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

Cryptage, arrêté : L'arrestation de Pavel Durov de Telegram

Greg Nojeim - CDT: Bonjour à tous. Je m'appelle Greg Nojeim. Je travaille au Centre pour la Démocratie et la Technologie. Bienvenue à cette partie de la Journée Mondiale du Chiffrement, le panel sur "Chiffrement Arrêté : Les Implications de l'Arrestation de Pavel Durov de Telegram pour des Accusations Liées au Chiffrement". Comme je l'ai dit, je suis Greg Nojeim, du Centre pour la Démocratie et la Technologie.

Je dirige notre projet de Sécurité et Surveillance. Je siège également au comité de pilotage de la Global Encryption Coalition, qui parraine cet événement et la Journée mondiale du chiffrement chaque année. Pardon, le 21 octobre de chaque année, la Global Encryption Coalition compte 434 membres répartis dans plus de 105 pays.

Le comité de pilotage de la Global Encryption Coalition comprend le Center for Democracy and Technology, mon organisation, Global Partners Digital, l'Internet Freedom Foundation, Mozilla Corporation et l'Internet Society, qui a gracieusement fourni la logistique pour la Journée mondiale du chiffrement.

Le contexte de cette affaire est qu'en août de cette année, la police française a arrêté le PDG de Telegram, Paval Durov, à l'aéroport Charles de Gaulle en France. Il a été arrêté par la police française. Il est citoyen français.

Il a été accusé de ne pas avoir respecté les demandes de retrait et de divulgation formulées par le gouvernement français, ainsi que de ne pas avoir enregistré un service chiffré et déclaré l'exportation de chiffrement. Il est important de garder à l'esprit, en discutant de cette affaire, que les accusations liées au chiffrement concernant Telegram sont un peu déplacées dans la mesure où la plupart des communications sur Telegram ne sont pas chiffrées.

Seules les communications en tête-à-tête sont chiffrées, uniquement lorsqu'une des parties active le chiffrement, et seulement lorsque les deux parties sont en ligne en même temps. Beaucoup de communications sur Telegram se font via des chaînes, elles sont diffusées à un large groupe, ou elles impliquent des discussions de groupe importantes. Aucun de ces types de communications n'est chiffré.

Donc, Telegram est plus un réseau social qu'une application de messagerie privée. Néanmoins, Durov a été arrêté pour des accusations incluant le non-enregistrement d'un service chiffré. Et je dois dire que cela a beaucoup préoccupé les personnes impliquées dans la défense du chiffrement, y compris notre organisation. En fait, je peux affirmer avec confiance que l'arrestation de M. Durov a été l'événement le plus discuté de 2024 sur la liste des participants de la Global Encryption Coalition.

Passons maintenant à nos panélistes pour éclaircir cette affaire. Tout d'abord, Noémie Levine. Elle est conseillère politique pour La Quadrature du Net, une organisation française de premier plan qui lutte pour les droits numériques. Elle travaille avec eux depuis plusieurs années, notamment sur des sujets de surveillance, comme la limitation des heures des services de renseignement et la documentation des pratiques policières, telles que l'utilisation de la vidéosurveillance biométrique algorithmique, ainsi que sur le chiffrement.

Nous allons commencer avec Noémie. Noémie, pourriez-vous nous dire quelles lois en France M. Durov est accusé d'avoir violées, et pourquoi a-t-il été arrêté, et je suppose si publiquement, en quelque sorte, directement à l'aéroport de Paris.

Noémie Levain - la Quadrature du Net: Bonjour à tous et merci pour l'invitation et de parler de ce sujet important. Comme vous l'avez bien décrit, le cas est assez singulier et compliqué, et cela ne ressemble pas à ce que nous avons vu auparavant. En tant qu'organisation française, nous étions aux premières loges pour constater cela.

Et nous pourrions, et comme vous l'avez mentionné, il y a deux niveaux dans cette affaire. Il y a un aspect juridique et un aspect politique. Sur les aspects juridiques, il est assez difficile de savoir exactement ce qui se passe car les seules informations que nous

avons sont celles fournies par le procureur de la République. Ils n'ont pas l'obligation de dire ce qui se passe, mais ils ont décidé de le faire.

Et c'est ainsi que l'aspect juridique et l'aspect politique se rejoignent, ce qui signifie que si Durev a été arrêté de manière aussi spectaculaire et avec le procureur public voulant divulguer des informations sur l'affaire, cela signifie qu'ils veulent en faire un événement politique et un avertissement, nous pensons, ou un grand, je veux dire, un événement important et peut-être un avertissement pour d'autres services de cryptage ou d'Internet.

Une fois que je dis cela, que savons-nous en ce moment ? Nous savons que Pavel Durov a été arrêté pour plusieurs raisons. La principale n'est pas le chiffrement, mais plutôt la modération de contenu, car Telegram est bien connu pour ne pas modérer suffisamment le contenu partagé, non pas dans les messages privés chiffrés, mais sur les listes publiques.

Donc, ce que nous comprenons des informations du procureur public est plus que cela. C'est cette approche envers Pavel Durov, ce qui signifie qu'il est poursuivi pour complicité de plusieurs infractions, telles que la pédopornographie, la pornographie infantile, et en disant qu'en tant que moyen de partage d'informations, Pavel Durov est pénalement responsable en tant que PDG de Telegram.

