larry, et cela pourrait éclairer certains des sujets dont nous avons parlé, notamment l'inclusion des jeunes dans la conversation et dans la recherche de solutions.

Donc, ConnectSafely a un Conseil consultatif des jeunes adultes. Comment le fait de travailler directement avec des jeunes a-t-il influencé votre travail, et quelles sont certaines des principales choses que vous entendez de leur part en ce moment ?

Larry Magid - ConnectSafely.org: Avoir un conseil consultatif de jeunes nous ancre vraiment de nombreuses façons, et cela nous apprend certaines des choses auxquelles les jeunes aspirent, ainsi que certaines des préoccupations qu'ils ont. Je dois vous dire que, dans certains domaines, les jeunes sont un peu plus conservateurs que moi sur certaines questions.

Il m'arrive d'être surpris par leur inquiétude face aux nombreux dangers sur Internet et par leur désir de voir plus de contrôles mis en place. Nous n'avons pas encore eu de conversations approfondies sur le chiffrement. Nous prévoyons de le faire à l'avenir dans le cadre de notre programme, mais j'imagine que nous aurons des divergences d'opinion.

Cela semble être l'une des choses que l'on apprend en parlant à des personnes de n'importe quel groupe démographique : on ne peut pas enfermer un groupe démographique dans une case, que ce soit par genre, race, orientation sexuelle, âge ou autre. Les gens sont des individus avec des opinions différentes. Mais dans l'ensemble, je pense que certains des jeunes avec qui j'ai parlé ont un désir très fort de voir un Internet sécurisé et privé et comprennent vraiment le besoin de cryptage de manière

similaire à ce que Mark et d'autres ont mentionné, comme un moyen de les protéger des abus potentiels en ligne.

Il y a d'autres personnes qui pourraient être préoccupées par les limitations ou les défis que cela pose aux forces de l'ordre, et c'est quelque chose qui ferait partie d'un programme éducatif pour essayer de faire comprendre aux gens pourquoi le chiffrement est si important et comment les forces de l'ordre peuvent toujours faire leur travail malgré les outils, tout comme elles font leur travail malgré les diverses protections légales en place aux États-Unis et dans d'autres pays non autoritaires, dans la mesure où les États-Unis restent, espérons-le, un pays non autoritaire.

Mais oui, il est tellement important pour ceux d'entre nous dans le monde des politiques de parler aux jeunes. Et encore une fois, ne pas faire de suppositions sur ce qu'ils pourraient dire, mais leur donner une place à la table. En fait, cette année, Connect Safely est l'hôte américain de la Journée pour un Internet plus sûr.

Et cette année, nous allons avoir une conversation politique à Sacramento, le gouvernement de l'État où se trouve la capitale de la Californie, pour essayer de donner aux jeunes un rôle à la table afin que, lorsque les législateurs adoptent des lois, que ce soit sur le chiffrement, le contrôle parental, la vérification de l'âge, les réseaux sociaux, ou les soi-disant mesures anti-addiction, ou quoi que ce soit d'autre, les jeunes fassent partie de cette conversation.

Nous voulons voir un nombre accru. Nous aimerions voir plus d'éducation pour les jeunes sur le chiffrement. L'une des raisons pour lesquelles Connect Safely a rédigé plusieurs articles et a eu l'honneur d'héberger le document que ce groupe a élaboré, est que nous voulons nous assurer que de plus en plus de jeunes comprennent le chiffrement.

Mon impression est que pour la plupart des gens, c'est un sujet qu'ils n'ont tout simplement pas vraiment abordé. Il y a donc un réel besoin d'avoir beaucoup de discussions éducatives avec des personnes de tous âges, mais surtout avec les adolescents.

Sharayah Lane - Internet Society: Oui, merci. Et j'ai partagé un lien vers la Journée pour un Internet plus sûr dans le chat si les gens sont intéressés à en savoir plus.

Larry Magid - ConnectSafely.org: Au fait, cette année, comme les années précédentes, nous offrons des subventions aux éducateurs et aux organisations à but non lucratif. Donc, si quelqu'un souhaite organiser un programme sur le chiffrement dans sa communauté ou dans ses écoles, nous avons des subventions allant jusqu'à 1 000 euros pour les enseignants et les organisations à but non lucratif afin de les aider à faire de l'éducation communautaire autour de la Journée pour un Internet plus sûr en février prochain.

Alors, veuillez revenir dans quelques semaines lorsque les candidatures seront lancées.

Sharayah Lane - Internet Society: Oui, merci pour cette ressource. C'est vraiment une excellente façon de faire le suivi de l'appel d'aujourd'hui. Donc, je voulais, avec cela, passer à Ezequiel pour continuer cette conversation parce que Ezequiel, tu travailles également en étroite collaboration avec les enfants, les jeunes et leurs familles.

Et j'espère pouvoir vous poser la grande question et aborder l'éléphant dans la pièce : les matériaux d'abus sexuels sur enfants, les matériaux CSAM. J'ai également vu un commentaire à ce sujet dans le chat. Alors, comment nous en protégeons-nous ? Et que contient cette boîte à outils ? Et quels sont certains des travaux que vous avez réalisés à ce sujet chez FonoDigital ?

