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

Encriptación, Arrestado: La detención de Pavel Durov de Telegram

Greg Nojeim - CDT: Hola a todos. Mi nombre es Greg Nojeim. Soy del Centro para la Democracia y la Tecnología. Bienvenidos a esta parte del Día Global de la Encriptación, el panel sobre "Encriptación Detenida: Las Implicaciones del Arresto de Pavel Durov de Telegram por Cargos Relacionados con la Encriptación". Como dije, soy Greg Nojeim. Soy del Centro para la Democracia y la Tecnología.

Dirijo nuestro Proyecto de Seguridad y Vigilancia. También formo parte del comité directivo de la Coalición Global de Cifrado, que patrocina este evento y el Día Global del Cifrado cada año. Perdón, el 21 de octubre de cada año, la Coalición Global de Cifrado está compuesta por 434 miembros, ubicados en más de 105 países.

El comité directivo de la Coalición Global de Cifrado está compuesto por el Centro para la Democracia y la Tecnología, mi organización, Global Partners Digital, la Fundación para la Libertad en Internet, Mozilla Corporation y la Internet Society, que ha proporcionado amablemente la logística para el Día Global del Cifrado.

El contexto de este caso es que en agosto de este año, la policía francesa arrestó al CEO de Telegram, Paval Durov, en el Aeropuerto Charles de Gaulle en Francia. Fue arrestado por la policía francesa. Es ciudadano de Francia.

Fue acusado de no cumplir con las demandas de eliminación y divulgación hechas por el gobierno de Francia, y también de no registrar un servicio encriptado y registrar la exportación de encriptación. Es importante tener en cuenta al discutir este caso que los cargos relacionados con la encriptación respecto a Telegram están un poco fuera de lugar, en el sentido de que la mayoría de las comunicaciones en Telegram no están encriptadas.

Solo las comunicaciones uno a uno están encriptadas, solo cuando una de las partes habilita la encriptación, y solo cuando ambas partes están en línea al mismo tiempo. Muchas de las comunicaciones en Telegram se realizan en canales, se transmiten a un grupo grande, o involucran chats de grupo grandes. Ninguno de esos tipos de comunicaciones está encriptado.

Así que Telegram es más una red social que una aplicación de mensajería privada. No obstante, Durov fue arrestado bajo cargos que incluyen la falta de registro de un servicio encriptado. Y tengo que decir que esto fue motivo de gran preocupación para las personas involucradas en la defensa de la encriptación, incluida nuestra organización. De hecho, puedo decir con confianza que el arresto del Sr. Durov fue el desarrollo más comentado en toda la lista de participantes de la Coalición Global de Encriptación en 2024.

Así que vamos a dar la palabra a nuestros panelistas para arrojar algo de luz sobre este caso. Primero, Noémie Levine. Es asesora de políticas para La Quadrature du Net, una organización francesa líder en la lucha por los derechos digitales. Ha estado trabajando con ellos durante varios años, especialmente en temas de vigilancia, como la limitación de las horas de los servicios de inteligencia y la documentación de prácticas policiales, como el uso de CCTV biométrico basado en algoritmos, y también en temas de encriptación.

Comenzaremos con Noémie. Noémie, ¿podrías decirnos qué leyes en Francia se acusa a Mr. Durov de violar, y por qué fue arrestado, y supongo que tan públicamente, en cierto sentido, justo en el aeropuerto de París?

Noémie Levain - la Quadrature du Net: Hola, hola a todos y gracias por la invitación y por hablar sobre este tema tan importante. Como lo describiste bien, el caso es bastante singular y complicado, y no parece ser así. Como organización francesa, fuimos los primeros en verlo de cerca.

Y podríamos, y como mencionaste, hay dos niveles en este caso. Hay uno legal y uno político. En los aspectos legales, es bastante difícil saber exactamente qué está pasando porque la única información que tenemos es la proporcionada por el fiscal público. No tienen la obligación de decir lo que está ocurriendo, pero decidieron hacerlo.

Y así es como se unen los aspectos legales y políticos, lo que significa que si Durev fue arrestado de una manera tan espectacular y con el fiscal queriendo divulgar

información sobre el caso, significa que quieren politizarlo y quieren hacerlo como una advertencia, creemos, o como un gran, quiero decir, como un evento importante y una advertencia tal vez para otros servicios de cifrado o de Internet.

Una vez dicho esto, ¿qué sabemos ahora? Sabemos que Pavel Durov ha sido arrestado por varias razones. La principal no es la encriptación, sino más bien la moderación de contenido, porque Telegram es bien conocido por no moderar suficientemente el contenido compartido, no en los mensajes privados encriptados, sino en las listas públicas.

Entonces, lo que entendemos de la información del fiscal es más que eso. Es este enfoque hacia Pavel Durov, lo que significa que está siendo procesado por complicidad en varios delitos, como pedopornografía, pornografía infantil, y diciendo que, como medio de compartir información, Pavel Durov es responsable penalmente como el CEO de Telegram.