Mais une fois que nous disons cela, lorsque nous creusons un peu plus les informations que nous avons, nous voyons que cela peut ne pas concerner uniquement la modération de contenu, mais aussi le chiffrement et plus généralement le rôle d'intermédiaire technique. Nous pensons cela parce que dans les divers motifs et la base légale qui ont été communiqués, nous voyons des éléments concernant, comme vous l'avez mentionné, l'enregistrement ou la déclaration en tant que services de chiffrement, ce qui est en fait une vieille loi datant du début des années 2000 qui n'est pas vraiment connue pour être appliquée ou souvent appliquée.

Mais quand vous voyez que le juge, le procureur, utilise cette base légale, c'est qu'il y a quelque chose à voir autour des messages privés étant chiffrés. Et l'autre chose que nous avons en tête, c'est qu'ils disent que Telegram n'a pas respecté l'obligation de divulguer des informations à la police pour effectuer des interceptions légales.

Et généralement, ce motif est plus pour les écoutes téléphoniques ou les téléphones classiques. Et donc, nous nous disons, d'accord, si Telegram doit divulguer des informations pour l'interception, peut-être que ce sont les clés de chiffrement. Nous ne savons pas. Cela provient uniquement du communiqué de presse du procureur public. Et c'est, nous, et c'est vraiment difficile de savoir ce qui va se passer, mais nous voyons que c'est assez complexe et derrière la modération de contenu, nous pouvons croire que cela pourrait aussi être une porte ouverte pour ensuite poser des questions sur le fonctionnement du service et peut-être demander des informations sur le chiffrement.

Greg Nojeim - CDT: Alors, où en est l'affaire dans les procédures judiciaires en ce moment ? Va-t-il bientôt aller au tribunal ou est-ce là où nous en sommes dans les démarches ?

Noémie Levain - la Quadrature du Net: Donc ce n'est que le début de l'enquête. Il a été arrêté uniquement pour être interrogé. Nous saurons plus tard si le procureur maintiendra tous les motifs légaux qu'il a communiqués, ou s'il dira peut-être, d'accord, nous ne poursuivons que.

Pavel seulement pour trois d'entre eux, et nous abandonnons tout le reste. Nous ne savons pas cela, et c'est encore le début donc cela peut durer des années. Et aussi, comme je l'ai mentionné plus tôt, il n'y a aucune obligation de divulguer des informations sur l'affaire, donc nous sommes en quelque sorte dépendants de ce que dira le procureur, ou, comme cela arrive souvent en France, s'il y a des fuites dans la presse.

Donc maintenant, il s'agit simplement d'une enquête pour voir si Telegram a joué un rôle, a eu un rôle plus important dans toutes les infractions et les motifs légaux dont il a été accusé, tels que la complicité de plusieurs crimes ou le fait de ne pas avoir déclaré certains outils de cryptage ou de ne pas avoir divulgué des informations pour des interceptions.

Greg Nojeim - CDT: Alors, quel est le contexte politique pour le chiffrement en France ? Le gouvernement est-il favorable au chiffrement ?

Noémie Levain - la Quadrature du Net: Donc, si nous revenons aux années 90, il est important de savoir que la France a été l'un des derniers pays à abandonner le chiffrement lorsqu'il était une compétence privée de l'État.

Donc, ce n'est qu'à la fin des années 90 qu'elle l'a libéralisée et rendue gratuite. Et ces dernières années, nous avons été inquiets car nous avons vu des tentatives de restriction sur le chiffrement et les communications privées à plusieurs niveaux, politiques et judiciaires. Par exemple, l'année dernière, il y a eu ce grand procès contre des militants.

Il y avait beaucoup de choses dans cette affaire, ils ont été poursuivis pour avoir planifié une attaque qu'ils n'ont pas commise, mais parmi tous les éléments, il a été dit qu'ils utilisaient des outils de cryptage tels que Signal ou Tor, ou un VPN, et le juge a dit que cela montrait qu'ils voulaient vivre dans la clandestinité et qu'ils voulaient cacher quelque chose.

Donc, c'était comme si on revenait 30 ans en arrière avec l'ancienne approche de l'encryption, disant que c'était un outil criminel. C'était vraiment un précédent. Nous étions vraiment inquiets qu'un juge puisse penser que l'utilisation de Signal puisse être

considérée comme une preuve, entre autres choses, que cela puisse faire de quelqu'un un criminel.

Dans d'autres contextes, nous voyons un cadre politique plus général, où le gouvernement français affirme toujours que certains réseaux sociaux, ou certaines communications, font partie de certains crimes. Laissez-moi m'expliquer. Par exemple, l'année dernière, il y a eu des émeutes dans le pays après qu'un policier a tué un jeune garçon.

Et le gouvernement a demandé aux réseaux sociaux de supprimer certains contenus et a déclaré que les réseaux sociaux avaient une part de responsabilité. La même chose s'est produite cette année en Nouvelle-Calédonie, qui est un département français où il y a eu des émeutes et le gouvernement a bloqué TikTok sur toute l'île.

Nous voyons donc une nouvelle ère où le gouvernement cible les réseaux sociaux, cible les moyens de communication en disant qu'ils sont complices. Vous pouvez voir l'indice de complicité dans le crime. Et pour finir, nous voyons également de nombreux cas où la police, la police française, a aidé. À affaiblir le chiffrement, comme AnchorChat, ou SkyECC, ou plus récemment, l'application de messagerie Ghost, où la police a joué un grand rôle dans l'affaiblissement, dans la recherche d'un moyen de contourner le chiffrement.