Ezequiel Passeron - University of Barcelona (2): Comme je vous l'ai dit auparavant, l'hypersexualisation de la société, mais aussi des enfants, est un sujet majeur auquel nous devons faire face, et la manière dont nous interagissons avec les plateformes numériques joue un rôle dans ce contexte. Nous ne croyons pas à la détermination des médias de masse sur nos pratiques, mais ils ont une forte influence, cela ne fait aucun doute.

En Argentine, nous avons un travail important réalisé par des procureurs spécialisés en cybercriminalité. Nous savons qu'il existe une coopération internationale étendue, notamment avec le réseau NMAC, qui facilite l'échange d'informations sur les cas et l'avancement des enquêtes à chaque étape. Le fait est que ce genre de cas, nous l'appelons en espagnol, masi nous avons tout le temps cette idée fausse de pornographie enfantine ou de pornographie infantile.

C'est du matériel d'exploitation sexuelle des enfants et nous devons. Nous devons le dire haut et fort pour comprendre l'ampleur du problème. C'est un phénomène de plus en plus émergent. Nous avons de nombreux cas d'enfants et d'écoles qui ne savent pas comment, quoi faire. Donc, il y a un rôle clé à jouer pour impliquer les procureurs.

Et les postes de police qui travaillent sur ce genre de cas. Nous voyons également dans nos ateliers que des technologies comme l'IA sont utilisées pour générer des images d'enfants qui violent leurs droits et leur vie privée. La semaine dernière, nous avons eu un cas récent qui a fait la une des journaux et des médias.

Et comment. Pouvons-nous nous protéger de cela ? Et avec quels outils ? Je pense que ce sont les questions clés à se poser. Encore une fois, nous mettons l'accent sur l'éducation, la citoyenneté numérique et la création d'espaces de dialogue. Je pense que ce genre de sujets sexuels sont parfois un peu tabous dans nos sociétés.

Mais quand les enfants sont sur Internet et entre les plateformes numériques, il n'y a pas de tabou. Nous apprenons en faisant. Et la plupart du temps, avant d'avoir un

espace pour poser des questions, nous découvrons notre sexualité avec nos parents ou un adulte de confiance. Nous croyons en l'éducation, nous croyons au dialogue et à la création d'espaces sûrs pour que les enfants puissent exprimer leurs curiosités et apprendre progressivement. Ce sont les principales choses que nous devons promouvoir et défendre.

Sharayah Lane - Internet Society: Oui, et il y a vraiment tellement de façons différentes de voir cela. Il n'y a pas de réponse claire et je pense que c'est vraiment au cœur de notre appel aujourd'hui, c'est de traiter la question. Lorsqu'il s'agit du chiffrement et de l'impact sur la sécurité des enfants en ligne, une grande partie de l'attention a été portée sur les auteurs d'abus et sur les adultes et la communauté.

Les implications du chiffrement pour les jeunes en ligne se perdent vraiment dans cette conversation. Donc, comment maintenir une protection pour les jeunes en ligne grâce au chiffrement tout en poursuivant et en abordant la question des contenus d'abus sexuels sur enfants est une question ouverte en ce moment, et c'est quelque chose sur lequel beaucoup de gens travaillent et réfléchissent.

Et c'est vraiment l'un des grands défis du moment, car comme nous l'avons entendu de nos intervenants précédents, le nombre de façons dont le chiffrement joue un rôle pour les jeunes est considérable. Donc, le supprimer a aussi un effet. Merci donc pour un peu plus de contexte à ce sujet. Je sais que c'est toujours une question difficile.

Et Sabine, je voulais revenir vers vous. Vous avez travaillé de manière approfondie en conseillant les décideurs politiques du monde entier sur la technologie. Quel est l'un des principaux conseils que vous donnez aux décideurs en matière de sécurité des enfants en ligne ?

Dr Sabine K Witting - Leiden University: Oui, merci beaucoup pour cette question. Bien sûr, nous abordons toujours les choses du point de vue des droits de l'homme et des droits de l'enfant.

Notre principal conseil est vraiment que nous ne pouvons pas isoler la sécurité des enfants et leur droit à la protection des autres droits des enfants. Et selon la Convention des Nations Unies relative aux droits de l'enfant, tous ces différents droits des enfants sont interdépendants, indivisibles et interconnectés.

Cela signifie que nous ne pouvons pas promouvoir un droit sans considérer l'impact négatif ou positif sur les autres droits de la convention. Et concrètement, cela se traduit par des conseils sur ce que les législateurs devraient faire lorsqu'ils réfléchissent à des lois et des politiques.

La première étape pour la sécurité en ligne des enfants est de réaliser une évaluation de l'impact sur les droits de l'homme, en mettant un accent particulier sur les droits des

enfants. Cela signifie utiliser la méthodologie proposée par les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, pour réfléchir aux droits de l'homme affectés dans leur ensemble, non seulement pour les adultes, mais spécifiquement pour les populations vulnérables et les enfants.

Et puis une deuxième étape consiste à réfléchir à l'ampleur de l'impact de ces droits. Quelle est l'échelle ? Quelle est la portée à travers différentes juridictions ? Et je pense que c'est l'une des choses que nous soulignons toujours : même si vous êtes l'UE et que vous envisagez des politiques qui affectent le chiffrement de bout en bout, vous devez savoir que cela a un impact sur les lois et les politiques dans le monde entier.

