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

Criptografia, Detido: A Prisão de Pavel Durov do Telegram

Greg Nojeim - CDT: Olá a todos. Meu nome é Greg Nojeim. Eu trabalho no Centro para Democracia e Tecnologia. Bem-vindos a esta parte do Dia Global da Criptografia, o painel sobre Criptografia Detida: As Implicações da Prisão de Pavel Durov do Telegram por Acusações Relacionadas à Criptografia. Como eu disse, sou Greg Nojeim, do Centro para Democracia e Tecnologia.

Eu dirijo nosso Projeto de Segurança e Vigilância. Também faço parte do comitê diretor da Coalizão Global de Criptografia, que está patrocinando este evento e o Dia Global da Criptografia todos os anos. Desculpe, no dia 21 de outubro de cada ano, a Coalizão Global de Criptografia é composta por 434 membros, localizados em mais de 105 países.

O comitê diretor da Global Encryption Coalition é composto pelo Center for Democracy and Technology, minha organização, Global Partners Digital, a Internet Freedom Foundation, a Mozilla Corporation e a Internet Society, que gentilmente forneceu a logística para o Dia da Criptografia Global.

O contexto deste caso é que, em agosto deste ano, a polícia francesa prendeu o CEO do Telegram, Paval Durov, no Aeroporto Charles de Gaulle, na França. Ele foi preso pela polícia francesa. Ele é cidadão francês.

Ele foi acusado de não cumprir as exigências de remoção e divulgação feitas pelo governo da França, e também de não registrar um serviço criptografado e registrar a exportação de criptografia. É importante lembrar, ao discutirmos este caso, que as acusações relacionadas à criptografia no Telegram são um pouco fora de contexto, no sentido de que a maioria das comunicações no Telegram não são criptografadas.

Apenas as comunicações um a um são criptografadas, somente quando uma das partes ativa a criptografia, e apenas quando ambas as partes estão online ao mesmo tempo. Muitas comunicações no Telegram ocorrem em canais, são transmitidas para um grande grupo, ou envolvem chats em grupo. Nenhum desses tipos de comunicação é criptografado.

Então, o Telegram é mais uma rede social do que um aplicativo de mensagens privadas. No entanto, Durov foi preso sob acusações que incluem a falha em registrar um serviço criptografado. E devo dizer que isso foi motivo de grande preocupação para as pessoas envolvidas na defesa da criptografia, incluindo nossa organização. Na verdade, posso dizer com confiança que a prisão do Sr. Durov foi o desenvolvimento mais comentado em 2024 na lista de participantes da Coalizão Global de Criptografia.

Então, vamos agora aos nossos painelistas para esclarecer este caso. Primeiro, Noémie Levine, que é consultora de políticas da La Quadrature du Net, uma organização francesa líder na luta pelos direitos digitais. Ela trabalha com eles há vários anos, especialmente em tópicos de vigilância, como a limitação das horas dos serviços de inteligência e a documentação das práticas policiais, como o uso de CFTV biométrico baseado em algoritmos, e também sobre criptografia.

Vamos começar com Noémie. Noémie, você poderia nos dizer quais leis na França o Sr. Durov é acusado de violar, e por que ele foi preso, e acho que tão publicamente, de certa forma, bem no aeroporto de Paris?

Noémie Levain - la Quadrature du Net: Oi, olá a todos e obrigado pelo convite para falar sobre este assunto tão importante. Como você descreveu bem, o caso é bastante singular e complicado, e não parece ser assim. Como uma organização francesa, estávamos na linha de frente para ver isso.

E como você mencionou, há dois níveis neste caso. Há um nível legal e um nível político. Nos aspectos legais, é bastante difícil saber exatamente o que está acontecendo porque a única informação que temos é a fornecida pelo promotor público. Eles não têm a obrigação de dizer o que está acontecendo, mas decidiram fazê-lo.

E é assim que o aspecto legal e político se unem, significando que se Durev foi preso de maneira tão espetacular e com o promotor público querendo divulgar informações sobre o caso, isso significa que eles querem politizá-lo e fazer disso um aviso, pensamos, ou um grande, quero dizer, um evento importante e talvez um aviso para outros serviços de criptografia ou da Internet.

Uma vez dito isso, o que sabemos agora? Sabemos que Pavel Durov foi preso por várias razões. A principal não é a criptografia, mas sim a moderação de conteúdo, porque o Telegram é bem conhecido por não moderar o conteúdo o suficiente, não nas mensagens privadas criptografadas, mas nas listas públicas.

Então, o que entendemos das informações do promotor público é mais do que isso. É esta abordagem a Pavel Durov, significando que ele está sendo processado por cumplicidade em vários delitos, como pedopornografia, pornografia infantil, e dizendo que, como um meio de compartilhamento de informações, Pavel Durov é criminalmente responsável como CEO do Telegram.

