LIÇÕES DOS ESTADOS UNIDOS:

A NECESSIDADE PRÁTICA DOS "PRINCÍPIOS INTERNACIONAIS SOBRE VIGILÂNCIA E DIREITOS HUMANOS".

POR: HANNI FAKHOURY

Introdução

O objetivo dos Princípios Sobre Vigilância e Direitos Humanos ("Princípios") é fornecer um quadro pelo qual as leis e práticas de vigilância atuais ou propostas possam ser avaliadas para garantir que sejam consistentes com os direitos humanos. O desenvolvimento destes princípios oferece uma oportunidade única para rever a experiência dos Estados Unidos na regulamentação da vigilância do governo e no acesso a dados eletrônicos, para entender a necessidade dos Princípios.

Este trabalho pretende oferecer uma breve explicação da legislação norte-americana, no que tange a cada um dos Princípios. Embora a legislação dos Estados Unidos seja desenvolvida tanto em nível federal quanto estadual, este trabalho enfoca a legislação federal. Este trabalho também lança um olhar à legislação que rege investigações nacionais, e apenas brevemente discute coleta de informações estrangeiras e segurança nacional.

Legalidade

Nos Estados Unidos, o direito à privacidade eletrônica está contido em duas fontes legais: (1) as Constituições Federal e Estadual; e (2) o direito positivo federal ou estadual.

A Quarta Emenda da Constituição dos Estados Unidos aplica-se ao governo federal e a todos os Estados, e proíbe o governo de exercitar buscas e apreensões irracionais. Ela exige que as autoridades policiais obtenham um "mandado de busca e apreensão" antes de revistar um lugar, incluindo dispositivos eletrônicos e outros tipos de dados digitais. Uma "busca", nos termos da Constituição, é definida tanto como uma (1) invasão pelo governo em propriedade privada com a finalidade de obter informações; ou (2) uma intromissão do governo em um lugar onde uma pessoa possui uma expectativa subjetiva de privacidade que a sociedade aceita como razoável.

Sob o direito positivo federal, a Lei de Privacidade de Comunicações Eletrônicas ("ECPA", na sigla em inglês) regula o acesso das autoridades policiais a muitos tipos de dados eletrônicos. A ECPA tem divisões, lidando com tipos específicos de dados; o Título I da ECPA é a Lei da Interceptação, que regula a forma como o governo pode ouvir ou interceptar o conteúdo de uma comunicação privada como, por exemplo, as chamadas telefônicas. O Título II da ECPA é a Lei de Comunicações Armazenadas ("SCA", na sigla em inglês), que regula a forma como o governo pode acessar o conteúdo de comunicações eletrônicas (tais como e-mails, tweets, mensagens de texto etc.), bem como outras informações sem conteúdo (tais como registros de localização de celular) de um provedor de armazenamento em nuvem ou de comunicação eletrônica. Finalmente, os estatutos de Dispositivo

de Registro de Caneta/Dispositivo de Captura e Rastreamento ("Pen/Trap") regulam como o governo pode obter informações de roteamento e transmissão por meio de telefonemas e outras formas de conteúdo eletrônico, tais como endereços IP e cabeçalhos de e-mail.

A maioria dos Estados adotou total ou parcialmente estas disposições da lei federal. Em geral, os Estados são livres para adotar maior proteção legal do que aquela existente sob a lei federal, mas não podem oferecer menos proteção à privacidade. Alguns Estados tomaram algumas medidas para melhorar seus estatutos de privacidade eletrônica e geralmente moveram-se muito mais rápido do que o governo federal, que não foi capaz de atualizar a ECPA adequadamente desde que ela foi promulgada em 1986.

Necessidade

Sob a quarta emenda, um mandado de busca deve ser limitado tanto quanto possível, para evitar que se vasculhem de maneira geral os pertences de uma pessoa, incluindo seus dados eletrônicos. Isso inclui a exigência de que a polícia retorne ao juiz com um inventário do que apreendeu, de modo que o tribunal possa supervisionar a polícia. Quando se trata de dados eletrônicos, um tribunal advertiu (PDF) que os juízes devem exercer "maior vigilância" para garantir que o governo não colete mais que os dados necessários.