Donc, vous pouvez voir qu'en ce moment, c'est un gros sujet en France, et en fait, certaines institutions disent qu'aujourd'hui le chiffrement est un obstacle pour elles, et elles essaient de trouver des moyens de le contourner dans les affaires criminelles.

Greg Nojeim - CDT: Laissez-moi rester avec vous un peu plus longtemps. Cela m'a vraiment surpris qu'une personne puisse être arrêtée pour ne pas avoir enregistré un service de cryptage, surtout lorsque la plupart des communications sur le service ne sont même pas cryptées.

C'était vraiment un choc. Et je pense que cela envoie un message aux autres PDG de grandes entreprises qu'ils doivent s'inquiéter d'être arrêtés lorsqu'ils voyagent.

Avez-vous déjà entendu parler de quelqu'un arrêté pour ne pas avoir enregistré un service crypté ? Avez-vous déjà entendu parler d'un autre pays exigeant une telle inscription ?

Noémie Levain - la Quadrature du Net: Non, en fait c'est la première fois et c'est pourquoi au début je disais qu'il y a à la fois des aspects juridiques et politiques liés, car nous pensons qu'ils utilisent cette vieille loi.

Donc cette obligation d'enregistrement est apparue au début des années 2000 avec la libéralisation du chiffrement. Ils ont dit, d'accord, le chiffrement est libre, mais il y a

quelques obligations pour garder un peu de contrôle. Mais nous n'y avons jamais prêté attention parce que nous n'avons jamais entendu d'histoires à ce sujet. Alors quand vous voyez que certains juges, certains procureurs, ressortent cela des bas-fonds des lois, que tout le monde a oublié.

Vous vous dites, d'accord, peut-être qu'ils veulent essayer tout ce qu'ils peuvent pour atteindre Paval Durov, y compris les messages chiffrés. Ou peut-être qu'ils ne savent pas ce qu'ils font, ou peut-être qu'ils savent vraiment ce qu'ils font et qu'ils veulent vraiment atteindre la partie chiffrement, ou qu'ils veulent atteindre Telegram en général, parce que Telegram est montré comme l'ennemi, je ne sais pas si c'est le bon mot, mais c'est pourquoi nous pensons que c'est très politique de rendre cela public, de l'arrêter comme ça, de l'arrêter sur des bases légales très étranges et surprenantes, c'est pour envoyer un signal, pour avertir d'autres services qui ne se conformeraient pas aux obligations légales de modération de contenu.

C'est ce que nous pensons. Mais c'est toujours disproportionné. Il est normal que vous ayez été surpris, et il est normal que vous soyez inquiet, et nous sommes inquiets aussi.

Greg Nojeim - CDT: Oui, je dois dire que c'était un choc. Notre autre intervenant, Daniel Kahn Gilmore, a des difficultés à se connecter, donc nous devrons peut-être continuer l'événement, juste toi et moi, Noémie.

Continuons la conversation. Ce dont je voulais parler avec Dan, c'est le fait que les services chiffrés ne sont pas tous WhatsApp. Ils ne sont pas tous énormes. En fait, vous pourriez avoir une conversation chiffrée dans un jeu. Et il y a des gens qui développent toutes sortes de moyens de communication qui incluent le chiffrement mais qui ne sont pas vraiment de grands services. Ce sont juste des outils que quelqu'un a créés pour pouvoir communiquer avec ses amis et avec des personnes partageant les mêmes idées.

Parle-nous un peu, Noémie, de la surprise que cela peut représenter pour une personne qui développe un service de messagerie chiffrée de se retrouver soudainement confrontée à l'obligation, qu'elle ne pouvait pas connaître, d'enregistrer son service auprès du gouvernement.

Noémie Levain - la Quadrature du Net: Oui, bien sûr, je suis sûr que beaucoup de gens viennent de découvrir cette obligation. Et encore une fois, je pense qu'ici, la spécificité est de la lier à l'aspect politique. Je ne suis pas magicien, je ne sais pas tout, mais je ne pense pas que le gouvernement ferait cela avec un petit service, pas encore, ce n'est pas encore le premier ennemi, mais quand même, ennemi. Par exemple, j'ai découvert que la France était le seul pays à avoir ce genre d'obligation. Nous savions que c'était une vieille loi, mais quand je vous ai vu être choqué, et j'ai vu beaucoup de gens dans le monde être choqués par cette obligation, nous avons réalisé à quel point la France était mauvaise avec cela.

Et aussi, nous savons que Telegram a beaucoup de problèmes avec de nombreux pays. Et quand vous voyez que la France est celle qui a décidé de tirer en premier, sans se soucier autant des droits de chiffrement et des droits à la vie privée, vous pouvez sentir que la démocratie en France n'est pas, n'est pas au meilleur stade qu'elle était.

Mais bien sûr, pour les petits fournisseurs, ce n'est pas du tout un bon signe pour ce qui pourrait arriver dans les prochaines années, si la loi change ou si certains juges décident d'appliquer cette loi que tout le monde a oubliée.

Greg Nojeim - CDT: Merci, Noémie. Passons maintenant à Daniel Kahn Gillmor qui s'est joint à notre discussion.

Bonjour, Daniel. Pourquoi ne pas prendre une minute pour vous présenter et nous parler de l'importance de cette affaire pour les technologues et les autres personnes travaillant avec le chiffrement ?

Daniel Kahn Gillmor - ACLU: Bien sûr. Merci. Et encore une fois, désolé pour le retard. Je suis Daniel Kahn Gillmor.