Mas uma vez que dizemos isso, quando investigamos um pouco mais as informações que temos, vemos que pode não ser apenas sobre moderação de conteúdo, mas também sobre criptografia e, de forma mais geral, sobre ser um intermediário técnico. Pensamos isso porque, nos vários fundamentos e na base legal que foi comunicada, vemos algumas coisas sobre, como você mencionou, registro ou declaração de ser um serviço de criptografia, que na verdade é uma lei antiga que remonta ao início dos anos 2000 e que não é realmente conhecida por ser aplicada ou frequentemente aplicada.

Mas quando você vê que o juiz, o promotor, usa essa base legal, é porque há algo relacionado às mensagens privadas estarem criptografadas. E a outra coisa que temos em mente é que eles dizem que o Telegram não cumpriu a obrigação de divulgar informações à polícia para realizar algumas interceptações legais.

E geralmente essa base é mais para escutas telefônicas ou telefones clássicos. E então pensamos, ok, se o Telegram tem que divulgar informações para interceptação, talvez sejam as chaves de criptografia. Não sabemos. Ainda assim, isso é apenas do comunicado de imprensa do promotor público. E é, e é realmente difícil saber o que vai acontecer, mas vemos que é bastante complexo e, por trás da moderação de conteúdo, podemos acreditar que isso também pode ser uma porta aberta para então fazer perguntas sobre como o serviço funciona e talvez pedir informações sobre criptografia.

Greg Nojeim - CDT: Então, como está o caso nos procedimentos legais agora? Ele vai a julgamento em breve ou é aqui que estamos nos procedimentos?

Noémie Levain - la Quadrature du Net: Então, é apenas o início da investigação. Ele foi preso apenas para responder a algumas perguntas. Saberemos mais adiante se o promotor público manterá todas as bases legais que comunicou, ou se talvez ele dirá, ok, vamos processar apenas.

Pavel apenas para três deles, e deixamos o resto. Não sabemos disso, e ainda é o começo, então pode durar anos. E também, como mencionei antes, não há obrigação de divulgar informações sobre o caso, então estamos meio que dependentes do que o promotor público dirá ou, como acontece muito na França, se houver alguns vazamentos para a imprensa.

Então agora é apenas uma investigação para ver se o Telegram tem um papel a desempenhar, teve um papel mais ativo em todas as ofensas e as bases legais das quais ele foi acusado, como cumplicidade em vários crimes ou não declarar algumas ferramentas de criptografia ou não divulgar informações para interceptações.

Greg Nojeim - CDT: Então, qual é o contexto político para a criptografia na França? O governo é favorável à criptografia?

Noémie Levain - la Quadrature du Net: Então, se voltarmos aos anos 90, é importante saber que a França foi um dos últimos países a liberar a criptografia, que costumava ser uma competência exclusiva do estado.

Então, só foi liberalizado e tornou-se gratuito no final dos anos 90. E temos nos preocupado nos últimos anos porque vimos algumas tentativas de restringir a criptografia e a comunicação privada em vários aspectos, tanto políticos quanto judiciais. Por exemplo, no ano passado houve um grande julgamento contra ativistas.

Havia muitas coisas nesse caso, eles foram processados por planejar um ataque que não cometeram, mas entre todos os elementos foi dito que estavam usando ferramentas de criptografia como Signal ou Tor, ou VPN, e o juiz disse que isso mostrava que queriam viver na clandestinidade e que queriam esconder algo.

Então, era como se estivéssemos 30 anos atrás na abordagem antiga da criptografia, dizendo que era uma ferramenta criminosa. Isso foi realmente um precedente. Estávamos realmente preocupados com o fato de que um juiz pudesse pensar que usar o Signal poderia ser uma pista. Entre outras coisas, que isso poderia fazer de alguém um criminoso.

Em outras questões, vemos um contexto político mais geral, onde o governo francês sempre diz que algumas redes sociais, ou algumas comunicações, fazem parte de algum crime. Deixe-me explicar. Por exemplo, no ano passado, houve alguns tumultos no país após um policial matar um jovem.

E o governo pediu às redes sociais para removerem alguns conteúdos e disse que as redes sociais tinham parte da responsabilidade. A mesma coisa aconteceu este ano na Nova Caledônia, que é um departamento francês onde houve alguns distúrbios e o governo bloqueou o TikTok em toda a ilha.

Então vemos uma nova era em que o governo está mirando nas redes sociais, mirando nos meios de comunicação, dizendo que são cúmplices. Você pode ver a pista de cumplicidade no crime. E só para finalizar, vemos também muitos casos em que a polícia, a polícia francesa, ajudou. Minando a criptografia, como no caso do AnchorChat, ou SkyECC, ou mais recentemente, o aplicativo Ghost Messaging, onde a polícia teve um grande papel em minar, em encontrar uma maneira de contornar a criptografia.

Então, você pode ver que, neste momento, isso é um grande problema na França, e, na verdade, algumas instituições dizem que hoje a criptografia é um obstáculo para elas, e estão tentando encontrar maneiras de contorná-la em casos criminais.