No entanto, os estatutos de privacidade eletrônica nos Estados Unidos possuem um registro confuso quando se trata de limitar o acesso das autoridades policiais. A Lei da Interceptação tem incorporada uma forte proteção à privacidade, exigindo que a polícia minimize as conversas telefônicas interceptadas para garantir que capturem apenas conversas sobre atividade criminosa. Mas os estatutos SCA e Pen/Trap não têm requisitos semelhantes de minimização para o conteúdo de comunicações eletrônicas ou informações de roteamento de internet. Isso precisa ser mudado – particularmente o SCA –, pois pode potencialmente assegurar às autoridades policiais amplo acesso a e-mails e outras formas de conteúdo eletrônico.

Adequação

Conforme explicado acima e como demonstrou o escândalo Petraeus, os policiais dos Estados Unidos têm sido tudo, menos contidos, quando se trata de busca e apreensão de dados eletrônicos.

Para piorar a situação, tem havido grande pressão das autoridades policiais sobre o Congresso para implementar políticas de retenção de dados para uma ampla gama de dados armazenados por provedores de serviços de comunicação, tais como informações de endereço IP e mensagens de texto. Ali, as políticas exigiriam que os provedores mantivessem informações unicamente para que as autoridades policiais pudessem examiná-las em um momento posterior, muitas vezes contra a vontade – e interesses de negócio – dos provedores.

É preciso que haja resistência contra estes tipos de política, que têm apenas a finalidade de vigilância governamental, e, tal como descrito em mais detalhes abaixo, apresentam riscos para a segurança.

Proporcionalidade

A Quarta Emenda da Constituição dos Estados Unidos exige que a polícia obtenha um "mandado de busca" para realizar uma "busca" ou apreender dados eletrônicos ou físicos. Para obter tal "mandado de busca", os policiais devem demonstrar ao juiz que têm uma "causa provável" – mais provável do que improvável – de que a prova de um crime será encontrada no lugar que desejam revistar. Se o juiz acredita que a polícia demonstrou a causa provável, ele pode emitir o mandado de busca, embora deva especificar em quais locais específicos a polícia pode procurar, e quais itens específicos ela pode apreender.

Mas esta norma de causa provável só se aplica se o governo estiver envolvido em uma "busca". E há muitas exceções (na verdade, em número alto demais) à exigência de mandado de busca. Além disso, embora esteja claro

que a Quarta Emenda se aplica a dados armazenados no dispositivo físico de uma pessoa, como um telefone celular, por exemplo, é menos claro se ela se aplica a dados armazenados por terceiros e na nuvem.

Alguns tribunais têm interpretado a Quarta Emenda no sentido de que uma pessoa não tem uma expectativa razoável de privacidade quando as informações são entregues a outra pessoa, por exemplo, um ISP ou um site de mídia social, o que significa que as autoridades policiais não estão sob nenhuma obrigação constitucional de apresentar um mandado de busca para obter informações de clientes e dados junto a empresas como Facebook, Twitter ou Google. Um Tribunal de Nova York, por exemplo, decidiu que Ministério Público não precisava obter um mandado de busca e apreensão para obter dados do Twitter sobre Malcolm Harris, um manifestante do movimento Occupy Wall Street, e em vez disso poderia obter informações como tweets, login de endereço IP com uma intimação, uma vez que os dados pertenciam ao Twitter, e não a Harris. A mesma coisa aconteceu com os registros de Twitter sobre Birgitta Jonsdottir, membro do parlamento islandês, que o governo federal queria acessar em conexão com sua investigação em curso sobre o caso Wikileaks. Outros tribunais têm discordado, achando que, apesar de as informações como e-mails serem entregues a terceiros, ainda estão constitucionalmente protegidas, e as autoridades policiais devem obter um mandado de busca e apreensão para examiná-las.

Para piorar as coisas, o direito positivo federal também não usa esta norma de causa provável para todos os tipos de informação. Em vez disso, diferentes normas jurídicas de vários graus de proteção de privacidade aplicam-se os diversos tipos de informações eletrônicas e digitais nos Estados Unidos.

A proteção de privacidade mais forte é a Lei da Interceptação, que não só exige que as autoridades policiais tenham causa provável para acreditar que interceptar telefonemas levará a evidências de crimes especificamente listados, mas também exige que demonstrem: (1) causa provável de que as comunicações relacionadas com o crime serão obtidas através da interceptação; (2) que os procedimentos de investigação normal foram empreendidos e falharam, ou que é razoavelmente improvável que tenham sucesso se forem experimentados, ou que são demasiadamente perigosos; e (3) causa provável para acreditar que o número de telefone ou outro dispositivo eletrônico onde ocorre a comunicação a ser interceptada tem uma ligação com o crime ou a pessoa a ser investigado.