Pero una vez que decimos eso, cuando profundizamos un poco más en la información que tenemos, vemos que puede no ser solo sobre la moderación de contenido, sino también sobre la encriptación y, en general, sobre ser un intermediario técnico. Pensamos eso porque en los varios fundamentos y esa base legal que se comunicó, vemos algunas cosas sobre, como mencionaste, el registro o la declaración de ser un servicio de encriptación, que en realidad es una ley antigua que data de principios de los 2000 y que no es realmente conocida por ser aplicada o aplicada con frecuencia.

Pero cuando ves que el juez, el fiscal, utiliza esta base legal, es porque hay algo relacionado con los mensajes privados que están encriptados. Y lo otro que tenemos en mente es que dicen que Telegram no cumplió con la obligación de divulgar información a la policía para realizar algunas interceptaciones legales.

Y generalmente, estos fundamentos son más para intervenciones telefónicas o teléfonos clásicos. Y entonces pensamos, bueno, si Telegram tiene que divulgar información para la interceptación, tal vez sean las claves de cifrado. No lo sabemos. Aún así, esto es solo del comunicado de prensa del fiscal público. Y es, nosotros, y es realmente difícil saber qué sucederá, pero vemos que es bastante complejo y detrás de la moderación de contenido, podemos creer que también podría ser una puerta abierta para luego hacer preguntas sobre cómo funciona el servicio y tal vez pedir información sobre el cifrado.

Greg Nojeim - CDT: Entonces, ¿cómo está el caso en los procedimientos legales en este momento? ¿Va a ir a juicio muy pronto o es aquí donde estamos en los procedimientos?

Noémie Levain - la Quadrature du Net: Entonces, es solo el comienzo de la investigación. Fue arrestado solo para hacerle algunas preguntas. Más adelante sabremos si el fiscal mantendrá todos los fundamentos legales que comunicó, o si tal vez dirá, de acuerdo, solo lo acusamos.

Pavel solo por tres de ellos, y dejamos caer el resto. No lo sabemos, y todavía es el comienzo, por lo que puede durar años. Y también, como mencioné antes, no hay obligación de divulgar información sobre el caso, así que dependemos de lo que diga el fiscal o, como sucede mucho en Francia, si hay algunas filtraciones a la prensa.

Así que ahora es solo una investigación para ver si Telegram tiene un papel que jugar, tuvo un papel más en todos los delitos y los fundamentos legales de los que fue acusado, como complicidad en varios crímenes o no declarar algunas herramientas de cifrado o no divulgar información para interceptaciones.

Greg Nojeim - CDT: ¿Cuál es el contexto político para la encriptación en Francia? ¿Es el gobierno favorable a la encriptación?

Noémie Levain - la Quadrature du Net: Entonces, si volvemos a los años noventa, es importante saber que Francia fue uno de los últimos países en abandonar la encriptación cuando solía ser una competencia privada del estado.

Así que solo lo liberalizó y lo hizo gratuito a finales de los 90. Y hemos estado preocupados en los últimos años porque vimos algunos intentos de controlar la encriptación y la comunicación privada en varios aspectos, tanto políticos como judiciales. Por ejemplo, el año pasado hubo un gran juicio contra activistas.

Había muchas cosas en este caso, fueron acusados de planear un ataque que no hicieron, pero entre todos los elementos se dijo que estaban usando herramientas de encriptación como Signal o Tor, o VPN, y el juez dijo que eso mostraba que querían vivir en la clandestinidad y que querían ocultar algo.

Así que estábamos como 30 años atrás en el antiguo enfoque de la encriptación, diciendo que era una herramienta criminal. Esto realmente sentó un precedente. Nos preocupaba mucho que un juez pudiera pensar que usar Signal podría hacerte parecer sospechoso. Entre otras cosas, que podría hacer que alguien pareciera un criminal.

En otras cosas, vemos un contexto político más general, donde el gobierno francés siempre dice que algunas redes sociales, o algunas comunicaciones, son parte de algún crimen. Déjame explicarme. Por ejemplo, el año pasado, hubo algunos disturbios en el país después de que un policía matara a un joven.

Y el gobierno pidió a las redes sociales que eliminaran algunos contenidos y dijo que las redes sociales tenían parte de la responsabilidad. Lo mismo ocurrió este año en Nueva Caledonia, que es un departamento francés donde hubo disturbios y el gobierno bloqueó TikTok en toda la isla.

Entonces vemos una nueva era en la que el gobierno apunta a las redes sociales, apuntando a los medios de comunicación y diciendo que son cómplices. Se puede ver la

pista de complicidad en el crimen. Y para terminar, también vemos muchos casos donde la policía, la policía francesa, ayudó. Socavando la encriptación, como AnchorChat, o SkyECC, o más recientemente, la aplicación de mensajería Ghost, donde la policía tuvo un gran papel en socavar, en encontrar una manera de eludir la encriptación.

Así que puedes ver que en este momento es un gran tema en Francia, y de hecho algunas instituciones dicen que hoy en día la encriptación es un obstáculo para ellas, y están tratando de encontrar formas de sortearla en casos criminales.