Greg Nojeim - CDT: Deixe-me ficar com você por mais um pouco. Realmente me surpreendeu que uma pessoa pudesse ser presa por não registrar um serviço de criptografia, especialmente quando a maior parte da comunicação no serviço nem é criptografada.

Foi realmente um choque. E acho que isso envia uma mensagem aos outros CEOs de grandes empresas de que eles precisam se preocupar com a possibilidade de serem presos quando viajam.

Você já ouviu falar de alguém sendo preso por não registrar um serviço criptografado? Já ouviu falar de outro país que exige tal registro?

Noémie Levain - la Quadrature du Net: Não, na verdade é a primeira vez e é por isso que no início eu estava dizendo que há aspectos legais e políticos interligados, porque achamos que eles estão usando essa lei antiga.

Então, essa obrigação de registro surgiu no início dos anos 2000 com a liberalização da criptografia. Eles disseram: "Ok, a criptografia é livre, mas há algumas obrigações para manter um pouco de controle sobre ela." Mas nunca prestamos atenção a isso porque nunca ouvimos histórias a respeito. Então, quando você vê que alguns juízes, alguns promotores, estão resgatando isso do fundo das leis, que todo mundo esqueceu.

Você pensa, ok, talvez eles queiram tentar de tudo para chegar a Paval Durov, incluindo mensagens criptografadas. Ou talvez eles não saibam o que estão fazendo, ou talvez realmente saibam o que estão fazendo e queiram mesmo chegar à parte da criptografia, ou queiram atingir o Telegram em geral, porque o Telegram é visto como o inimigo, não sei se é a palavra certa, mas é por isso que achamos que é muito político tornar isso público, prendê-lo assim, prendê-lo com bases legais muito estranhas e surpreendentes, para mostrar um sinal, para dar um aviso a outros serviços que não cumpram a obrigação legal de moderação de conteúdo.

É isso que pensamos. Mas ainda é desproporcional. É normal que você tenha ficado surpreso, e é normal que você esteja preocupado, e nós também estamos preocupados.

Greg Nojeim - CDT: Sim, tenho que dizer que foi um choque. Nosso outro palestrante, Daniel Kahn Gilmore, está tendo problemas para entrar, então talvez tenhamos que continuar com o evento, só você e eu, Noémie.

Vamos continuar a conversa. O que eu queria discutir com o Dan é o fato de que os serviços criptografados não são todos como o WhatsApp. Eles não são todos enormes. Na verdade, você pode ter uma conversa criptografada em um jogo. E há pessoas desenvolvendo todos os tipos de meios de comunicação que incluem criptografia, mas que não são realmente grandes serviços. São apenas algo que alguém criou para poder se comunicar com seus amigos e com pessoas de ideias semelhantes.

Fale um pouco, Noémie, sobre como pode ser surpreendente para uma pessoa que está desenvolvendo um serviço de mensagens criptografadas de repente enfrentar uma exigência que ela não poderia saber, de registrar seu serviço com o governo.

Noémie Levain - la Quadrature du Net: Sim, claro, tenho certeza de que muitas pessoas acabaram de descobrir essa obrigação. E, novamente, acho que aqui, a especificidade disso é, mais uma vez, ligá-la ao aspecto político. Não sou mágico, não sei de tudo, mas não acho que o governo faria isso com uma pequena empresa, ainda não, não é o primeiro inimigo ainda, mas ainda assim, inimigo. Por exemplo, descobri que a França era o único país a ter esse tipo de obrigação. Sabíamos que era uma lei antiga, mas quando vi você chocado, e vi muitas pessoas no mundo chocadas com essa obrigação, percebemos o quão ruim a França estava com isso.

E também, sabemos que o Telegram tem muitos problemas com vários países. E quando você vê que a França foi a primeira a atacar, sem se importar muito com os direitos de criptografia e privacidade, você pode sentir que a democracia na França agora não está no seu melhor estágio como antes.

Mas é claro, para pequenos provedores, isso não é um bom sinal de forma alguma para o que pode vir nos próximos anos, se a lei mudar ou se alguns juízes decidirem aplicar essa lei que todos esqueceram.

Greg Nojeim - CDT: Obrigado, Noémie. Vamos falar com Daniel Kahn Gillmor, que se juntou à nossa discussão.

Oi, Daniel. Por que você não se apresenta e nos conta sobre a importância deste caso para os tecnólogos e outras pessoas que trabalham com criptografia?

Daniel Kahn Gillmor - ACLU: Claro. Obrigado. E novamente, peço desculpas pelo atraso. Sou Daniel Kahn Gillmor.

Sou tecnólogo da União Americana pelas Liberdades Civis. É uma ONG dos EUA que se concentra em direitos civis e liberdades civis, e eu trabalho no projeto de tecnologia de privacidade de discurso lá porque nossa infraestrutura tem um impacto nos tipos de direitos, seja em questões de privacidade ou censura. Também sou desenvolvedor de software livre e contribuo para o projeto Debian, que é uma distribuição fundamental de software livre Linux.