Mas outros trechos da ECPA não têm as mesmas proteções fortes de privacidade contidas na Lei da Interceptação. A SCA exige que as autoridades policiais somente obtenham um mandado de busca para acessar o conteúdo das comunicações eletrônicas armazenadas eletronicamente por menos de 180 dias. Aquelas mais antigas, bem como outros tipos de dados eletrônicos armazenados, no entanto, podem ser obtidos sem um mandado de busca e apreensão sob a SCA.

Se o governo puder demonstrar a um juiz "fatos específicos e articuláveis" de que os dados são "relevantes e materiais para uma investigação criminal em curso" – uma norma menor que a norma de causa provável do mandado de busca – a SCA permite que o governo obtenha: (1) o conteúdo das comunicações armazenadas eletronicamente por mais de 180 dias (tal como um antigo e-mail localizado em uma caixa de entrada de e-mail); (2) o conteúdo de comunicações eletrônicas armazenadas em um provedor de armazenamento em nuvem, sem ter que enviar uma notificação ao assinante (tal como um PDF armazenado na Dropbox ou no Google Drive); e (3) outros registros de cliente não incluindo conteúdos (tal como informações de endereço IP ou informações de localização do site de celular).

E apenas com uma intimação – que não tem absolutamente nenhuma supervisão judicial e pode ser emitida por um advogado, desde que seja "relevante" – o governo pode acessar: (1) o conteúdo de comunicações eletrônicas armazenadas em um provedor de armazenamento em nuvem com notificação prévia ao cliente; e (2) outras "informações do assinante", incluindo o nome do cliente, endereço, registros de conexão de telefone local e interurbano ou registros de hora e duração de sessão, tipo e duração de serviço (incluindo a data de início), número de telefone ou outro número de assinante ou identidade, incluindo qualquer endereço de rede temporariamente atribuído e meios e fontes de pagamento do serviço.

Finalmente, os estatutos Pen/Trap permitem ao governo obter informações de roteamento, se ele puder provar a um juiz que os dados desejados são "relevantes para uma investigação criminal em curso".

As diferentes normas nesses estatutos criam confusão para todos. Os consumidores não têm certeza de quanta proteção de privacidade eles têm. As autoridades policiais, conforme foi demonstrado, não são claras e consistentes no uso da norma jurídica correta para obter dados. E os tribunais estão lutando para aplicar jurisprudência formada muito antes do advento de tecnologias tais como telefones celulares e redes de mídia social ao mundo moderno em que vivemos agora.

Uma norma uniforme que se aplique a todas as tipos de dados eletrônicos e que contenha fortes proteções à privacidade, como aquelas recomendadas nos Princípios, beneficia igualmente os consumidores e as autoridades.

Devido Processo Legal

Conforme explicado acima, nem todos os pedidos de dados eletrônicos por autoridades exigem autorização judicial prévia. E mesmo quando a aprovação judicial é necessária, as normas para divulgação diferem, dependendo dos dados que estão sendo solicitados. Mas, ainda mais problemático de uma perspectiva de "devido processo legal" é a dificuldade em provar as violações, tanto em contextos de direito penal quanto civil.

Um réu em um processo criminal pode contestar as buscas e apreensões de dados eletrônicos pelo governo que ocorram sem mandado de busca, ou se o mandado de busca for deficiente de alguma forma. Mais comumente, isso ocorre depois que uma pessoa foi acusada de um crime e apresenta uma moção para supressão de provas. Mas é só a prova que o governo pretende usar contra o réu no julgamento que pode ser suprimida. Tudo o que uma contestação bem sucedida fará será eliminar a capacidade do governo de usar certas formas de prova para condenar a pessoa. Elas ainda podem enfrentar acusação e prisão, em muitos casos, mesmo sem o uso das provas pelo governo. E embora os tribunais "suprimam" provas obtidas com violação da Quarta Emenda, há muitas exceções ao recurso da supressão que diminuem sua eficácia. Por exemplo, a prova não será suprimida se foi descoberta por agentes agindo de boa fé com uma crença razoável, mas equivocada, de que estavam autorizados a apreender o item. Além disso, os tribunais hesitam em criticar as autoridades policiais ou seus colegas do judiciário no que se refere a rever itens do processo de busca e apreensão. Como resultado, a supressão não é muito comum.