Greg Nojeim - CDT: Déjame quedarme contigo un poco más. Realmente me sorprendió que una persona pudiera ser arrestada por no registrar un servicio de encriptación, especialmente cuando la mayoría de las comunicaciones en el servicio ni siquiera están encriptadas.

Realmente fue un shock. Y creo que envía un mensaje a otros directores ejecutivos de grandes empresas de que deben preocuparse por ser arrestados cuando viajan.

¿Tienes alguna, de nuevo, surgió de la nada, ¿alguna vez has oído hablar de alguien arrestado por no registrar un servicio encriptado? ¿Alguna vez has oído hablar de otro país que requiera tal registro?

Noémie Levain - la Quadrature du Net: No, en realidad es la primera vez y por eso al principio decía que hay aspectos tanto legales como políticos vinculados, porque creemos que están utilizando esta ley antigua.

Entonces, esta obligación de registrarse surgió a principios de los 2000 con la liberalización de la encriptación. Dijeron, está bien, la encriptación es libre, pero hay algunas obligaciones para mantener un poco de control sobre ella. Pero nunca le prestamos atención porque nunca escuchamos historias al respecto. Así que cuando ves que algunos jueces, algunos fiscales, están sacando esto del fondo de las leyes, que todos olvidaron.

Estás como, bueno, tal vez quieren intentar lo que sea para llegar a Paval Durov, incluyendo los mensajes cifrados. O tal vez no saben lo que hacen, o tal vez realmente saben lo que hacen y realmente quieren llegar a la parte de cifrado, o quieren llegar a Telegram en general, porque Telegram se muestra como el enemigo, no sé si es la palabra correcta, pero por eso creemos que es muy político hacerlo público, arrestarlo así, arrestarlo con fundamentos legales muy extraños y sorprendentes, es para mostrar una señal, para advertir a otros servicios que no cumplan con la obligación legal de moderación de contenido.

Eso es lo que pensamos. Pero sigue siendo desproporcionado. Es normal que te sorprendieras, y es normal que estés preocupado, y nosotros también estamos preocupados.

Greg Nojeim - CDT: Sí, tengo que decir que fue un shock. Nuestro otro orador, Daniel Kahn Gilmore, está teniendo problemas para iniciar sesión, así que puede que tengamos que continuar con el evento, solo tú y yo, Noémie.

Continuemos la conversación. Lo que quería discutir con Dan es el hecho de que los servicios encriptados no son todos como WhatsApp. No todos son enormes. De hecho, podrías tener una conversación encriptada en un juego. Y hay personas que están desarrollando todo tipo de medios para comunicarse que incluyen encriptación, pero que no son realmente servicios grandes. Son simplemente algo que alguien creó para poder comunicarse con sus amigos y con personas afines.

Háblanos un poco, Noémie, sobre lo sorprendente que podría ser para una persona que está desarrollando un servicio de mensajería encriptada enfrentarse de repente a un requisito que no conocía para registrar su servicio con el gobierno.

Noémie Levain - la Quadrature du Net: Sí, por supuesto, estoy seguro de que mucha gente acaba de descubrir esta obligación. Y de nuevo, creo que aquí, la especificidad de esto es, nuevamente, vincularlo con el aspecto político. No soy un mago, no lo sé todo, pero no creo que el gobierno haría eso con uno pequeño, aún no, no es el primer enemigo todavía, pero sigue siendo un enemigo. Por ejemplo, descubrí que Francia era el único país con este tipo de obligación. Sabíamos que era una ley antigua, pero cuando vi que te sorprendiste, y vi a mucha gente en el mundo sorprendida con esta obligación, nos dimos cuenta de lo mal que estaba Francia con esto.

Y también, sabemos que Telegram tiene muchos problemas con muchos países. Y cuando ves que Francia es la que decidió disparar primero, sin preocuparse tanto por los derechos de encriptación y privacidad, puedes sentir que la democracia en Francia en este momento no está en su mejor etapa como lo estaba antes.

Pero, por supuesto, para los pequeños proveedores, no es una buena señal en absoluto para lo que puede venir en los próximos años, si la ley cambia o si algunos jueces deciden hacer cumplir esta ley que todos olvidaron.

Greg Nojeim - CDT: Gracias, Noémie. Pasemos a Daniel Kahn Gillmor, quien se ha unido a nuestra discusión.

Hola, Daniel. ¿Por qué no te tomas un minuto para presentarte y contarnos sobre la importancia de este caso para los tecnólogos y otras personas que trabajan con cifrado?

Daniel Kahn Gillmor - ACLU: Claro. Gracias. Y nuevamente, disculpas por la demora. Soy Daniel Kahn Gillmor.

Soy tecnólogo para la Unión Americana de Libertades Civiles. Es una ONG de EE. UU. que se enfoca en los derechos civiles y las libertades civiles, y trabajo en el proyecto de tecnología de privacidad del habla allí porque nuestra infraestructura tiene un impacto en los tipos de derechos, ya sea en preocupaciones de privacidad o censura. También soy desarrollador de software libre y contribuyo al proyecto Debian, que es una distribución fundamental de software libre de Linux.