É um sistema operacional. É de onde estou ligando para você. E eu costumo usar apenas software livre, o que explica os desafios que tive para me conectar aqui, porque o Zoom insistia em me direcionar para o software proprietário deles, que eu preferiria não usar. Dito isso, também sou ativo no IETF. Vejo algumas pessoas no chat que também são ativas no IETF.

A IETF é a Força-Tarefa de Engenharia da Internet. E estou preocupado com a forma como garantimos que temos uma infraestrutura funcional para comunicações seguras e resistentes à censura. Uma das minhas grandes preocupações, então, a França não é a única nação a ter leis que regulam a importação ou exportação de criptografia.

E só consegui ouvir partes da sessão devido a alguns desafios de conexão que estava enfrentando. Então, espero não estar repetindo muito o que já foi dito, mas os EUA são um exemplo clássico. Os EUA tinham leis sobre a exportação de criptografia na década de 1990, e essas leis de exportação restringiam a tecnologia criptográfica que as empresas americanas podiam exportar. E isso, por si só, causava problemas para pessoas ao redor do mundo, porque se recebessem tecnologia de uma empresa americana, receberiam apenas as versões mais fracas da tecnologia de criptografia.

Não precisamos mais desses mesmos controles dos EUA, mas ainda vemos, décadas após essas regulamentações terem sido revertidas, esses sistemas criptográficos enfraquecidos legados sendo implantados ao redor do mundo. Portanto, há algumas preocupações sobre a criação de regulamentações que limitam a importação e exportação de criptografia, porque mesmo quando percebemos que elas não são úteis e que causam danos às pessoas que querem se comunicar de forma segura, que é todo mundo.

Mesmo quando corrigimos esses problemas e decidimos revogar essas regulamentações, às vezes o software antigo ainda está por aí. E pior ainda, porque alguns desses softwares antigos ainda existem, outras pessoas podem decidir que vão fazer suas ferramentas interoperarem com os sistemas mais fracos porque querem se comunicar com todos. E o resultado é que acabamos com sistemas que podem ser rebaixados ou enfraquecidos pelos erros legados que cometemos no passado.

Então, eu queria destacar que uma das preocupações com a regulamentação criptográfica é que quanto mais obstáculos você coloca, mais desafiador é criar um sistema criptográfico funcional. E quanto mais obstáculos colocamos para fazer um que realmente funcione, maior é o risco de errarmos, não apenas agora, mas no futuro.

Devemos remover os obstáculos para termos comunicações seguras, se acreditarmos que vale a pena que as pessoas possam se comunicar ao redor do mundo.

Greg Nojeim - CDT: Dan. Ótimo. Quantos serviços criptografados existem por aí? Estamos falando de centenas, milhares? Existe uma maneira de contar?

Daniel Kahn Gillmor - ACLU: Deixe-me contestar um pouco a ideia de serviços criptografados, na verdade, Greg.

Então, quando falamos sobre plataformas criptografadas hoje, pensamos na Internet em termos de plataformas, certo? Existem plataformas operadas pela Meta, há o Telegram, há, você sabe, o Signal, e pensamos nelas como esses serviços que funcionam. Mas a criptografia, se for uma criptografia forte, acontece na sua máquina.

Isso acontece no seu dispositivo, seja um iPhone, um computador rodando Debian, uma máquina com Windows, ou qualquer outro. A criptografia, a criptografia de ponta a ponta, acontece no ponto final que o usuário controla. E é possível sobrepor proteções criptográficas fortes, embora seja desafiador, sobre um sistema de comunicação que não as possui inicialmente.

O serviço não precisa ser a coisa que está criptografada, pode ser apenas o software que está fazendo a criptografia. Então, quando perguntamos quantos serviços existem, podemos contar os serviços web, os serviços que estão na rede e ver quantos deles existem. E provavelmente poderíamos chegar a um número em termos de, amplamente usados, na casa das dezenas.

Mas se falarmos sobre quais peças existem por aí que fornecem mecanismos criptográficos, essas são blocos de construção fundamentais para como usamos a Internet hoje, certo? Um pedaço de software que fornece a capacidade de usar TLS. Que todos estão usando hoje para falar nesta sessão, certo? Esta sessão do Zoom está coberta com, todos que se conectam a ela usam segurança da camada de transporte.

Esse é um mecanismo de criptografia para conectar aos servidores do Zoom, obter o áudio para ouvir o que estou dizendo agora e ver todos os nossos rostos na transmissão de vídeo. As pessoas que constroem kits de ferramentas TLS estão espalhadas por aí. Agora, não há mais de uma dúzia de kits de ferramentas TLS funcionais e amplamente usados, mas TLS não é a única coisa que faz criptografia.