Et comme vous l'avez dit, nous travaillons sur ces décisions politiques à travers le monde, et je ne peux pas vous dire combien de fois nous avons vu des dispositions, par exemple, de l'Online Safety Act du Royaume-Uni, copiées-collées dans de nouvelles lois sur la cybersécurité où le contexte est évidemment très différent dans des pays où l'état de droit n'est peut-être pas également respecté, et cela est bien sûr une préoccupation majeure.

Une fois cette évaluation de l'impact sur les droits de l'homme réalisée, nous devons vraiment réfléchir à quelles mesures nous pouvons maintenant mettre en place qui tiennent compte de tous ces différents droits affectés. Et c'est là que le terme proportionnalité devient important, et je pense que lorsque nous examinons les débats autour de la sécurité des enfants et du chiffrement de bout en bout.

Tout le monde affirme que ses mesures sont proportionnées. Et ce qui me frappe, c'est que les gens semblent penser que la proportionnalité n'a pas vraiment de méthodologie. C'est juste quelque chose que l'on ressent, si l'un ou l'autre est plus important, alors on revendique simplement la proportionnalité de cette mesure spécifique.

Et je pense, bien sûr, venant d'Allemagne et travaillant beaucoup au sein de l'UE, que nous mettons beaucoup l'accent sur la méthodologie derrière les tests de proportionnalité. Et il y a deux choses que j'aimerais souligner. La première est de se demander si cette mesure est vraiment nécessaire. Avons-nous des mesures tout aussi efficaces mais moins intrusives ?

Et ce n'est qu'une fois que nous aurons épuisé ces mesures que nous pourrons envisager des mesures plus intrusives. Et je pense que lorsque nous réfléchissons à des mesures moins intrusives, comme ces approches systématiques pour renforcer le système de protection de l'enfance, je pense que nous échouons encore considérablement dans tous les domaines. Si vous regardez certaines évaluations des systèmes de protection de l'enfance, même dans les pays du Nord global.

Le récit est presque toujours le même. Nous n'avons pas assez de travailleurs sociaux. Nous n'avons pas assez de forces de l'ordre spécialisées dans ces questions. Les

enseignants ne sont pas formés. Les médecins ne sont pas formés pour identifier les cas d'abus et d'exploitation. Alors ma question est, même si nous devions détecter toutes ces images d'abus sexuels sur enfants, qui va y répondre ?

Et donc, la réponse est probablement personne, car nous n'avons toujours pas un système de protection de l'enfance suffisamment équipé. Et je pense que c'est là que nous devons vraiment réfléchir à savoir si cette mesure est vraiment la meilleure façon de traiter ce problème. Et le deuxième point concerne le test de proportionnalité en soi, où l'une des premières étapes consiste à évaluer réellement, d'accord, à quel niveau un droit spécifique est-il atteint. Et ce niveau d'atteinte a une ligne rouge, et c'est ce que nous appelons l'essence du droit.

Et une fois que nous avons atteint l'essence d'un droit spécifique, alors c'est une ligne rouge. Et à ce moment-là, peu importe ce qui se trouve de l'autre côté de la balance, pour ainsi dire, ce droit est violé. ne peut pas être violé. Et cette ligne rouge, je pense, est quelque chose à laquelle nous devons vraiment réfléchir lorsque nous parlons d'abolir ou d'affaiblir le chiffrement de bout en bout dans le contexte des communications privées, car je dirais que cette ligne rouge a probablement été atteinte.

C'est quelque chose qui, je pense, n'est pas vraiment discuté suffisamment, et où nous devons vraiment revenir aux bases du droit des droits de l'homme, et évaluer de manière holistique ce que cette mesure signifie pour les droits de l'homme et les droits des enfants dans leur ensemble. Merci.

Sharayah Lane - Internet Society: Non, merci.

Et merci d'avoir mentionné la convention pour avoir un moyen de mesurer. Avoir un point de référence est vraiment utile et j'ai lu la convention sur les droits de l'enfant et je pense qu'il y a tellement de choses là-dedans qui sont pertinentes et qui s'alignent directement avec le chiffrement et l'accès des enfants au chiffrement en ligne.

Mais encore une fois, c'est une conversation en cours, donc je voulais passer à Mark. Vous avez fait une quantité significative de recherches sur le côté juridique de la technologie. Existe-t-il actuellement des lois soutenant le chiffrement dont nous devrions être au courant ? Si oui, quel pourrait être leur impact ? Sinon, pourquoi pensez-vous que c'est le cas ?

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Il y a très peu de lois qui disent réellement que vous devez avoir, je ne pense pas qu'il y ait de lois comme la Loi sur le chiffrement ou quelque chose de ce genre, mais nous avons un certain nombre de lois qui, en fait, soutiennent le chiffrement. En tant qu'universitaire européen travaillant aux côtés du Dr. Witting, aux Pays-Bas et au Royaume-Uni.

Le RGPD a évidemment une sorte de loi fondamentale sur la confidentialité des données et la protection des données pour l'UE avec un effet extraterritorial, et certains pourraient même parler de l'effet Bruxelles, en ce sens que d'autres pays doivent adopter ces règles pour se conformer à nos normes et avoir accès à notre marché.