Es un sistema operativo. Es desde donde te estoy llamando. Y tiendo a usar solo software libre, lo que explica los desafíos que tuve para conectarme aquí, porque Zoom seguía queriendo enrutarme a través de su software propietario, que preferiría no usar. Dicho esto, también estoy activo dentro del IETF. Veo a algunas personas en el chat que también están activas dentro del IETF.

La IETF es el Grupo de Trabajo de Ingeniería de Internet. Y me preocupa cómo asegurarnos de tener una infraestructura funcional para tener comunicaciones seguras y resistentes a la censura. Una de mis grandes preocupaciones, Francia no es la única nación que tiene leyes que regulan la importación o exportación de criptografía.

Y solo he logrado escuchar partes de la sesión debido a algunos problemas de conexión que estaba teniendo. Así que espero no estar repitiendo demasiado, pero Estados Unidos es un ejemplo clásico. Estados Unidos tenía leyes sobre la exportación de criptografía en la década de 1990, y esas leyes de exportación limitaban qué tecnología criptográfica podían exportar las empresas estadounidenses. Y eso en sí mismo tenía problemas para las personas de todo el mundo porque, si recibían tecnología de una empresa estadounidense, solo recibirían las versiones más débiles de la tecnología de encriptación.

Ya no requerimos esos mismos controles de los EE. UU., pero en realidad, décadas después de que esas regulaciones se eliminaron, todavía vemos estos sistemas criptográficos debilitados heredados desplegados por todo el mundo. Así que hay algunas preocupaciones sobre la creación de regulaciones que limiten la importación y exportación de criptografía porque, incluso cuando nos damos cuenta de que no son útiles y que causan daño a las personas que quieren comunicarse de manera segura, que es todo el mundo.

Incluso cuando solucionamos esos problemas y decimos, vamos a revertir esas regulaciones, a veces el software antiguo sigue existiendo. Y peor aún, debido a que parte del software antiguo sigue ahí, otras personas podrían decir que van a hacer que sus herramientas sean compatibles con los sistemas más débiles porque quieren comunicarse con todos. El resultado es que terminas con sistemas que pueden ser degradados o debilitados a los errores heredados que cometimos en el pasado.

Quería señalar que una de las preocupaciones con la regulación criptográfica es que cuantos más obstáculos pongamos, más difícil será crear un sistema criptográfico funcional. Y cuantos más obstáculos pongamos para hacer uno que realmente funcione, mayor será el riesgo de equivocarnos, no solo ahora, sino también en el futuro.

Deberíamos eliminar los obstáculos para poder tener comunicaciones seguras, si creemos que vale la pena que las personas puedan hablar entre sí en todo el mundo.

Greg Nojeim - CDT: Dan. Genial. ¿Cuántos servicios encriptados existen? ¿Estamos hablando de cientos, miles? ¿Hay alguna manera de contarlos?

Daniel Kahn Gillmor - ACLU: Permíteme cuestionar un poco el concepto de servicios encriptados, en realidad, Greg.

Entonces, cuando hablamos de plataformas encriptadas hoy en día, pensamos en Internet en términos de plataformas, ¿verdad? Hay plataformas operadas por Meta, está Telegram, está, ya sabes, Signal, y las consideramos como estos servicios que funcionan. Pero la criptografía, si es una criptografía fuerte, ocurre en tu máquina.

Ocurre en tu dispositivo, ya sea un iPhone, una computadora con Debian, una máquina con Windows, o lo que sea. La criptografía, la criptografía de extremo a extremo, ocurre en el punto final que controla el usuario. Y es posible superponer protecciones criptográficas fuertes, aunque es un desafío, sobre un sistema de comunicación que no las tiene desde el principio.

El servicio no tiene que ser lo que esté encriptado, podría ser solo el software. Eso es lo que hace la encriptación. Así que cuando decimos cuántos servicios hay, podríamos contar los servicios web, los servicios que están en la red y ver cuántos de esos hay. Y probablemente podríamos llegar a un número en términos de los más utilizados, en las docenas.

Pero si hablamos de qué piezas existen que proporcionan mecanismos criptográficos, esos son bloques fundamentales para cómo usamos Internet hoy en día, ¿verdad? Un software que proporciona la capacidad de usar TLS. Que todos están usando hoy para hablar en esta sesión, ¿verdad? Esta sesión de Zoom está cubierta con, todos los que se conectan a ella usan seguridad de la capa de transporte.

Ese es un mecanismo de encriptación para conectarse a los servidores de Zoom, obtener la transmisión de audio para escuchar lo que estoy diciendo ahora mismo y ver todas nuestras caras en la transmisión de video. Las personas que desarrollan kits de herramientas TLS están por todas partes. Ahora bien, no hay más de una docena de kits de herramientas TLS en funcionamiento y ampliamente utilizados, pero TLS no es lo único que hace encriptación.