A situação é ainda mais sombria quando se trata de provar violação das restrições legais ao acesso do governo a dados eletrônicos. A Lei da Interceptação tem um recurso legal de supressão, ao passo que nem a SCA, nem os estatutos Pen/Trap o têm. As contestações de apreensão ilegal do conteúdo de comunicações eletrônicas ou informações de roteamento devem ser apresentadas à luz da Quarta Emenda, e não dos estatutos em si.

Para indivíduos que foram vigiados ilegalmente, mas não foram acusados de um crime, tanto a Lei de Interceptação quanto a SCA permitem a um particular processar judicialmente por interceptações ilegais de áudio e apreensão de conteúdos eletrônicos. Mas é extremamente difícil superar os muitos obstáculos processuais necessários para entrar com uma ação civil contra o governo. A EFF tentou processar o governo por apreensões de dados eletrônicos em conexão com a desarticulação da Megaupload, bem como processar tanto a Administração Nacional de Segurança quanto a AT&T com base no programa de escuta sem mandado do governo federal sob o presidente George W. Bush, com variados graus de sucesso. O caso Megaupload ainda está *sub judice*, mas caminha lentamente. O caso contra a NSA também caminha lentamente, com a tentativa do governo de anulá-lo baseado no fato de que o litígio o forçaria a revelar "segredos de estado". E o Congresso aprovou uma lei garantindo imunidade à AT&T contra processos judiciais, encerrando efetivamente qualquer contestação legal do seu papel no programa de escutas telefônicas ilegais.

Notificação ao Usuário

O direito positivo Federal permite que autoridades policiais exijam que os provedores permaneçam calados sobre solicitações de dados de clientes. Por exemplo, como parte do PATRIOT Act após o 11 de setembro, o FBI pode ignorar tribunais e emitir cartas administrativas, chamadas Cartas de Segurança Nacional ("NSLs") (PDF), com base em sua própria autoridade, às empresas de telecomunicações. As NSLs não só exigem que as empresas divulguem informações sobre um cliente, mas também obrigam que estas não informem o cliente sobre aquele

pedido, e até mesmo mantenham em segredo o recebimento de uma NSL. Houve apenas um pequeno número de contestações legais a esta prática. Mesmo fora do contexto de Segurança Nacional, a SCA permite que o governo adie a notificação ao usuário sobre uma solicitação governamental do conteúdo das comunicações eletrônicas e outras informações por até 90 dias, e as autoridades policiais ainda podem solicitar prorrogações adicionais de mais 90 dias.

Na ausência de qualquer limite legal à capacidade do provedor de serviços de notificar seus usuários sobre solicitações de dados, as empresas não possuem um registro claro de informação aos clientes sobre pedidos de suas informações digitais por autoridades policiais. O Twitter, por exemplo, tem uma política de informar a seus usuários sobre todos os pedidos de informação antes de sua divulgação, a menos que esteja proibido por ordem judicial. A política do Facebook é mais vaga, insinuando que as autoridades policiais devem obter uma ordem judicial para impedir a notificação, mas também permitindo a confidencialidade caso a notificação "leve a risco de dano".

A importância da notificação ao usuário não pode minimizada: estes devem ter conhecimento das solicitações prontamente, a fim de proteger seus dados e procurar orientação e assistência jurídica. Qualquer requisição governamental para adiar a notificação deve ser limitada a circunstâncias de emergência, e deve ser o mais breve possível. O mecanismo NSL de acesso silencioso e secreto a dados de um usuário deveria ser rejeitado, bem como a abordagem da SCA de adiar notificações por longos e abrangentes períodos. Instituir essas normas para as autoridades policiais permitirá às empresas sentirem-se mais encorajadas a notificar seus usuários sobre pedidos de autoridades policiais, com maior frequência do que o fazem atualmente.

Transparência sobre a utilização de vigilância pelo governo

A legislação americana é totalmente falha quando se trata de transparência. Com exceção de ordens de interceptação sob a Lei de Interceptação, segundo a qual se exige que o governo publique um relatório anual sobre o uso de escutas telefônicas, há muito pouca transparência sobre a frequência com que o governo busca acesso a provas eletrônicas: até mesmo o Departamento de Justiça esteve sob escrutínio por não entregar registros e estatísticas completas da Lei de Interceptação ao Congresso, conforme exigido por lei. Fora os mandados de interceptação, porém há pouca transparência por parte do governo ou dos provedores sobre quanta informação o governo está coletando e para que fins.