Je suis technologue pour l'Union américaine pour les libertés civiles. C'est une ONG américaine qui se concentre sur les droits civils et les libertés civiles, et je travaille sur le projet de technologie de la confidentialité des discours, car notre infrastructure a un impact sur les types de droits, qu'il s'agisse de préoccupations en matière de confidentialité ou de censure. Je suis également développeur de logiciels libres et je contribue au projet Debian, qui est une distribution de logiciels libres Linux fondamentale.

C'est un système d'exploitation. C'est ce que j'utilise pour vous appeler. Et j'ai tendance à n'utiliser que des logiciels libres, ce qui explique les difficultés que j'ai eues pour me connecter ici, car Zoom voulait constamment me faire passer par leur logiciel propriétaire, que je préfère ne pas utiliser. Cela dit, je suis également actif au sein de l'IETF. Je vois déjà des personnes dans le chat qui sont également actives au sein de l'IETF.

L'IETF est l'Internet Engineering Task Force. Et je suis préoccupé par la manière dont nous assurons une infrastructure fonctionnelle pour avoir des communications sécurisées et résistantes à la censure. Une de mes grandes préoccupations, donc la France n'est pas la seule nation à avoir des lois qui régulent l'importation ou l'exportation de la cryptographie.

Et je n'ai réussi à entendre que des parties de la session en raison de certains problèmes de connexion que j'ai rencontrés. J'espère donc ne pas trop répéter ici, mais les États-Unis sont un exemple classique. Les États-Unis avaient des lois sur l'exportation de la cryptographie dans les années 1990, et ces lois d'exportation

limitaient la technologie cryptographique que les entreprises américaines pouvaient exporter. Et cela posait des problèmes pour les gens du monde entier, car s'ils recevaient de la technologie d'une entreprise américaine, ils ne recevaient que les versions plus faibles de la technologie de cryptage.

Nous n'avons plus besoin de ces mêmes contrôles des États-Unis, mais en réalité, des décennies après l'abrogation de ces réglementations, nous voyons encore ces anciens systèmes cryptographiques affaiblis déployés partout dans le monde. Il y a donc des préoccupations concernant la mise en place de réglementations qui limitent l'importation et l'exportation de la cryptographie, car même lorsque nous réalisons qu'elles ne sont pas utiles et qu'elles causent du tort à ceux qui veulent communiquer de manière sécurisée, c'est-à-dire tout le monde.

Même lorsque nous corrigeons ces problèmes et que nous disons, reprenons ces réglementations, parfois des logiciels anciens sont encore en circulation. Et pire encore, parce que certains de ces anciens logiciels existent toujours, d'autres pourraient dire que nous allons rendre nos outils compatibles avec ces systèmes plus faibles parce que nous voulons communiquer avec tout le monde. Le résultat est que vous vous retrouvez avec des systèmes qui peuvent être rétrogradés ou affaiblis par les erreurs du passé.

Je voulais donc signaler que l'une des préoccupations concernant la réglementation cryptographique est que plus vous mettez d'obstacles, plus il est difficile de créer un système cryptographique fonctionnel. Et plus nous mettons d'obstacles à en créer un qui fonctionne réellement, plus nous risquons de nous tromper, non seulement maintenant, mais aussi à l'avenir.

Nous devrions supprimer les obstacles pour permettre des communications sécurisées, si nous pensons qu'il est important que les gens puissent se parler à travers le monde.

Greg Nojeim - CDT: Dan. Super. Combien de services chiffrés existent-ils ? Parlons-nous de centaines, de milliers ? Y a-t-il un moyen de les compter ?

Daniel Kahn Gillmor - ACLU: Permettez-moi de contester un peu le cadre des services chiffrés, en fait, Greg.

Donc, quand nous parlons de plateformes chiffrées aujourd'hui, nous pensons à Internet en termes de plateformes, n'est-ce pas ? Il y a des plateformes gérées par Meta, il y a Telegram, il y a, vous savez, Signal, et nous les considérons comme ces services qui fonctionnent. Mais la cryptographie, si c'est une cryptographie forte, se fait sur votre machine.

Cela se passe sur votre appareil, que ce soit un iPhone, un ordinateur sous Debian, une machine Windows, ou autre. La cryptographie, la cryptographie de bout en bout, se fait sur le terminal que l'utilisateur contrôle. Et il est possible de superposer des protections cryptographiques solides, bien que ce soit un défi, sur un système de communication qui n'en dispose pas au départ.

Le service n'a pas besoin d'être celui qui est chiffré, cela pourrait être simplement le logiciel qui effectue le chiffrement. Donc, quand nous demandons combien de services existent, nous pourrions compter les services web, les services présents sur le réseau et voir combien il y en a. Et nous pourrions probablement arriver à un nombre, en termes de services largement utilisés, dans les dizaines.

Mais si nous parlons des éléments qui fournissent des mécanismes cryptographiques, ce sont des blocs de construction fondamentaux pour notre utilisation actuelle d'Internet, n'est-ce pas ? Un logiciel qui permet d'utiliser TLS. Que tout le monde utilise aujourd'hui pour participer à cette session, n'est-ce pas ? Cette session Zoom est protégée par, tout le monde qui s'y connecte utilise la sécurité de la couche de transport.

C'est un mécanisme de cryptage pour se connecter aux serveurs Zoom, pour obtenir le flux audio afin d'entendre ce que je dis en ce moment, et pour voir tous nos visages dans le flux vidéo. Les personnes qui construisent des kits d'outils TLS sont nombreuses. Maintenant, il n'y a pas plus d'une douzaine de kits d'outils TLS fonctionnels et largement utilisés, mais le TLS n'est pas la seule chose qui fait du cryptage.