Existem mecanismos de e-mail criptografado. Existem aplicativos de mensagens criptografadas, certo? Novamente, eu não considero o Telegram um aplicativo de mensagens totalmente criptografado. Ele é apenas parcialmente criptografado. Há uma pequena parte que você pode ativar a criptografia. Não é exatamente o que eu gostaria. Não é o melhor em termos de criptografia, mas em termos de distribuição de ferramentas que fornecem mecanismos de criptografia, há muitas por aí e não porque essas ferramentas também são redistribuíveis.

Não há um único distribuidor, certo? Então, o sistema operacional Debian coleta um monte de pacotes de software. Alguns deles fazem criptografia e vêm de diferentes lugares. Quem é responsável pela importação ou transferência desses sistemas criptográficos? É o colaborador francês do Debian? Eu não sou francês, mas há colaboradores franceses do Debian que pegam um software criptográfico de alguém, digamos, na Suécia e o colocam no Arquivo Debian, que é distribuído em espelhos ao redor do mundo, e então ele é repentinamente rebaixado para a França?

Onde isso acontece? E quem é o responsável, quem será parado na próxima vez que trocar de avião em Charles de Gaulle porque opera um espelho do Debian? Porque carregou algo no Arquivo Debian enquanto estava na França, e se não fosse francês? Há uma série de perguntas que essa lei levanta para as pessoas que querem distribuir os blocos de construção de uma infraestrutura eficaz.

A prisão de Durov por essas duas acusações em particular levanta grandes bandeiras de alerta. Devo me preocupar como desenvolvedor do Debian? Eu trabalho com software criptográfico e ajudo a contribuir e empacotar isso para o Debian. Não sou responsável por todo esse software. Estou no meio entre as pessoas que trabalham nisso em tempo integral, focadas nesse software específico, e as pessoas que o utilizam, que são muitas mais.

Mas devo me preocupar na próxima vez que viajar pela França por ter ajudado a distribuir software livre no país que possui capacidades criptográficas que não se limitam à autenticação? E, e eu não sei, isso levanta questões que são bastante preocupantes se quisermos um ecossistema de comunicações criptográficas funcional, disseminado e auditável.

Greg Nojeim - CDT: Não temos os promotores franceses na chamada, mas parece que você tem alguma preocupação e Noémie, as pessoas devem se preocupar? Pessoas na posição do Dan, elas realmente devem se preocupar? O promotor enviou algum sinal, não sobre o Signal, sobre qual é a intenção deles com essa lei, ou esse conjunto de leis?

Noémie Levain - la Quadrature du Net: Novamente, sobre os casos que foram descritos, acho que ainda não. O que o promotor vai procurar, mas ainda assim, como é legalmente possível, você pode não saber, mas como eu estava dizendo antes de você chegar, Daniel, que a lei, essa lei de registro que foi usada contra Pavel Durov, é uma lei antiga que ninguém realmente se importava porque não era reforçada, e também

porque não se encaixa em como a criptografia realmente funciona no mundo, já que é livremente usada, distribuída e desenvolvida, mas vemos que pode ser usada como uma arma legal contra alguém que é designado como inimigo do estado. E aqui foi o Telegram e Pavel Durov.

Então, mesmo que tenha sido inicialmente para moderação de conteúdo, vemos que essa lei antiga pode ser usada como outra opção. Então, eu diria que ainda assim, você deve considerar essa lei no contexto político do Telegram. Talvez as acusações com base nisso sejam retiradas, talvez não, e se não forem, acho que essa é a questão. Se as acusações não forem retiradas, teremos que ser muito cuidadosos com a forma como o juiz irá avaliá-las, porque acho que será uma das primeiras vezes.

Então, isso pode ser um precedente legal e nos ajudar a considerar se alguém está em perigo ao chegar na França, em Charles de Gaulle. Mas, novamente, precisamos estar mais preocupados com o contexto geral na França sobre criptografia e sobre criminalizar todos, todos que estão usando uma ferramenta de criptografia, em vez de nos preocuparmos com as pessoas que as estão desenvolvendo.

Atualmente, a atenção está mais voltada para quando vemos muitos casos criminais, eles estão procurando pessoas que usam isso. E também preocupante, mencionei isso muito brevemente, mas há casos do que aconteceu com o KICC, com o AnchorChat, e quais são os meios técnicos da polícia francesa agora, é muito difícil saber, mas parece que eles são bastante fortes e esse será meu ponto de atenção.

Daniel Kahn Gillmor - ACLU: Sim, eu concordo com você, Noémie, que há uma grande preocupação sobre quais são as capacidades técnicas para quebrar a comunicação criptografada das agências de aplicação da lei e não apenas para os franceses. Como americano, estou preocupado com as capacidades americanas, bem como com as capacidades dos adversários ou aliados americanos.

E a outra coisa estranha é que, para uma nação, para nações que aderem pelo menos àquelas que afirmam querer incentivar as pessoas a se comunicarem livremente e a terem livre associação, esses são ideais consagrados na Constituição Americana, para o governo acumular a capacidade de quebrar a comunicação das pessoas.