Existen mecanismos de correo electrónico encriptado. Existen aplicaciones de mensajería encriptada, ¿verdad? Nuevamente, no considero que Telegram sea una aplicación de mensajería completamente encriptada. Solo está parcialmente encriptada. Hay una pequeña parte que puedes activar para la encriptación. No es realmente lo que yo querría. No es lo mejor en términos de encriptación, pero en cuanto a la distribución de herramientas que proporcionan mecanismos de encriptación, hay muchas de esas por ahí y no es porque esas herramientas también sean redistribuibles.

No hay un solo distribuidor, ¿verdad? Entonces, el sistema operativo Debian recopila un montón de paquetes de software. Algunos de ellos hacen criptografía y provienen de diferentes lugares. ¿Quién es responsable de la importación o transferencia de estos sistemas criptográficos? ¿Es el colaborador francés de Debian? Yo no soy francés, pero hay colaboradores franceses de Debian que toman un software criptográfico de alguien en, digamos, Suecia y lo ponen en el Archivo Debian, que se distribuye en espejos por todo el mundo, ¿y luego de repente se vuelve a descargar en Francia?

¿Dónde sucede eso? ¿Y quién es responsable, quién va a ser detenido la próxima vez que cambie de avión en Charles de Gaulle porque opera un espejo de Debian? Porque subieron algo al Archivo de Debian mientras estaban en Francia, ¿qué pasa si no eran franceses? Hay un montón de preguntas que esta ley plantea para las personas que quieren distribuir los componentes básicos de una infraestructura efectiva.

El arresto de Durov por esos dos cargos en particular levanta grandes banderas de advertencia. ¿Debería preocuparme como desarrollador de Debian? Trabajo en software criptográfico y ayudo a contribuir y empaquetar eso para Debian. No soy responsable de todo ese software. Estoy en el medio entre las personas que trabajan en ello a tiempo completo, enfocadas en ese software en particular, y las personas que lo usan, que son muchas más.

¿Pero debería preocuparme la próxima vez que viaje a Francia por haber ayudado a distribuir software libre en Francia que tiene capacidades criptográficas que no se limitan a la autenticación? Y no sé, esto plantea preguntas bastante inquietantes si queremos un ecosistema de comunicaciones criptográficas funcional, extendido y auditable.

Greg Nojeim - CDT: No tenemos a los fiscales franceses en la llamada, pero parece que tienes algunas preocupaciones y Noémie, ¿deberían las personas estar preocupadas? Las personas en la posición de Dan, ¿deberían realmente estar preocupadas? ¿Ha enviado el fiscal alguna señal, no sobre Signal, sino sobre cuál es su intención con esta ley o este conjunto de leyes?

Noémie Levain - la Quadrature du Net: De nuevo, sobre los casos que se acaban de describir, creo que aún no. El que el fiscal buscará, pero aún así, como es legalmente posible, puede que no lo sepas, pero como decía antes de que llegaras, Daniel, que la

ley, esta ley de registro, la que se usó contra Pavel Durov, es una ley antigua de la que nadie realmente se preocupaba porque no se aplicaba, y también porque no se ajusta a cómo funciona realmente la encriptación en el mundo, ya que se usa, distribuye y desarrolla libremente, pero vemos que puede ser utilizada como un arma legal contra alguien que está designado como enemigo del estado. Y aquí fue Telegram y Pavel Durov.

Entonces, aunque inicialmente era para la moderación de contenido, vemos que esta vieja ley puede ser utilizada como otra opción. Así que diría que aún tienes que considerar esta ley en el contexto político de Telegram. Tal vez los cargos en este sentido sean retirados, tal vez no, y si no, creo que esto es lo importante. Si los cargos no son retirados, tendremos que ser muy cuidadosos con cómo el juez lo valorará porque creo que será una de las primeras veces.

Entonces puede ser un precedente legal y luego ayudarnos a considerar si alguien está en peligro cuando llega a Francia en Charles de Gaulle. Pero nuevamente, necesitamos estar más preocupados por el contexto general en Francia sobre la encriptación y sobre criminalizar a todos, todos los que usan una herramienta de encriptación, en lugar de preocuparnos por las personas que las desarrollan.

En este momento, la atención se centra más en los casos criminales, están buscando a personas que lo usan. Y también preocupa, lo mencioné muy brevemente, pero hay casos de lo que sucedió con KICC, con AnchorChat, y cuáles son los medios técnicos de la policía francesa en este momento, es muy difícil de saber, pero parece que son bastante fuertes y ese sería mi punto de atención.

Daniel Kahn Gillmor - ACLU: Sí, estoy de acuerdo contigo, Noémie, en que hay una gran preocupación sobre cuáles son las capacidades técnicas para romper la comunicación criptográfica por parte de las agencias de aplicación de la ley y no solo para los franceses. Como estadounidense, me preocupa las capacidades estadounidenses, así como las capacidades de los adversarios o aliados de Estados Unidos.