Il existe des mécanismes de messagerie électronique chiffrée. Il y a des applications de messagerie chiffrée, n'est-ce pas ? Encore une fois, je ne considère pas Telegram comme une application de messagerie entièrement chiffrée. Elle n'est que partiellement chiffrée. Il y a une petite option pour activer le chiffrement. Ce n'est pas vraiment ce que je voudrais. Ce n'est pas le meilleur en matière de chiffrement, mais en termes de distribution d'outils qui fournissent des mécanismes de chiffrement, il y en a beaucoup et ce n'est pas parce que ces outils sont également redistribuables.

Il n'y a pas un seul distributeur, n'est-ce pas ? Le système d'exploitation Debian collecte un ensemble de paquets logiciels. Certains d'entre eux font de la cryptographie et proviennent de différents endroits. Qui est responsable de l'importation ou du transfert de ces systèmes cryptographiques ? Est-ce le contributeur français de Debian ? Je ne suis pas français, mais il y a des contributeurs français de Debian qui prennent un logiciel cryptographique de quelqu'un en Suède, par exemple, et le mettent dans l'archive Debian, qui est distribuée sur des miroirs partout dans le monde, puis il est soudainement re-téléchargé en France ?

Où cela se passe-t-il ? Et qui est responsable, qui va se faire arrêter la prochaine fois qu'ils changent d'avion à Charles de Gaulle parce qu'ils gèrent un miroir Debian ? Parce

qu'ils ont téléchargé quelque chose dans l'archive Debian alors qu'ils étaient en France, et s'ils n'étaient pas français ? Il y a tout un tas de questions que cette loi pose pour les personnes qui veulent distribuer les éléments constitutifs d'une infrastructure efficace.

L'arrestation de Durov pour ces deux chefs d'accusation en particulier soulève de grands drapeaux rouges. Devrais-je m'inquiéter en tant que développeur Debian ? Je travaille sur des logiciels cryptographiques, et j'aide à contribuer et à les empaqueter pour Debian. Je ne suis pas responsable de tout ce logiciel. Je suis au milieu entre les personnes qui y travaillent à plein temps, qui se concentrent sur ce logiciel en particulier, et les utilisateurs, qui sont beaucoup plus nombreux.

Mais devrais-je m'inquiéter la prochaine fois que je voyage en France d'avoir contribué à la distribution de logiciels libres en France qui possèdent des capacités cryptographiques ne se limitant pas à l'authentification ? Et je ne sais pas, cela soulève des questions assez préoccupantes si nous voulons un écosystème de communications cryptographiques fonctionnel, répandu et auditable.

Greg Nojeim - CDT: Nous n'avons pas les procureurs français en ligne, mais il semble que vous ayez des préoccupations et Noémie, les gens devraient-ils s'inquiéter ? Les personnes dans la position de Dan, devraient-elles vraiment s'inquiéter ? Le procureur a-t-il envoyé des signaux, pas à propos de Signal, mais sur leurs intentions avec cette loi ou cet ensemble de lois ?

Noémie Levain - la Quadrature du Net: Encore une fois, à propos des cas qui viennent d'être décrits, je pense que ce n'est pas encore le cas. Celui que le procureur recherchera, mais comme c'est légalement possible, vous ne le savez peut-être pas, mais comme je le disais avant votre arrivée, Daniel, cette loi, cette loi d'enregistrement qui a été utilisée contre Pavel Durov, c'est une vieille loi dont personne ne se souciait vraiment parce qu'elle n'était pas appliquée, et aussi parce qu'elle ne correspond pas à la manière dont le chiffrement fonctionne réellement dans le monde, car il est librement utilisé, distribué et développé, mais nous voyons qu'elle peut être utilisée comme une arme légale contre quelqu'un qui est désigné comme un ennemi de l'État. Et ici, c'était Telegram et Pavel Durov.

Donc même si c'était initialement pour la modération de contenu, nous voyons que cette vieille loi peut être utilisée comme une autre option. Donc je dirais qu'il faut toujours considérer cette loi dans le contexte politique de Telegram. Peut-être que les accusations sur ce fondement seront abandonnées, peut-être pas, et si ce n'est pas le cas, je pense que c'est la chose. Si les accusations ne sont pas abandonnées, nous devrons être très attentifs à la manière dont le juge l'appréciera car je pense que ce sera l'une des premières fois.

Donc, cela peut constituer un précédent juridique et nous aider à déterminer si quelqu'un est en danger lorsqu'il arrive en France à Charles de Gaulle. Mais encore une fois, je serais plus préoccupé par le contexte général en France concernant le

chiffrement et la tendance à criminaliser tout le monde, tous ceux qui utilisent un outil de chiffrement, plutôt que de s'inquiéter des personnes qui les développent.

En ce moment, l'attention se porte davantage sur les nombreux cas criminels où ils recherchent des personnes qui l'utilisent. Et aussi, il y a des préoccupations, j'en ai parlé très brièvement, mais il y a des cas comme ce qui s'est passé avec KICC, avec AnchorChat, et quels sont les moyens techniques de la police française en ce moment, c'est très difficile à savoir, mais il semble qu'ils soient assez puissants et c'est là que je porterai mon attention.

Daniel Kahn Gillmor - ACLU: Oui, je suis d'accord avec toi, Noémie, qu'il y a une forte préoccupation concernant les capacités techniques des agences de la loi à briser les communications cryptographiques, et pas seulement pour les Français. En tant qu'Américain, je suis également préoccupé par les capacités américaines ainsi que par celles des adversaires ou des alliés des États-Unis.