Se as ferramentas de comunicação estão funcionando bem, nem mesmo os fornecedores dessas ferramentas deveriam ser capazes de revelar o conteúdo da comunicação. E na medida em que os estados-nação estão descobrindo vulnerabilidades, falhas nessas ferramentas, ou nas ferramentas que as cercam, para poder invadir essa comunicação, isso coloca o governo em conflito direto com as necessidades da cidadania e das pessoas que dependem dessa infraestrutura, certo?

É como se você soubesse, ah, há um tijolo que, se eu puxar, posso derrubar esta ponte. Mas vamos deixar a ponte assim, vamos deixar o tijolo lá para que, quando quisermos,

possamos puxar o tijolo e fazer a ponte desabar. Mas as pessoas precisam usar a ponte, e o governo deveria garantir que a infraestrutura da sociedade funcione.

para os objetivos que queremos. Então, eu concordo com você que temos uma preocupação muito forte sobre quais são as capacidades técnicas. Eu queria abordar seu ponto sobre o fato de que essa lei foi muito minimamente aplicada anteriormente. Esse tipo de perseguição seletiva também acontece nos Estados Unidos.

E me preocupa ver se isso for usado como uma arma contra os inimigos. Imagine as acusações contra Durov relacionadas à moderação de conteúdo. Imagine que essas acusações não se concretizem por qualquer motivo. Eles ainda poderiam continuar a processá-lo da mesma forma que nos EUA, fomos atrás de Al Capone por evasão fiscal quando o que realmente queríamos era acusá-lo de ser um mafioso e de mandar matar pessoas.

Eu não me oponho a perseguir pessoas por evasão fiscal. Devemos perseguir pessoas por evasão fiscal em geral. Mas se você tem uma lei que efetivamente criminaliza o que de outra forma seria uma conduta razoável, então os promotores podem, e os promotores podem usá-la a seu bel-prazer se todos estiverem sendo criminalizados ou se uma classe de pessoas estiver sendo criminalizada apenas com o objetivo de tentar ajudar a infraestrutura global a funcionar, mas vamos usá-la apenas para pegar pessoas específicas.

Isso me parece um problema. Essa não é uma situação em que eu gostaria que estivéssemos, de modo geral.

Greg Nojeim - CDT: Vou agora passar para algumas das perguntas que estão aparecendo no chat e na sessão de perguntas e respostas. Não podemos responder a todas, mas vamos começar. Joe Hall da ISOC pergunta: Parece que o controle de exportação/importação é realmente uma relíquia do passado para a criptografia?

Existe uma justificativa moderna legítima para controlar a criptografia ou outros tipos de tecnologia de aprimoramento de privacidade, como a privacidade diferencial? Não é controlado, mas se houver criptografia na sua solução, como computação segura de múltiplas partes, etc., então você deve enviar uma nota para a França e uma cópia do seu código-fonte se eles solicitarem.

É isso que a lei diz, que eles podem pedir o código-fonte também. Isso é uma relíquia ou há uma justificativa moderna legítima para controlar a criptografia?

Daniel Kahn Gillmor - ACLU: Não sei se "relíquia" é o termo que eu usaria, mas eu diria que parece singularmente inviável pedir controles de exportação. O código-fonte é uma quantidade relativamente pequena de dados. Não estou tão preocupado com a ideia

de solicitar o código-fonte. Eu tendo a preferir que o código-fonte dos meus sistemas de comunicação seja completamente aberto, visível e modificável, nesse caso.

Essa é a essência da promessa do software livre: os usuários estão no controle. Mas a ideia de que você efetivamente impediria sua transferência, são apenas alguns bytes. É uma quantidade muito pequena de dados que proporciona essa capacidade. E pensar que você pode realmente evitar que isso vaze através das fronteiras neste ponto me parece implausível.

Está dizendo, estamos bem com você fazendo matemática, mas se sua matemática envolver, a divisão longa está fora dos limites. Não queremos que você fale sobre como fazer divisão longa ainda. Sem nos avisar que você está fazendo isso. E isso simplesmente não é plausível.

A divisão longa surge de outras partes da matemática que você vai fazer, assim como a criptografia. Agora, dou algum crédito ao decreto francês de 2007 por separar os serviços criptográficos que fazem apenas autenticação e verificação dos serviços que fazem criptografia. Pelo menos eles não tentaram nos impedir de verificar atualizações de software sem primeiro consultar as autoridades.

Certo? Isso é bom. Pelo menos perceberam que não podiam fazer isso. Mas uma vez que você tem as ferramentas para fazer autenticação e verificação criptográfica, que, aliás, são necessárias para fazer criptografia forte, você precisa saber com quem está falando. Não é um grande salto adicionar uma camada criptografada a isso.