Il y a deux ou trois choses différentes à ce sujet. La première est l'obligation de l'Article 25 concernant la protection des données dès la conception et par défaut. Donc, si vous développez une technologie où vous pourriez protéger les données, ou si vous devez protéger les données, alors en intégrant le chiffrement dès la phase de conception, ce n'est pas une obligation obligatoire de le faire, mais cela aide les entreprises à réfléchir aux risques et à prendre des mesures pour garantir que les données sont sûres et sécurisées.

Pourquoi est-ce important ? Parce qu'en vertu de l'article 32, les responsables du traitement et les sous-traitants sont tenus de mettre en œuvre des mesures techniques et organisationnelles appropriées pour sécuriser les données personnelles. Et l'une des choses mises en avant pour garantir la sécurité des données est le chiffrement. Quel est l'impact de cela ? L'impact est que, selon le RGPD, si des données chiffrées sont compromises lors d'une violation mais restent inaccessibles grâce à un chiffrement fort, les sanctions pour l'entreprise pourraient être considérablement réduites.

Cela devient donc une incitation majeure pour les entreprises à mettre en œuvre des protocoles de chiffrement. Le fait est, comme je l'ai suggéré plus tôt, que le RGPD a un effet d'entraînement sur les lois de protection de la vie privée et des données dans le monde entier. De nombreuses entreprises, même celles en dehors de l'UE, adoptent le chiffrement comme une meilleure pratique pour se conformer.

Les géants mondiaux de la technologie comme Apple, WhatsApp et Google se sont tournés vers le chiffrement de bout en bout en partie pour se conformer aux normes du RGPD. Le chiffrement de bout en bout de WhatsApp garantit que seules les parties communicantes peuvent, en théorie, lire les messages, empêchant même l'entreprise d'accéder au contenu.

Aux États-Unis, le CCPA, le California Consumer Privacy Act, souvent considéré comme l'équivalent américain du RGPD, souligne l'importance de sécuriser les données personnelles. Ce n'est donc pas obligatoire, mais c'est traité comme un facteur atténuant lors de l'évaluation des sanctions pour les violations de données, tout comme le RGPD. Si une entreprise subit une violation mais peut prouver que les données compromises étaient cryptées, la responsabilité et les dommages peuvent être réduits. Le CCPA est en fait devenu un catalyseur pour les lois fédérales et étatiques sur la confidentialité.

Si vous construisez des lois sur le modèle du CCPA, l'incorporation du chiffrement devient une mesure de sécurité recommandée. La loi relativement méconnue sur la confidentialité et la protection des données dans l'UE est la directive sur la vie privée et

les communications électroniques. Elle est souvent appelée la loi sur les cookies. Elle régit la confidentialité des communications au sein de l'UE.

L'idée ici est que cette loi et le règlement proposé qui la remplacera devraient renforcer le rôle du chiffrement pour garantir la confidentialité des communications électroniques. Ces lois en elles-mêmes, vous pouvez aller au Brésil, vous pouvez voir le chiffrement comme une pratique de sécurité standard pour les entreprises opérant au Brésil.

Cela aide le chiffrement à montrer qu'ils se sont conformés à la LGPD et aussi à rester compétitifs sur les marchés mondiaux. Ensuite, vous avez d'autres spécificités sectorielles, comme la HIPAA aux États-Unis, la loi sur la portabilité et la responsabilité en matière d'assurance maladie. Encore une fois, elle ne rend pas le chiffrement obligatoire, mais elle incite les prestataires de soins de santé, les régimes de santé et leurs partenaires commerciaux à mettre en place des mesures de protection techniques pour protéger les informations de santé.

Il s'agit donc d'une mesure de protection adressable, ce qui signifie que bien qu'elle ne soit pas obligatoire, elle doit soit être mise en œuvre, soit documenter pourquoi une mesure alternative est suffisante. Ainsi, même les réglementations comme HIPAA favorisent l'expansion du chiffrement dans la technologie de la santé. Alors que nous construisons des systèmes entiers pour le partage des données de santé d'un fournisseur à un autre, pour travailler avec des médecins, des hôpitaux, des compagnies d'assurance, etc., afin de transférer les données de santé de manière fluide et transparente, le chiffrement est considéré comme l'outil pour protéger la confidentialité de ces communications.

Il y a des éléments dans l'amendement de la législation sur les télécommunications et autres en Australie sous la loi d'assistance et d'accès. Voici un autre exemple de tentative de rendre le chiffrement obligatoire. Le dernier point est pourquoi n'y a-t-il pas plus de lois rendant le chiffrement obligatoire ? Dans certains domaines, cela revient à équilibrer la sécurité nationale et la vie privée.

Nous avons abordé ce point dans ma discussion précédente. Les gouvernements hésitent à l'imposer car cela pourrait interférer avec les opérations des forces de l'ordre et de la sécurité nationale. Dans d'autres pays en développement, il semble que l'infrastructure juridique pour soutenir le chiffrement n'a pas encore pleinement évolué, et donc vous n'avez pas de lois sur la vie privée en vigueur, et le chiffrement n'a pas toujours été une priorité.