Et l'autre chose étrange est que pour une nation, pour des nations qui adhèrent au moins à l'idée de vouloir encourager les gens à communiquer librement et à avoir une libre association, ce sont des idéaux inscrits dans la Constitution américaine, que le gouvernement accumule la capacité de briser la communication des gens.

Si les outils de communication fonctionnent bien, même les fournisseurs de ces outils ne devraient pas être capables de révéler le contenu des communications. Et dans la mesure où les États-nations découvrent des vulnérabilités, des défaillances dans ces outils, ou dans les outils qui les entourent, pour pouvoir pénétrer ces communications, cela met le gouvernement en contradiction directe avec les besoins des citoyens et des personnes qui dépendent de cette infrastructure, n'est-ce pas ?

C'est comme si vous saviez, oh il y a une brique que si je retire, je peux faire tomber ce pont. Mais ne réparons pas le pont, laissons la brique là pour que, quand nous le voudrons, nous puissions retirer la brique et faire s'effondrer le pont. Mais les gens ont besoin d'utiliser le pont, et le gouvernement devrait s'assurer que l'infrastructure de la société est fonctionnelle.

pour les objectifs que nous voulons. Donc, je suis d'accord avec vous que nous avons une, c'est une préoccupation très forte concernant les capacités techniques. Je voulais cependant aborder votre point sur le fait que cette loi a été très peu appliquée auparavant. Ce genre de poursuite sélective se produit également aux États-Unis.

Et cela me dérange de voir si c'est utilisé comme une arme contre les ennemis, imaginez les accusations contre Durov concernant la modération de contenu. Imaginez que celles-ci ne tiennent pas pour une raison quelconque. Ils pourraient toujours continuer à le poursuivre de la même manière qu'aux États-Unis, nous avons poursuivi Al Capone pour évasion fiscale alors que ce que nous essayions de le poursuivre pour des accusations de gangster et de meurtre.

Je ne m'oppose pas à poursuivre les gens pour évasion fiscale. Nous devrions généralement poursuivre les gens pour évasion fiscale. Mais si vous avez une loi qui criminalise effectivement ce qui est autrement un comportement raisonnable, alors les procureurs peuvent l'utiliser à leur guise. Si tout le monde est criminalisé ou si une classe de personnes est criminalisée juste dans le but d'aider l'infrastructure mondiale à fonctionner, mais que nous allons simplement l'utiliser pour cibler des personnes spécifiques.

Cela me semble être un problème. Ce n'est pas une situation dans laquelle je voudrais que nous nous trouvions en général.

Greg Nojeim - CDT: Je vais maintenant me tourner vers certaines des questions qui apparaissent dans le chat et dans la section Q&R. Nous ne pourrons pas répondre à toutes, mais commençons. Joe Hall de l'ISOC demande : Il semble que le contrôle des exportations/importations soit vraiment une relique du passé pour la cryptographie ?

Existe-t-il une justification moderne légitime pour contrôler le chiffrement ou d'autres types de technologies améliorant la confidentialité comme la confidentialité différentielle ? Ce n'est pas contrôlé, mais s'il y a du chiffrement dans votre solution, comme le calcul multipartite sécurisé, etc., alors vous devez envoyer une note à la France et une copie de votre code source s'ils le demandent.

C'est ce que dit la loi, qu'ils peuvent aussi demander le code source. Est-ce une relique ou y a-t-il une raison moderne légitime de contrôler le chiffrement ?

Daniel Kahn Gillmor - ACLU: Je ne suis pas sûr que le terme "relique" soit celui que j'utiliserais, mais je dirais qu'il semble particulièrement irréaliste de demander des contrôles à l'exportation. Le code source est une quantité relativement petite de données. Je ne suis pas aussi préoccupé par l'idée de demander le code source. Je préfère généralement que le code source de mes systèmes de communication soit complètement ouvert, visible et modifiable d'ailleurs.

C'est en quelque sorte l'essence de la promesse du logiciel libre : les utilisateurs sont aux commandes. Mais l'idée que vous pourriez effectivement empêcher son transfert, ce sont quelques octets seulement. C'est une très petite quantité de données qui offre cette capacité. Et penser que vous pouvez réellement empêcher cela de franchir les frontières me semble invraisemblable à ce stade.

Il dit, nous sommes d'accord pour que vous fassiez des mathématiques, mais si vos mathématiques impliquent, la division longue est hors limites. Nous ne voulons pas que vous parliez de la façon de faire une division longue pour l'instant. Sans nous informer que vous le faites. Et, ce n'est tout simplement pas plausible.

La division longue découle d'autres éléments des mathématiques que vous allez faire, tout comme la cryptographie. Maintenant, je donne un certain crédit au décret français de 2007 pour avoir distingué les services cryptographiques qui ne font que l'authentification et la vérification des services qui font le chiffrement. Au moins, ils n'ont pas essayé de nous empêcher de vérifier les mises à jour logicielles sans d'abord consulter les autorités.

N'est-ce pas ? C'est bien. Ils ont au moins compris que ce n'était pas possible. Mais une fois que vous avez les outils pour faire l'authentification et la vérification cryptographiques, qui, soit dit en passant, sont nécessaires pour une cryptographie forte, vous devez savoir à qui vous parlez. Ce n'est pas un grand pas de là à ajouter une couche chiffrée.