Y lo otro extraño es que para una nación, para naciones que se adhieren al menos a la idea de querer fomentar que las personas se comuniquen libremente y tengan libre asociación, estos son ideales consagrados en la Constitución estadounidense, que el gobierno acumule la capacidad de romper la comunicación de las personas.

Si las herramientas de comunicación funcionan bien, ni siquiera los proveedores de esas herramientas deberían poder revelar el contenido de la comunicación. Y en la medida en que los estados nacionales descubren vulnerabilidades, fallos en esas herramientas o en las herramientas que las rodean, para poder infiltrarse en esa comunicación, eso pone al gobierno en conflicto directo con las necesidades de la ciudadanía y las personas que dependen de esa infraestructura, ¿verdad?

Es como si supieras, oh, hay un ladrillo que si lo saco, puedo derribar este puente. Pero no arreglemos el puente, dejemos el ladrillo ahí para que cuando queramos, podamos sacar el ladrillo y hacer que el puente colapse. Pero la gente necesita usar el puente, y el gobierno debería estar en el negocio de asegurarse de que la infraestructura de la sociedad funcione.

para los objetivos que queremos. Así que estoy de acuerdo contigo en que tenemos una preocupación muy fuerte sobre cuáles son las capacidades técnicas. Sin embargo, quería abordar tu punto sobre si, el hecho de que esta ley ha sido aplicada de manera muy mínima anteriormente. Ese tipo de enjuiciamiento selectivo también ocurre en los Estados Unidos.

Y me preocupa ver si se usa como un arma contra los enemigos, imagina los cargos contra Durov relacionados con la moderación de contenido. Imagina que esos cargos no prosperan por cualquier razón. Aún podrían seguir procesándolo de la misma manera que en los EE. UU. fuimos tras Al Capone por evasión de impuestos cuando lo que realmente queríamos era acusarlo de ser un mafioso y de matar gente.

No me opongo a perseguir a las personas por evasión de impuestos. Deberíamos perseguir a las personas por evasión de impuestos en general. Pero si tienes una ley que efectivamente criminaliza lo que de otro modo sería una conducta razonable, entonces los fiscales pueden, y los fiscales pueden usarla a su antojo si todos están siendo criminalizados o si una clase de personas está siendo criminalizada solo con el propósito de intentar ayudar a que la infraestructura global funcione, pero solo vamos a usarla para seleccionar a personas específicas.

Eso me parece un problema. No es una situación en la que quisiera que estuviéramos en general.

Greg Nojeim - CDT: Voy a pasar ahora a algunas de las preguntas que están apareciendo en el chat y en la sección de preguntas y respuestas. No podemos responder a todas, pero déjame empezar. Joe Hall de ISOC pregunta: ¿Parece que el control de exportación/importación es realmente una reliquia del pasado para la criptografía?

¿Existe una justificación moderna legítima para controlar la encriptación u otros tipos de tecnología que mejoran la privacidad, como la privacidad diferencial? No está controlado, pero si hay encriptación en tu solución, como el cálculo seguro de múltiples partes, etc., entonces tienes que enviar una nota a Francia y una copia de tu código fuente si te lo piden.

Eso es lo que dice la ley, que también pueden pedir el código fuente. ¿Es un vestigio del pasado o hay una justificación moderna legítima para controlar la encriptación?

Daniel Kahn Gillmor - ACLU: No estoy seguro de si reliquia es el término que usaría, pero diría que parece singularmente inviable pedir controles de exportación. El código fuente es una cantidad relativamente pequeña de datos. No me preocupa tanto la idea de solicitar el código fuente. Tiendo a preferir que el código fuente de mis sistemas de comunicación sea completamente abierto, visible y modificable, en ese caso.

Esa es la esencia de la promesa del software libre: que los usuarios tienen el control. Pero la idea de que efectivamente se podría prevenir su transferencia, estamos hablando de un número muy pequeño de bytes. Es una cantidad muy pequeña de datos que proporciona esta capacidad. Y pensar que realmente se puede evitar que cruce fronteras en este punto me parece implausible.

Está diciendo, estamos bien con que hagas matemáticas, pero si tus matemáticas implican, la división larga está fuera de los límites. No queremos que hables sobre cómo hacer la división larga todavía. Sin informarnos que lo estás haciendo. Y eso simplemente no es plausible.

La división larga se deriva de otras partes de las matemáticas que vas a hacer, al igual que la criptografía. Ahora, le doy algo de crédito al decreto francés de 2007 por separar los servicios criptográficos que solo hacen autenticación y verificación de los servicios que hacen cifrado. Al menos no intentaron bloquearnos de verificar actualizaciones de software sin primero consultar con las autoridades.

¿Verdad? Eso es bueno. Al menos vieron que no se podía hacer eso. Pero una vez que tienes las herramientas para hacer autenticación y verificación criptográfica, que, por cierto, son necesarias para hacer criptografía fuerte, necesitas saber con quién estás hablando. No es un gran salto pasar de ahí a añadir una capa cifrada.