Esses mecanismos são úteis em todas essas formas. Então, eu simplesmente não vejo o controle de exportação como algo viável de operar. Em particular, se o objetivo é manter a criptografia forte fora das mãos dos bandidos, isso simplesmente não vai acontecer, certo? Uma vez que você permite que os mecanismos de criptografia em geral, mesmo deixando de lado a parte da criptografia, uma vez que os mecanismos de criptografia em geral se tornem amplamente difundidos, você não vai impedir que os piores dos piores usem os mecanismos de criptografia.

Então, tudo o que você vai fazer é impedir que todos os outros usem os mecanismos de criptografia. E, como resultado, quem terá a base de comunicação mais fraca? Será o público em geral. Isso me parece contraproducente.

Greg Nojeim - CDT: Então, houve uma pergunta no Q&A que eu quero destacar.

Não sei se alguém tem a resposta, mas a pergunta é: existe uma lista de leis ruins de criptografia no mundo? Ou seja, vamos mudar essa lei francesa. Mas o que vem a seguir na lista que precisa ser mudado? Eu não vi isso. Existe uma lista assim?

Noémie Levain - la Quadrature du Net: Eu não sei, não sei se você quer dizer globalmente ou na França, mas globalmente, eu não sei. Na França, eu também acompanho o que está acontecendo no nível da União Europeia. Também sei que há algumas tentativas nas instituições europeias de minar a criptografia que estão por vir.

Mas, no momento, se há uma lista de leis existentes a serem revisadas, na verdade, não sei se há outros alvos a serem identificados e melhorados. Talvez Daniel, alguns ou...

Daniel Kahn Gillmor - ACLU: Eu esperava deixar isso para você, já que você tem a expertise jurídica, Noémie.

Greg Nojeim - CDT: Na verdade, isso parece algo que deveríamos organizar na Coalizão Global de Criptografia, se possível.

Daniel Kahn Gillmor - ACLU: Concordo.

O desafio é que ninguém... Eu não tenho expertise jurídica no sistema legal dos EUA como tecnólogo, essa não é a minha especialidade. E as pessoas que têm expertise jurídica em um sistema legal provavelmente não têm nos outros 180 sistemas legais que existem.

Então, seria necessário um esforço colaborativo e, claro, haverá alguns estados-nação que simplesmente não conseguiremos mover. Mas, identificar alguns dos padrões comuns, identificar as semelhanças certamente seria útil. E como Noémie mencionou, há várias tentativas pendentes, isso vem acontecendo desde as guerras criptográficas dos anos 1990, de adicionar essas leis, certo?

Portanto, não devemos apenas ter a lista de leis ruins, mas também de propostas de leis ruins, porque essas precisam ser constantemente combatidas. Nos EUA, a linguagem que vem da aplicação da lei é esse tipo de debate sobre "ficar no escuro", e isso se torna cansativo. Já tivemos esse debate por muito tempo.

Não parece mudar muito. E, em última análise, as concessões subjacentes são se queremos ter uma sociedade onde as pessoas possam se comunicar sem se preocupar com a interferência de uma terceira parte. Seja essa terceira parte a aplicação da lei, adversários criminosos, espionagem industrial, amantes rejeitados ou qualquer outra coisa.

Greg Nojeim - CDT: Parece-me que seria muito difícil compilar esta lista porque existem as leis que controlam explicitamente a criptografia, dizendo que você não pode exportá-la ou que deve registrá-la. Mas também existem as leis que tornam arriscado oferecer um serviço criptografado.

Porque você não pode moderar o conteúdo tão bem quando não pode vê-lo e muitos governos estão falando sobre impor deveres de cuidado nas plataformas que são difíceis de suportar quando você não pode realmente ler o conteúdo. Uma pergunta feita na sessão de perguntas e respostas foi: até que ponto a mensagem criptografada é um canário na mina de carvão?

Um tipo de sinal de alerta precoce para outras tecnologias de segurança como o TLS. Esse é o caso Durov, é uma disputa entre o estado e um fornecedor de software por causa do que as pessoas estão compartilhando na plataforma. Acho que isso está provavelmente correto. Em que ponto esse tipo de pressão? desce da camada de aplicação para coagir o conteúdo, para coagir outras ações.

Daniel Kahn Gillmor - ACLU: Posso falar sobre isso do ponto de vista dos protocolos criptográficos. Então, definitivamente vimos tentativas de fazer com que os protocolos criptográficos de nível inferior forneçam recursos adicionais para fins de escuta telefônica. E nos EUA temos a legislação CALEA. A CALEA é a Lei de Assistência às Comunicações para a Aplicação da Lei.

e basicamente exige que você tenha backdoors em mecanismos de telefonia. O que, felizmente, não inclui TLS. Mas esses backdoors obrigatórios foram forçados nos equipamentos de telecomunicações pelos EUA, e esses backdoors nos equipamentos de telecomunicações têm sido, eles próprios, locais de inúmeros comprometimentos, incluindo, você pode voltar ao caso de Atenas em 2005, onde partes além das agências de aplicação da lei que pedem esses recursos conseguiram entrar e comprometer as comunicações das pessoas.