Ces mécanismes sont utiles sous toutes ces formes. Donc, je ne vois tout simplement pas le contrôle des exportations comme quelque chose de faisable à mettre en œuvre. En particulier, si l'objectif est d'empêcher les méchants d'avoir accès à un chiffrement fort, cela ne va tout simplement pas arriver, n'est-ce pas ? Une fois que vous laissez les mécanismes cryptographiques se répandre, même en mettant de côté la partie chiffrement, vous n'allez pas empêcher les pires des pires d'utiliser les mécanismes de chiffrement.

Donc, tout ce que vous allez faire, c'est empêcher tout le monde d'utiliser les mécanismes de cryptage. Et par conséquent, qui aura la base de communication la plus faible ? Ce sera le grand public. Cela me semble contre-productif.

Greg Nojeim - CDT: Il y avait une question dans la session de questions-réponses que je veux mettre en avant.

Je ne suis pas sûr que quelqu'un ait la réponse, mais la question est : existe-t-il une liste des mauvaises lois sur le chiffrement dans le monde ? C'est-à-dire, changeons cette loi française. Mais quelle est la prochaine sur la liste qui doit être modifiée ? Je n'ai pas vu cela. Existe-t-il une telle liste ?

Noémie Levain - la Quadrature du Net: Je ne sais pas, je ne sais pas si vous parlez au niveau mondial ou en France, mais au niveau mondial, je ne sais pas. En France, je suis également ce qui se passe au niveau de l'Union européenne. Je sais aussi qu'il y a des tentatives au sein des institutions européennes pour saper le chiffrement, et cela arrive.

Mais en ce moment, s'il y a une liste de lois existantes à attaquer, je ne sais pas vraiment s'il y a d'autres cibles à repérer et à améliorer. Peut-être Daniel, ou...

Daniel Kahn Gillmor - ACLU: J'espérais m'en remettre à toi puisque tu as l'expertise juridique, Noémie.

Greg Nojeim - CDT: Cela ressemble en fait à quelque chose que nous devrions organiser au sein de la Coalition Mondiale pour le Chiffrement, si possible.

Daniel Kahn Gillmor - ACLU: Je suis d'accord.

Le défi, c'est que personne... Je n'ai pas d'expertise juridique dans le système juridique américain en tant que technologue, ce n'est pas mon domaine de compétence. Et les personnes qui ont une expertise juridique dans un système juridique n'en ont probablement pas dans les 180 autres systèmes juridiques existants.

Donc, il faudrait que ce soit un effort collaboratif et bien sûr, il y aura certains États-nations que nous ne pourrons tout simplement pas faire bouger. Mais, identifier certains des schémas communs, identifier les similitudes serait certainement utile. Et comme Noémie l'a mentionné, il y a plusieurs tentatives en cours, cela dure depuis les guerres cryptographiques des années 1990, pour ajouter ces lois, n'est-ce pas ?

Nous ne devrions pas seulement avoir une liste des mauvaises lois, mais aussi des mauvaises propositions de lois, car elles nécessitent une vigilance constante. Aux États-Unis, le discours des forces de l'ordre tourne autour de ce débat sur l'obscurcissement, et cela devient lassant. Nous avons eu ce débat pendant longtemps.

Cela ne semble pas changer grand-chose. Et, en fin de compte, les compromis sous-jacents sont de savoir si nous voulons avoir une société où les gens peuvent communiquer sans craindre l'interférence d'un tiers. Que ce tiers soit les forces de l'ordre, des adversaires criminels, de l'espionnage industriel, des amants éconduits ou autre.

Greg Nojeim - CDT: Il me semble que ce serait vraiment difficile de dresser cette liste parce qu'il y a les lois qui contrôlent explicitement le chiffrement, qui disent que vous ne pouvez pas l'exporter ou que vous devez vous enregistrer. Mais il y a aussi les lois qui font que proposer un service chiffré devient risqué.

Parce que vous ne pouvez pas modérer le contenu aussi bien quand vous ne pouvez pas le voir et beaucoup de gouvernements parlent d'imposer des devoirs de vigilance aux plateformes qui sont difficiles à assumer quand vous ne pouvez pas réellement lire le contenu. Une question posée lors de la séance de questions-réponses était : dans quelle mesure la messagerie chiffrée est-elle un signe avant-coureur ?

Un signe avant-coureur pour d'autres technologies de sécurité comme TLS. C'est le cas Durov, un conflit entre l'État et un fournisseur de logiciels à cause de ce que les gens partagent sur la plateforme. Je pense que c'est probablement juste. À quel moment ce genre de pression descend-il de la couche applicative pour contraindre le contenu, pour contraindre d'autres actions ?

Daniel Kahn Gillmor - ACLU: Je peux en parler du point de vue des protocoles cryptographiques. Nous avons certainement vu des tentatives pour que les protocoles cryptographiques de bas niveau fournissent des fonctionnalités supplémentaires à des fins d'écoute téléphonique. Et aux États-Unis, nous avons la législation CALEA. La CALEA est la loi sur l'assistance aux communications pour les forces de l'ordre.

et cela impose essentiellement d'avoir des portes dérobées dans les mécanismes de téléphonie. Ce qui n'inclut heureusement pas le TLS. Mais ces portes dérobées obligatoires ont été intégrées dans les équipements de télécommunications par les États-Unis, et ces portes dérobées dans les équipements de télécommunications ont elles-mêmes été le site de nombreuses compromissions, y compris, vous pouvez remonter à l'affaire d'Athènes en 2005, où des parties autres que les agences de maintien de l'ordre qui demandent ces fonctionnalités sont entrées et ont compromis les communications des gens.