Et le troisième est la pression réelle des régimes autoritaires. Ainsi, le chiffrement est perçu comme un outil pouvant permettre la dissidence, affaiblissant ainsi le contrôle de l'État sur l'information. En conséquence, certains régimes découragent activement l'utilisation du chiffrement ou imposent des restrictions légales à son égard. Vous

pouvez donc voir la sorte de dichotomie entre la vie privée et la sécurité, et entre l'autoritarisme et la démocratie.

Et je pense savoir de quel côté je veux être et je vais m'en tenir à cela. Merci beaucoup.

Sharayah Lane - Internet Society: Oui, merci pour cet aperçu. Et je pense que nous continuerons probablement une partie de cette conversation lors de notre prochain panel, car ce sera un sujet important. Ce qui est si intéressant du côté juridique du chiffrement, c'est que vous voyez une telle différence où certains endroits travaillent à protéger légalement ce droit à la vie privée et certains pays travaillent à le démanteler totalement.

Et il est juste intéressant de constater qu'il y a une si grande différence entre les deux et de voir ces différentes tendances à travers le monde. C'est une partie majeure de notre travail de plaidoyer à l'ISOC : examiner les lois sur le chiffrement ou les lois qui affaibliraient le chiffrement dans le monde entier et mener des actions de plaidoyer à l'échelle mondiale.

C'était un excellent aperçu. Merci pour cela. Je pense que nous avons le temps pour une dernière question. Je vais poser notre question individuelle avant de passer à la session de questions-réponses. Dernière chance, nous allons bientôt passer à la session de questions-réponses, donc si vous avez des questions pour nos panélistes, veuillez les poser dans la fonctionnalité de questions-réponses sur Zoom, qui se trouve en bas près du bouton de chat et du bouton des participants sur votre écran.

Dernière question, je voulais revenir à Ezequiel. Et je voulais demander, quelle est une chose importante, et je dis bien une chose car je suis sûr qu'il y en a beaucoup, mais quelle est une chose importante que vous avez apprise en créant une organisation comme Faro Digital sur les expériences des jeunes en ligne et comment nous pouvons travailler pour améliorer ces expériences à l'avenir ?

Ezequiel Passeron - University of Barcelona (2): Super. Merci pour la dernière question. Ces dernières années, en raison de l'économie de l'attention et du fonctionnement des plateformes, nous avons remarqué un intérêt croissant et une forte influence sur la subjectivité des jeunes concernant ce que nous appelons la monétisation. Cela se réfère à la recherche de gratification et de récompenses dans chaque action, une caractéristique commune à tout réseau social.

Cela crée une dynamique où Internet ou l'espace numérique est perçu comme une source de revenus à domicile sans apparemment peu d'effort. Des pratiques telles que les jeux d'argent en ligne où les adultes, nous sommes très préoccupés, mais lorsque nous allons dans des ateliers et écoutons les jeunes, ils ne le voient pas comme une conception honteuse.

Il y a donc un très grand fossé ou une brèche que nous devons combler. La vente d'images intimes, les investissements ont émergé en Argentine. Une réglementation est en place depuis quelques semaines, permettant aux personnes de plus de 13 ans d'entrer sur le marché financier. Et cette réglementation, ce n'est pas quelque chose d'isolé. Merci.

Cela, cela fait référence à une pratique qu'ils ont en ligne dans leurs pratiques en ligne. Donc, ce que nous voyons comme un problème ou plutôt comme un défi, c'est la question de la confiance. Ce qui les amène à, à devenir victimes d'escroqueries numériques, par exemple. En Argentine, nous parlons de Poncidemic, un problème alimenté par l'émergence de ces jeunes influenceurs qu'ils appellent Poncipros.

Ils sont tout le temps comme, mec, tu dois investir dans ça, tu dois suivre ce cours, ce sont des soi-disant influenceurs qui encouragent d'autres jeunes à devenir leurs propres patrons, à avoir du temps libre, à gagner beaucoup d'argent chaque mois depuis leur canapé. Bien sûr, ce sont les anciennes arnaques de type Ponzi qui existaient avant Internet, mais qui ont maintenant trouvé dans les plateformes numériques des moyens de recruter et d'attirer plus de gens, surtout dans des contextes économiquement défavorisés.

Dans le monde numérique, nous vivons dans un territoire où notre attention est exploitée, où nos émotions et désirs sont au cœur des affaires des grandes entreprises technologiques. C'est pourquoi nous devons créer, c'est pourquoi je parle de créer du temps et des espaces, juste entre parenthèses, nous aimons le concevoir comme une métaphore.

Nous devons protéger, nous devons prendre soin, nous devons créer ces espaces où les enfants et les jeunes peuvent se développer ensemble avec les autres. Où ils peuvent étudier et pratiquer les affaires mondiales sans but, sans objectif, ni utilité. Juste en essayant de comprendre le monde et de le renouveler, comme Hannah Arendt nous l'a dit il y a un demi-siècle.

Notre époque est celle de ce grand problème, Wilson. CODIS, nous avons des émotions paléolithiques, des institutions de l'âge de pierre, et des technologies divines. Nous adorons cette phrase. Nous pensons que nous sommes à une époque où nous devons retrouver le sens de la phrase de Descartes, Cogito Ergo Sum. Quand nous pensons à cette phrase, nous la traduisons par, Je pense, donc je suis.