A margem de manobra de que você está falando, identificar leis ruins, Greg, é complicada. Eu só li uma tradução para o inglês do decreto francês neste caso, então não sei quão precisa ela é, talvez, sabendo que você pode falar sobre isso, mas parecia ter algumas exceções sobre a declaração ser marcada como aceitável ou inaceitável pela ANSI, com base em se colocava em risco os interesses nacionais ou a segurança nacional ou algo assim.

E isso é um grande... quando ouço as palavras segurança nacional, fico preocupado porque elas são usadas como pretexto para qualquer agenda que as pessoas estejam promovendo. Então, Noémie, não sei se você pode falar sobre essas exceções.

Noémie Levain - la Quadrature du Net: Eu não tenho todo o decreto em mente, mas é verdade que, como você disse, sempre que há uma isenção ou objetivo de segurança nacional, é uma maneira de impor algumas medidas muito intrusivas. Na França, não sei o que vai acontecer a seguir, porque você vê muita intenção política de tentar enfraquecer a criptografia, pedindo backdoors, mas também a ANSI, que é como a agência de cibersegurança, há tensão entre o governo e a ANSI porque a ANSI continua dizendo que se você enfraquecer a criptografia para procedimentos criminais, você enfraquece a criptografia para todos e para muitas outras camadas técnicas, etc.

Então, a tensão, como você disse, vem acontecendo há anos e décadas, mas vemos, agora, mais esforços. E o problema com um aplicativo de mensagens criptografadas é que eles têm essa imagem no mundo político da mídia de serem ferramentas de bandidos. Por isso, eles vão primeiro para esses tipos de ferramentas. Toda vez que você lê um artigo sobre, sei lá, algumas gangues, eles dizem que estavam usando aplicativos criptografados, mesmo que não tenha nada a ver com o assunto.

Então você pode ver que piorou na, na, narrativa é a imaginação e é por isso que estamos preocupados, porque se a narrativa continuar primeiro, então é mais fácil para o governo ou o juiz dizer que faz parte do crime, que é cúmplice, etc. Então vemos que eles estão indo para.

Eles atacam isso primeiro e talvez ataquem outros tipos de outras camadas depois. E estou tentando lembrar a outra parte das perguntas, mas novamente, ah sim, sobre segurança nacional, na verdade, como eu disse, o decreto, esse tipo de decreto antigo não é muito aplicado, então não temos muitos precedentes ainda, mas e o caso Durov, não é sobre segurança nacional, mas sobre crimes gerais, como é em inglês? Mas crimes graves.

Mas você estava falando sobre o "going dark" e todas as tentativas em andamento no nível europeu ou na França. É sempre a segurança nacional que é, que é, que é colocada em primeiro lugar pelo governo e então não podemos fazer nada em relação a isso porque é a desculpa para todas as exceções e todas as tentativas.

E então, neste momento, a tensão de que eu estava falando entre a ANSI e o governo está se mantendo, e a criptografia ainda está preservada, mas não sabemos o que acontecerá nos próximos anos ou meses.

Daniel Kahn Gillmor - ACLU: Quero dizer, Greg, queria mencionar mais uma coisa. E sua pergunta é sobre esses projetos de lei que estão sendo propostos e que podem acabar tornando desafiador cumprir o objetivo do projeto sem remover a criptografia de um serviço.

E nos EUA, alguns desses projetos de lei têm exceções explícitas que dizem que nada neste projeto deve ser interpretado como uma exigência para remover a comunicação criptografada. E ainda assim, quando você lê a linguagem simples do projeto, não sei como você faria isso sem remover a criptografia de ponta a ponta.

Então, realmente é uma questão de como nós...? As pessoas que estão redigindo os projetos de lei estão cientes, o que é bom. É uma situação melhor do que no passado, pois eles sabem que não querem esses efeitos colaterais negativos. Mas eu não sei como interpretar claramente os projetos de lei ou quem vai interpretá-los quando chegar a hora.

Greg Nojeim - CDT: Sim, é um problema real. É um problema nos EUA, na Europa, em todo o mundo. Ouçam, nosso tempo acabou e precisamos encerrar. Mas direi isto: estaremos acompanhando o caso Durov na Global Encryption Coalition.

Se houver desenvolvimentos significativos, Noémie, mantenha-nos informados e manteremos o mundo todo preocupado com a criptografia atualizado. Quero agradecer ao Dan e à Noémie por se juntarem a nós hoje e agradecer a todos por se inscreverem para ouvir, e obrigado à ISOC por cuidar da logística para a Coalizão Global de Criptografia no Dia Global da Criptografia.

E eu gostaria de me despedir e dizer adeus a todos.

Noémie Levain - la Quadrature du Net: Tchau.

Greg Nojeim - CDT: Obrigado a todos.