La marge de manœuvre dont tu parles, identifier les mauvaises lois, Greg, est délicate. Je n'ai lu qu'une traduction en anglais du décret français dans ce cas, donc je ne sais pas à quel point elle est précise, peut-être que tu peux en parler, mais il semblait y avoir des exceptions concernant la déclaration jugée acceptable ou inacceptable par l'ANSI, en fonction de si elle mettait en danger les intérêts nationaux ou la sécurité nationale ou quelque chose comme ça.

Et c'est un grand... quand j'entends les mots sécurité nationale, je m'inquiète parce qu'ils sont utilisés comme un prétexte pour n'importe quel agenda que les gens poussent. Donc Noémie, je ne sais pas si tu peux parler de ces exceptions-là.

Noémie Levain - la Quadrature du Net: Je n'ai pas tout le décret en tête, mais c'est vrai que, comme vous, vous avez raison sur ce point, chaque fois qu'il y a une exemption ou un objectif de sécurité nationale, c'est un moyen d'imposer des mesures très intrusives. En France, c'est très... je ne sais pas ce qui va se passer ensuite, parce que vous voyez beaucoup d'intentions politiques de s'attaquer au chiffrement, en demandant des portes dérobées, mais aussi l'ANSI, donc c'est comme l'agence de cybersécurité, il y a une tension entre le gouvernement et l'ANSI parce que l'ANSI continue de dire que si vous affaiblissez le chiffrement pour des procédures criminelles, vous affaiblissez le chiffrement pour tout le monde et pour beaucoup d'autres couches techniques, etc.

Donc la tension, comme vous l'avez dit, dure depuis des années et des décennies, mais nous voyons, en ce moment, plus d'efforts. Et le problème avec une application de messagerie chiffrée, c'est qu'elle a cette image dans le monde médiatique et politique d'être des outils de méchants. C'est pourquoi ils s'y attaquent en premier. À ce genre d'outils en premier, chaque fois que vous lisez un article sur, je ne sais pas, des gangs, ils disent qu'ils utilisaient des applications chiffrées, même si cela n'a rien à voir avec l'affaire.

Donc, vous pouvez voir que cela s'est aggravé dans le, dans le, récit est l'imagination et c'est pourquoi nous sommes inquiets parce que si le récit passe en premier, alors il est plus facile pour le gouvernement ou le juge de dire que cela fait partie du crime, que c'est complice, etc. Donc, nous voyons qu'ils vont.

Ils l'attaquent en premier et peut-être qu'ils attaqueront d'autres types de couches après. Et j'essaie de me rappeler l'autre partie des questions mais encore une fois, ah oui, à propos de la sécurité nationale en fait, comme je l'ai dit, le décret, ce genre de vieux décret n'est pas très appliqué, donc nous n'avons pas encore beaucoup de précédents, mais et le cas Durov, ce n'est pas à propos de la sécurité nationale, mais de la criminalité générale, comment dit-on en anglais ? Mais des infractions criminelles majeures.

Mais vous parliez de l'obscurcissement et de toutes les tentatives en cours au niveau européen ou en France. C'est toujours la sécurité nationale qui est mise en avant par le gouvernement et ensuite, nous ne pouvons rien faire contre cela parce que c'est l'excuse pour toutes les exemptions et toutes les tentatives.

Et donc en ce moment, la tension dont je parlais entre l'ANSI et le gouvernement persiste, et le chiffrement est toujours préservé, mais nous ne savons pas ce qui se passera dans les prochaines années ou mois à venir.

Daniel Kahn Gillmor - ACLU: Je voulais dire, Greg, je voulais mentionner une autre chose. Et ta question concerne ces projets de loi qui pourraient rendre difficile l'atteinte de l'objectif du projet sans supprimer le chiffrement d'un service.

Et aux États-Unis, certains de ces projets de loi comportent des exceptions explicites qui disent que rien dans ce projet de loi ne doit être interprété comme vous obligeant à supprimer la communication chiffrée. Et pourtant, quand on lit le texte du projet de loi, je ne vois pas comment vous pourriez faire cela sans supprimer le chiffrement de bout en bout.

Et donc, la vraie question est de savoir comment nous... Les personnes qui rédigent les projets de loi en sont conscientes, ce qui est bien. C'est une meilleure situation que par le passé, car ils savent qu'ils ne veulent pas de ces effets secondaires négatifs. Mais je ne sais pas comment lire ces projets de loi clairement ou qui va les interpréter, quand les choses se compliquent.

Greg Nojeim - CDT: Oui, c'est un vrai problème. C'est un problème aux États-Unis, un problème en Europe, un problème partout dans le monde. Écoutez, nous arrivons à la fin et nous allons devoir conclure. Je dirai cependant que nous suivrons l'affaire Durov au sein de la Global Encryption Coalition.

S'il y a des développements significatifs, Noémie, tiens-nous au courant et nous informerons le monde entier concerné par le chiffrement. Je tiens à remercier Dan et Noémie de nous avoir rejoints aujourd'hui et merci à vous tous de vous être connectés pour écouter, et merci à l'ISOC pour avoir géré la logistique de la Coalition mondiale pour le chiffrement pour la Journée mondiale du chiffrement.

Et j'aimerais conclure en disant au revoir à tout le monde.

Noémie Levain - la Quadrature du Net: Au revoir.

Greg Nojeim - CDT: Merci à tous.