Como resultado disso, as informações sobre uso pelo governo de vários tipos de dados eletrônicos só veio à luz através de uma solicitação do Congresso por informações sobre solicitações a empresas de telefonia celular, um pedido sob a Lei de Liberdade de Informações ("FOIA", na sigla em inglês) protocolada pelo Sindicado Americano de Liberdades Civis ("ACLU") junto às agências policiais locais relativo ao uso de informações de localização de torre de celular, e um relatório produzido por iniciativa próprias por algumas empresas (como Google e Twitter) sobre o número de pedidos domésticos e internacionais de informações de usuários por autoridades policiais. Infelizmente esses relatórios são a exceção, não a regra. A maioria das empresas de tecnologia não revela voluntariamente essa informação. E as tentativas em nível estadual de obrigá-las a fazê-lo têm sido recebidas com forte oposição pelas empresas.

Em última análise, o quadro pintado por essas solicitações informais é de aumento das solicitações de dados do usuário pelo governo. Assim, é preciso ter maior transparência para permitir que os usuários acompanhem essas crescentes demandas e reajam contra os excessos.

Vigilância

Nos Estados Unidos a vigilância se origina presumivelmente dentro dos diferentes ramos do governo. As agências de execução da legislação no poder executivo possuem inspetores gerais que revisam práticas internas e, em última análise, reportam-se ao Diretor de Inteligência Nacional. No poder legislativo, as comissões de

supervisão congressional recebem relatórios de diferentes agências de execução legal. E o poder judiciário ouve as contestações legais à vigilância do governo.

Mas nenhuma dessas comissões de supervisão é realmente independente. Mesmo as comissões que deveriam ser "independentes" não o são em nenhum sentido da palavra. Por exemplo, o Conselho de Supervisão de Inteligência ("IOB") é um painel civil de supervisão independente nomeado pelo presidente e que assegura que o governo esteja em conformidade com a lei durante investigações de inteligência estrangeira. Mesmo assim, suas ações, incluindo, por algum tempo, sua composição, são envoltas em segredo. Para inteligência doméstica, o Conselho de Supervisão de Privacidade e Liberdades Civis (PCLOB) destinava-se a agir como verificador independente das práticas de vigilância doméstica, mas tem agido de forma amplamente ineficaz, negligenciado tanto pelo presidente Bush quanto pelo presidente Obama, e já se reorganizou (PDF) apesar da sua existência relativamente curta. Tanto o IOB quanto o PCLOB encontram-se dentro do gabinete do presidente e a ele se reportam, colocando sua verdadeira "independência" em sérias dúvidas.

Assim, exceto quanto aos esforços das diversas organizações de liberdades civis como FEP, ACLU, Centro para Democracia e Tecnologia ("CDT"), Centro de Informação de Privacidade Eletrônica ("EPIC") e outros que se encarregam de acompanhar as práticas domésticas de vigilância do governo, não há nenhuma comissão pública de supervisão independente eficaz encarregada de rever essas práticas. E naturalmente, apesar dos seus melhores esforços, essas organizações tem acesso limitado às informações. A maior parte dessas informações é obtida através de processos judiciais e solicitações sob a FOIA, e as organizações certamente não possuem condições de revisar informação secreta ou confidencial na maioria dos casos.

É necessário haver uma comissão de fiscalização mais formal e verdadeiramente independente, encarregada de analisar as práticas tanto nacionais quanto internacionais de vigilância e coleta de informações, para evitar abusos de liberdades civis e conferir transparência às práticas do governo.

Integridade de comunicações e sistemas

A integridade da arquitetura de rede é fundamental para um mundo digital seguro. Mas o governo dos Estados Unidos vem há muito tempo travando uma batalha aparentemente incompatível com este objetivo. Apesar dos riscos óbvios à privacidade e segurança, ele exortou Congresso a implementar longos períodos de retenção obrigatória de dados, pressionou pela proibição de criptografia – uma ferramenta fundamental para proteger comunicações eletrônicas –, tudo isso ao mesmo tempo em que fazia lobby para garantir o seu próprio acesso pela porta dos fundos a sistemas de comunicação.