Estos mecanismos son útiles en todas estas formas. Así que, simplemente, no veo que el control de exportación sea algo factible de operar. En particular, si el objetivo es mantener la encriptación fuerte fuera del alcance de los malos, eso simplemente no va a suceder, ¿verdad? Una vez que permites que los mecanismos criptográficos en general se difundan, incluso dejando de lado la parte de encriptación, no vas a impedir que los peores de los peores usen los mecanismos de encriptación.

Entonces, lo único que vas a lograr es impedir que todos los demás usen los mecanismos de encriptación. Y como resultado, ¿quién tendrá la base de comunicaciones más débil? Será el público en general. Eso me parece contraproducente.

Greg Nojeim - CDT: Entonces, hubo una pregunta en la sesión de preguntas y respuestas que quiero destacar.

No estoy seguro si alguien tiene la respuesta, pero la pregunta es: ¿existe una lista de leyes de cifrado deficientes a nivel global? Es decir, cambiemos esta ley francesa. Pero, ¿qué sigue en la lista que necesita ser cambiado? No he visto eso. ¿Existe tal lista?

Noémie Levain - la Quadrature du Net: No sé, no sé si te refieres a nivel global o en Francia, pero a nivel global, no lo sé. En Francia, también sigo lo que está ocurriendo a nivel de la Unión Europea. También sé que hay algunos intentos en las instituciones europeas para socavar la encriptación que están por venir.

Pero en este momento, si hay una lista de leyes existentes para revisar, en realidad no sé si hay otros objetivos que identificar y mejorar. Tal vez Daniel, algunos o...

Daniel Kahn Gillmor - ACLU: Esperaba poder deferir a ti, ya que tienes la experiencia legal, Noémie.

Greg Nojeim - CDT: Esto en realidad suena como algo que deberíamos organizar en la Coalición Global de Cifrado, si podemos.

Daniel Kahn Gillmor - ACLU: Estoy de acuerdo.

El desafío es que nadie... Yo no tengo experiencia legal en el sistema legal de EE. UU. como tecnólogo, esa no es mi área de especialización. Y las personas que sí tienen experiencia legal en un sistema legal probablemente no la tengan en los otros 180 sistemas legales que existen.

Entonces, sería necesario un esfuerzo colaborativo y, por supuesto, habrá algunos estados nacionales que simplemente no podremos mover. Pero, identificar algunos de los patrones comunes, identificar las similitudes ciertamente sería útil. Y como mencionó Noémie, hay múltiples intentos pendientes, esto ha estado ocurriendo desde las guerras criptográficas de los años 90, para agregar estas leyes, ¿verdad?

Entonces, no solo deberíamos tener una lista de malas leyes, sino también de malas propuestas de leyes, porque esas necesitan ser rechazadas continuamente. Dentro de los EE. UU., el lenguaje que proviene de las fuerzas del orden es este tipo de debate sobre "quedarse a oscuras", y se vuelve agotador. Hemos tenido este debate durante mucho tiempo.

No parece cambiar mucho. Y, en última instancia, las concesiones subyacentes son si queremos tener una sociedad donde las personas puedan comunicarse sin preocuparse por la interferencia de un tercero. Ya sea que ese tercero sea la policía, adversarios criminales, espionaje industrial o amantes despechados, o lo que sea.

Greg Nojeim - CDT: Me parece que sería realmente difícil elaborar esta lista porque existen leyes que controlan explícitamente la encriptación, que dicen que no puedes

exportarla o que debes registrarla. Pero también hay leyes que hacen que ofrecer un servicio encriptado se vuelva arriesgado.

Porque no puedes moderar el contenido tan bien cuando no puedes verlo y muchos gobiernos están hablando de imponer deberes de cuidado en las plataformas que son difíciles de asumir cuando no puedes leer el contenido. Una pregunta hecha en la sesión de preguntas y respuestas fue, ¿hasta qué punto es la mensajería encriptada un canario en la mina de carbón?

Una especie de señal de advertencia temprana para otras tecnologías de seguridad como TLS. Ese es el caso de Durov, es una disputa entre el estado y un proveedor de software debido a lo que la gente está compartiendo en la plataforma. Creo que eso es probablemente correcto. ¿En qué momento este tipo de presión? baja desde la capa de aplicación para coaccionar contenido, para coaccionar otras acciones.

Daniel Kahn Gillmor - ACLU: Puedo hablar de eso desde la perspectiva de los protocolos criptográficos. Así que definitivamente hemos visto intentos de hacer que los protocolos criptográficos de nivel inferior proporcionen características adicionales con el propósito de realizar escuchas telefónicas. Y en los EE. UU. tenemos la legislación CALEA. La CALEA es la Ley de Asistencia en las Comunicaciones para la Aplicación de la Ley.

y básicamente exige que haya puertas traseras en los mecanismos de telefonía. Afortunadamente, esto no incluye TLS. Pero esas puertas traseras obligatorias han sido impuestas en equipos de telecomunicaciones por los EE. UU., y esas puertas traseras en los equipos de telecomunicaciones han sido en sí mismas sitios de numerosos compromisos, incluyendo, puedes remontarte al caso de Atenas en 2005, donde partes distintas a las agencias de aplicación de la ley que solicitan estas características han entrado y comprometido las comunicaciones de las personas.