Mais quand nous étudions l'étymologie du mot cogito, nous découvrons qu'il se réfère à la fois à "je pense" et à "je prends soin". Alors je vous laisse une question. Qui sont ceux dans notre société qui sont responsables des pratiques de soin ? Je pense qu'il y a un enjeu révolutionnaire immense et rebelle que nous devons combattre et défendre pour placer les soins à un autre endroit dans notre société.

Merci.

Sharayah Lane - Internet Society: Non, c'est un excellent rappel que beaucoup du défi ou du problème réside dans notre façon de le percevoir. Et la manière dont nous abordons les choses, je pense que beaucoup de nos approches jusqu'à présent proviennent d'une perspective et d'une compréhension quelque peu dépassées. Il est nécessaire de réfléchir profondément à ces questions, de vraiment comprendre ce que les jeunes affrontent et traversent, et de prendre le temps de le comprendre.

Toutes ces choses sont si importantes dans notre conversation plus large. Merci d'avoir abordé l'aspect philosophique de la question, car je pense que c'est un élément manquant. Un élément manquant de la conversation. Donc, nous allons, il ne nous reste que quelques minutes. Nous allons passer à notre session de questions-réponses avec le public.

J'ai une question traduite ici. Elle dit, et c'est pour n'importe lequel des panélistes, alors n'hésitez pas à intervenir et à répondre. J'ai trouvé le chiffrement des images d'enfants intéressant. En tant que facteur de protection contre l'utilisation des images de ce profil utilisateur ou non utilisateur, selon l'âge de l'enfant, le chiffrement pourrait-il être utilisé pour rechercher, sélectionner et supprimer les images des enfants qui n'ont pas l'autonomie d'exprimer leur volonté ?

Larry Magid - ConnectSafely.org: Cela pourrait certainement être utilisé pour cacher ces images afin de s'assurer qu'elles ne soient pas partagées sans le consentement de l'enfant ou de ses parents. Je ne suis pas sûr que cela puisse être utilisé de manière indépendante pour les rechercher. Peut-être que certains des experts techniques ont une réponse à ce sujet.

Mais cela peut certainement protéger la confidentialité de ces images pour s'assurer qu'elles ne parviennent qu'aux personnes avec qui elles sont destinées à être partagées.

Sharayah Lane - Internet Society: Oui, donc en tant que mesure rétroactive, ou pour revenir en arrière et supprimer ou cacher des images, je ne pense pas que le chiffrement puisse être utilisé comme un tel outil, mais c'est plutôt une fonctionnalité préventive, donc cela empêcherait Merci. Merci. L'utilisation non autorisée des images dès le départ, mais si cela,

Larry Magid - ConnectSafely.org: s'il y a, du moins aux États-Unis, une image sexuellement explicite d'un enfant en ligne, vous pouvez aller sur, je crois que c'est takeitdown.

org, c'est un service de NECMEC, et le faire retirer, et puis il y a un certain nombre de sites qui aident à lutter contre la pornodivulgation et d'autres distributions d'images intimes d'adultes également. Donc, il existe des outils que vous pouvez utiliser pour les supprimer, mais je ne crois pas, comme vous l'avez dit, que vous puissiez les chiffrer rétroactivement.

Sharayah Lane - Internet Society: D'accord, je vais juste obtenir le lien vers cette ressource. Je vais également le mettre dans le chat. Et avec cela, je sais que je crois que Mark a répondu un peu à cette question dans sa réponse, mais je vais aussi la poser à tout le groupe. En ce qui concerne la législation et les politiques sur la sécurité en ligne des enfants, il y a une tendance aux propositions descendantes, plutôt qu'aux mesures qui pourraient permettre aux parents de prendre des décisions éclairées sur les activités en ligne de leurs enfants.

Par exemple, une proposition consiste à interdire légalement aux mineurs d'utiliser les réseaux sociaux après certaines heures. Existe-t-il un équilibre entre les règles imposées par le gouvernement, comme les lois sur la protection des données aux États-Unis, et l'autonomisation des parents ? Et il est dit, n'hésitez pas à contester entièrement ma formulation.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Puis-je ajouter à ma réponse ?

Sharayah Lane - Internet Society: Oui.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Sabina avait aussi levé la main. Je suis sûr qu'elle a quelque chose à dire à ce sujet. Je pense qu'il est important que les parents réalisent que les enfants ont également droit à la vie privée vis-à-vis de leurs parents. Et que nous parlons souvent de cela comme étant quelque chose que nous voulons donner aux parents pour qu'ils aient plus de contrôle.

Mais je pense aussi que nous devons reconnaître que la nouvelle norme devrait être que les enfants aient un espace sûr pour communiquer librement, sans l'intervention des parents. Et je vais vous donner quelques exemples très rapidement pour illustrer ce point. Le premier est qu'il existe de nombreuses cultures où être LGBT est mal vu à la maison.

Et si vous allez explorer votre sexualité, votre identité sexuelle, vous voulez pouvoir parler librement, sans que vos parents fouinent et examinent vos communications. Le deuxième, et le plus évident pour les personnes des cultures occidentales, je pense, surtout à notre époque, ce sont les personnes qui recherchent des informations sur la santé sexuelle et leur identité.