A proposta de um acesso às comunicações de internet por *backdoor* vem de uma pressão para atualizar o Projeto de Aplicação da Lei para as Comunicações ("CALEA"). O Congresso aprovou o CALEA em 1994, forçando as empresas de telefonia a redesenhar suas arquiteturas de rede para facilitar as escutas. Mas ela excluía especificamente os dados de tráfego via internet. À medida que a internet se expandiu, as autoridades policiais exerceram pressão crescente sobre o Congresso para atualizar a CALEA e exigir que os provedores de comunicações assegurassem que suas redes tivessem uma *backdoor* que permitisse ao governo interceptar também as comunicações via internet. Esta atualização proposta para a CALEA (muito parecida com a pressão das autoridades pela lei de retenção de dados) tem longo alcance e, obviamente, consequências negativas para a privacidade, segurança e inovação.

Além disso, por vezes, o governo perseguiu com mão pesada as pessoas que expuseram falhas e vulnerabilidades de segurança. Um pesquisador foi recentemente condenado por crime federal, com base na lei que proíbe o acesso ilegal a computadores, quando expôs uma falha no site da AT&T que lhe permitiu obter endereços de e-mail de clientes de iPad AT&T apenas visitando um site sem restrições, e sem violar quaisquer barreiras tecnológicas para acessá-lo. Em outro caso, a Autoridade de Transporte de Massachusetts tentou silenciar pesquisadores que estavam planejando apresentar numa conferência uma pesquisa sobre as vulnerabilidades que descobriram no sistema de pagamento de tarifa de transporte.

Em última análise, o governo deveria incentivar as empresas de tecnologia a manter os dados de seus clientes em segurança. Mas minimizar o risco de divulgação deve incluir impedir que o governo acesse sistemas por *backdoor* e limitar a retenção de dados. Ao mesmo tempo, os pesquisadores de segurança que não acessam informações eletrônicas ilegalmente não devem ser tratados como criminosos por simplesmente informar ao público de suas descobertas.

Salvaguardas para cooperação internacional

Infelizmente, muitos países vêm tentando importar algumas das piores práticas de vigilância dos Estados Unidos. Desafortunadamente, alguns países têm usado a cooperação internacional como meio para vigiar pessoas violando suas próprias leis nacionais. Por exemplo, na investigação criminal norte-americana do site Megaupload e seu fundador Kim Dotcom por violação de direitos autorais, descobriu-se que autoridades da Nova Zelândia obtiveram não apenas mandados de busca inadequados para a casa de Dotcom no país, mas também o espionaram ilegalmente, monitorando todo o tráfego de internet que entrava e saía de sua casa.

Por isso é importante assegurar que qualquer lei ou tratado que legitime a vigilância em massa deve ser contestado. E qualquer tratado de assistência jurídica mútua (MLAT) deve garantir que, diante de normas jurídicas conflitantes, o padrão mais alto e mais protetor seja aplicado.

Impedindo o acesso ilegítimo

Conforme explicado acima, em contextos não criminais os indivíduos que foram vítimas de vigilância ilegal têm recursos tanto sob a Lei de Interceptação quanto sob a SCA para instaurar processos judiciais. Mas os tribunais e os legisladores deveriam garantir que não haja barreiras processuais excessivamente onerosas à instauração de um processo.

Custo de vigilância

Um pedido FOIA abrangente feito pela ACLU em 2012 revelou em detalhes os preços que as empresas cobravam das autoridades policiais pelo acesso a interceptações e registros de localização de celulares. Apesar de as empresas insistirem que não estão lucrando com a execução da lei, e que estão meramente recuperando custos, o registro é menos claro. Um executivo da Sprint indicou que o seu sistema automatizado para a manipulação de pedidos de autoridades policiais é "extremamente barato e fácil de operar". E os argumentos do setor de telefones celulares contra a imposição da obrigatoriedade para o fornecimento de informações como um fardo dispendioso foram descartados como "risíveis" e "sem fundamento". Proibir as empresas de lucrar com a imposição da lei as incentivaria a ser proteger melhor a privacidade, eliminando seu incentivo financeiro para aderir cegamente às solicitações de dados por autoridades policiais.

Conclusão

Esperamos que esta cartilha sobre a lei dos Estados Unidos demonstre a importância prática dos Princípios. Como os erros da legislação dos Estados Unidos deixam bem claro, há muitas maneiras em que a privacidade pode ser corroída e a vigilância desenfreada pode florescer. Os Princípios são um primeiro passo crucial não só para garantir que a privacidade eletrônica floresça internacionalmente, mas também para iniciar o processo de preenchimento das lacunas de proteção de privacidade existentes na legislação dos Estados Unidos.