El margen de maniobra del que hablas, identificar leyes malas, Greg, es complicado. Solo he leído una traducción al inglés del decreto francés en este caso, así que no sé cuán precisa es, tal vez, sabiendo que puedes hablar de eso, pero parecía tener algunas excepciones sobre la declaración siendo marcada como aceptable o inaceptable por ANSI, en base a si ponía en riesgo los intereses nacionales o la seguridad nacional o algo así.

Y eso es un gran... cuando escucho las palabras seguridad nacional, me preocupo porque se usan como un pretexto para cualquier agenda que la gente esté impulsando. Así que Noémie, no sé si puedes hablar sobre esas excepciones.

Noémie Levain - la Quadrature du Net: No tengo todo el decreto en mente, pero es cierto que, como tú, tienes razón en el lugar, cada vez que hay una exención o un objetivo de seguridad nacional, es una forma de imponer algunas medidas muy intrusivas. Pero en Francia, no sé qué pasará después, porque ves mucha intención

política de intentar la encriptación, pidiendo puertas traseras, pero también la ANSI, así que es como la agencia de ciberseguridad, hay tensión entre el gobierno y la ANSI porque la ANSI seguirá diciendo que si socavas la encriptación para procedimientos criminales, socavas la encriptación para todos y para muchas otras capas técnicas, etcétera.

Entonces, la tensión, como dijiste, ha estado ocurriendo durante años y décadas, pero vemos, en este momento, más esfuerzos. Y el problema con una aplicación de mensajería encriptada es que tienen esta imagen en el mundo mediático y político de ser herramientas de los malos. Por eso van a ellas primero. A este tipo de herramientas primero cada vez que lees un artículo sobre, no sé, algunas pandillas, dicen que estaban usando aplicaciones encriptadas, incluso si no tiene nada que ver con el asunto.

Entonces puedes ver que empeoró en la, en la, narrativa es la imaginación y por eso estamos preocupados porque si la narrativa sigue primero, entonces es más fácil para el gobierno o el juez decir que es parte del crimen, que es cómplice, etc. Así que vemos que van a.

Primero lo atacan y tal vez ataquen otros tipos de capas después. Y estoy tratando de recordar la otra parte de las preguntas, pero de nuevo, ah sí, sobre la seguridad nacional, en realidad, como dije, el decreto, este tipo de decreto antiguo no se aplica mucho, así que no tenemos muchos precedentes todavía, pero en el caso de Durov, no se trata de seguridad nacional, sino de delitos penales generales, ¿cómo se dice en inglés? Pero delitos penales mayores.

Pero estabas hablando sobre el "going dark" y todos los intentos que se están llevando a cabo a nivel europeo o en Francia. Siempre es la seguridad nacional la que, la que, la que se pone en primer lugar por parte del gobierno y luego no podemos hacer nada al respecto porque es la excusa para todas las excepciones y todos los intentos.

Entonces, en este momento, la tensión de la que hablaba entre el ANSI y el gobierno se mantiene, y la encriptación sigue preservada, pero no sabemos qué pasará en los próximos años o meses.

Daniel Kahn Gillmor - ACLU: Quiero decir, Greg, quería mencionar otra cosa. Y tu pregunta es sobre estos proyectos de ley que se están proponiendo y que podrían hacer difícil cumplir con el objetivo del proyecto sin eliminar la encriptación de un servicio.

Y en los EE. UU., algunos de esos proyectos de ley tienen excepciones explícitas que dicen que nada en este proyecto de ley debe interpretarse como una obligación de eliminar la comunicación encriptada. Y sin embargo, cuando lees el lenguaje claro del proyecto de ley, no sé cómo lo harías sin eliminar la encriptación de extremo a extremo.

Entonces, realmente es una cuestión de, ¿cómo hacemos...? Las personas que redactan los proyectos de ley están al tanto, lo cual es bueno. Es una situación mejor que en el pasado, ya que son conscientes de que no quieren estos efectos secundarios negativos. Pero no sé cómo leer claramente los proyectos de ley o quién los interpretará cuando llegue el momento decisivo.

Greg Nojeim - CDT: Sí, es un verdadero problema. Es un problema en los EE. UU., un problema en Europa, un problema en todo el mundo. Escuchen, se nos ha acabado el tiempo y tenemos que terminar. Sin embargo, diré esto: estaremos siguiendo el caso Durov en la Coalición Global de Cifrado.

Si hay desarrollos significativos, Noémie, mantennos informados y nosotros mantendremos al mundo entero al tanto sobre la encriptación. Quiero agradecer a Dan y Noémie por acompañarnos hoy y gracias a todos por conectarse para escuchar, y gracias a ISOC por encargarse de la logística para la Coalición Global de Encriptación en el Día Global de la Encriptación.

Y me gustaría despedirme y decir adiós a todos.

Noémie Levain - la Quadrature du Net: Adiós.

Greg Nojeim - CDT: Gracias a todos.