Et puis, le troisième point est de protéger l'enfant des communications qui pourraient être nuisibles, non désirées ou non sollicitées. Donc, si vous leur offrez un espace sûr pour communiquer, l'enfant est en fait habilité à tenir les autres enfants à l'écart. C'est mon ajout à la question, mais je pense qu'il est également important de reconnaître que les parents doivent offrir à l'enfant un espace sûr où il peut communiquer librement, sans surveillance parentale.

Et je suis sûr que Sabina aura également d'autres réflexions à ce sujet.

Dr Sabine K Witting - Leiden University: Oui, merci, Sabine. Oui, merci beaucoup. Je pense que Mark a également abordé ce point. Je pense que lorsque nous nous concentrons toujours sur les parents, nous disons oh, nous ne devrions pas faire ou nous ne devrions pas empiéter sur l'anti-chiffrement. Nous devrions nous concentrer sur la littératie numérique et le rôle des parents.

Et je suis d'accord avec cela. Et je pense qu'il y a, dans une certaine mesure, une idée fausse selon laquelle nous pensons que les parents agissent toujours dans l'intérêt supérieur de l'enfant. Et je pense que ce n'est certainement pas le cas. Et Mark a mentionné quelques exemples où cela pourrait ne pas être le cas, donc mettre le parent en charge ne rendra pas nécessairement l'enfant plus en sécurité, et je pense que c'est quelque chose à considérer.

Et je pense aussi que dans ce débat, il y a un peu de, c'est un, il y a soit un accent sur le chiffrement de bout en bout ou sur la littératie numérique, et c'est soit on utilise ceci, soit on utilise l'autre mesure. Et je pense que cela laisse un peu trop facilement les entreprises technologiques s'en tirer. Parce que même si nous ne voulons pas qu'elles créent des failles ou qu'elles reviennent sur ce chiffrement de bout en bout, nous voulons que les entreprises technologiques créent un environnement sûr.

Pour les enfants, et cela devrait être fait par des efforts législatifs. Mark et moi avons écrit un chapitre de livre à ce sujet, qui, je pense, sortira l'année prochaine, où nous examinons le Digital Services Act, par exemple, et les types de mesures que ce dernier impose aux intermédiaires pour créer activement un environnement sûr pour les enfants, comme le signalement obligatoire de matériel illégal, la création de mécanismes de signalement adaptés aux enfants, et la notification.

Et ainsi de suite. Je pense donc qu'il y a certainement un rôle important pour l'éducation numérique, mais nous ne devrions pas seulement mettre la responsabilité sur les parents ou les enfants et laisser les entreprises technologiques s'en tirer à bon compte. Merci.

Sharayah Lane - Internet Society: Oui, je suis d'accord. Merci. Et Larry.

Larry Magid - ConnectSafely.org: Oui, cela varie selon les pays, mais aux États-Unis, il y a, je ne dirais pas un consensus, mais la culture est construite autour de l'idée que les parents contrôlent leurs enfants et que tous les droits d'un enfant passent vraiment par le parent, tandis que les Européens ont une attitude quelque peu différente, je pense, et le fait est, comme Mark l'a si bien dit, que les enfants ont besoin d'un certain degré d'autonomie, même vis-à-vis de leurs propres parents, et pas seulement pour les raisons que Mark a spécifiées, qui étaient toutes très bonnes, qu'un parent pourrait en fait avoir une attitude différente envers la santé reproductive, l'identité de genre, l'orientation sexuelle, etc.

Mais aussi, tous les parents ne sont pas à l'aise ou équipés pour interagir avec les autorités, et même les entreprises de médias sociaux peuvent être perçues comme une autorité. Ils peuvent avoir des préoccupations concernant l'immigration, craignant que, en s'impliquant en ligne pour leurs enfants, ils augmentent le risque d'avoir des problèmes avec les autorités de l'immigration.

Ils peuvent ne pas avoir la littératie, que ce soit la littératie technique ou la littératie linguistique. Ils peuvent ne pas être au courant, et il y a des enfants qui, malheureusement, ont des parents qui ne sont pas bien équipés, peut-être à cause de problèmes de santé mentale, ou simplement parce que leur vie est trop chaotique ou trop occupée, etc.

Tous les enfants ne sont pas soutenus par leurs parents et tous les parents ne sont pas équipés pour fournir le type de soutien et de cadre de permission que certaines de ces lois exigent d'eux. Je m'inquiète donc des enfants laissés pour compte pour toutes sortes de raisons, et ce, avant même que ces lois ne soient adoptées.

Nous devons réfléchir aux conséquences imprévues.

Sharayah Lane - Internet Society: Oui, c'est très important. Je tiens à vous remercier tous de nous avoir rejoints aujourd'hui. Il nous reste environ 6 minutes ensemble et, pour conclure, j'aimerais demander à chacun de nos panélistes une pensée finale, donc une phrase ou deux sur le rôle du chiffrement dans la sécurité des enfants.

Alors la question pour vous est : pourquoi le chiffrement est-il important pour vous en ce qui concerne la sécurité des enfants en ligne ? Et nous pouvons commencer avec Mark.

Dr Mark Leiser - Digital, Internet, and Platform Regulation: Pour ma part, je pense qu'en une ou deux phrases, au niveau sociétal, la confidentialité et la sécurité ne sont pas seulement liées mais sont des piliers qui se renforcent mutuellement. Merci. Dans une démocratie fonctionnelle, lorsque les enfants se sentent autonomes et en sécurité, sachant que leurs informations personnelles ne leur causeront pas de tort, cela contribue à un sentiment plus large de sécurité des enfants et de confiance tant dans l'environnement numérique que physique.

Et en affaiblissant les protections de la vie privée, on peut alors entraîner une perte de sécurité. Et je pense que lorsque vous donnez la priorité à la vie privée et à la sécurité de l'enfant, vous assurez la protection de leurs droits, de leurs libertés civiles et de leur confiance dans les technologies numériques.

Sharayah Lane - Internet Society: Wow, c'est bien. Ezequiel, à toi.

Ezequiel Passeron - University of Barcelona: C'est compliqué de passer après Mark.

Merci pour cela. Oui, je pense d'un côté que nous devons vraiment poser des questions plus larges, comme Sabine nous l'a dit avant, nous essayons toujours de penser à une solution technique pour les problèmes que nous avons dans notre relation avec les techniques. Je pense que la nature humaine est technique, n'est-ce pas ?

Sans une langue commune, nous ne pouvons pas nous comprendre ici. C'est pourquoi nous pensons qu'il est nécessaire de commencer à trouver de nouvelles voies et techniques pour protéger nos droits fondamentaux. Je pense que l'autonomisation des enfants et des jeunes est essentielle. Je crois vraiment que cette métaphore créée en 2001 des Natifs Numériques, je pense qu'elle est apparue comme un problème majeur pour nous, les adultes, de prendre soin des enfants parce que nous pensons qu'ils savent tout du monde numérique et que nous ne pouvons pas les aider.

Je pense vraiment que le cryptage est un moyen sûr pour être autonomes dans un territoire où de nombreuses entreprises essaient de faire des affaires avec notre temps et notre attention. Je crois vraiment que ce type de techniques peut protéger nos droits et créer des environnements puissants pour que nous puissions y vivre et en profiter sans être exploités, en quelques mots.

Sharayah Lane - Internet Society: Oui, c'est parfait. Merci. Sabine ?

Dr Sabine K Witting - Leiden University: Oui, je pense que si nous continuons à polariser la discussion comme elle l'est actuellement, nous créons une distraction parfaite pour les deux parties prenantes qui devraient en fait investir dans la prévention et la réponse, à savoir les gouvernements en investissant réellement dans le système de protection de l'enfance, mais aussi les entreprises technologiques, en créant des produits sûrs et respectueux des droits.

Donc, je pense que mon appel serait de vraiment prendre du recul et de se demander Cui Bono, et ce sont certainement les gouvernements et les entreprises technologiques. Merci.

Sharayah Lane - Internet Society: C'est tellement important. Merci. Et enfin, Larry.

Larry Magid - ConnectSafely.org: Je pense que toutes les personnes, quel que soit leur âge, ont droit à la vie privée et à la sécurité, ainsi qu'à des communications qui restent entre elles et les autres.

Et je pense qu'après avoir écouté les intervenants et réfléchi à notre rôle, nous devons renverser la situation. Sur cette notion de protection de l'enfance et ne pas permettre à ceux qui pensent que la protection de l'enfance consiste simplement à donner aux forces de l'ordre tous les outils et moyens de surveillance dont ils ont besoin, mais aussi à protéger les gens des criminels, des membres de la famille, si nécessaire, et des connaissances, des gouvernements qui pourraient les opprimer.

Ou simplement parce qu'ils veulent avoir des communications privées. Et enfin, je pense que nous devons redoubler d'efforts en matière d'éducation. Cela me fait vraiment réfléchir, en pensant à la Journée pour un Internet plus sûr et au travail que ConnectSafely fait avec les adolescents, que nous devons tous fournir aux adolescents, et aux enfants d'ailleurs, tous les outils possibles pour les aider à protéger leur vie privée et leur sécurité.

Et cela s'ajoute à tout ce que nous continuons de faire concernant le phishing et les mots de passe. Nous leur apprenons également à utiliser un chiffrement robuste comme moyen de se protéger.

Sharayah Lane - Internet Society: Oui, encore une fois, merci beaucoup à tous. Nous avons eu une richesse d'expertise et de connaissances lors de l'appel d'aujourd'hui, donc je vous remercie vraiment d'avoir pris le temps de partager avec nous tous aujourd'hui.

Nous avons d'excellentes ressources dans le chat, alors n'hésitez pas à consulter les liens partagés aujourd'hui. Nous espérons que vous pourrez nous rejoindre pour notre prochaine session, qui commencera dans environ 10 minutes, intitulée "Encryption Arrested : l'arrestation de Pavel Durov de Telegram pour ne pas avoir enregistré les services cryptés."

Encore une fois, cela semble être un complément à notre conversation juridique sur le chiffrement et la loi d'aujourd'hui. Donc, si vous souhaitez faire une pause, vous aurez environ 10 minutes avant notre prochaine session pour la Journée mondiale du chiffrement, mais merci à nos intervenants et merci à tous nos participants de nous avoir rejoints aujourd'hui.

D'accord. Merci. Au revoir.