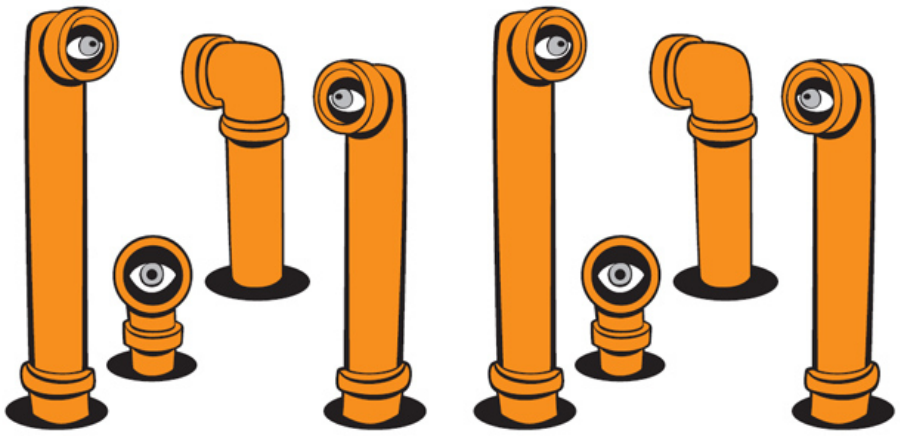
Direitos Humanos e o comércio de tecnologias: como as corporações podem evitar colaborar com regimes repressivos

*Por **Cindy Cohn**, diretora da Electronic Frontier Foundation*

*Por **Trevor Timm**, colaborador ativista da Electronic Frontier Foundation*

*Por **Jillian C.York**, diretora da Electronic Frontier Foundation*



Data da publicação:

Maio de 2012

Já há anos é possível encontrar provas suficiente de que governos autoritários ao redor do mundo têm contado com tecnologias produzidas por empresas americanas, canadenses e europeias para facilitar violações de direitos humanos – e hoje tudo indica que esta tendência é crescente. De softwares que permitem filtramento e bloqueio de conteúdo online a ferramentas que ajudam governos a espionarem seus cidadãos, muitas de tais empresas estão servindo ativamente a governos autocráticos, como “pequenos ajudantes da repressão”.

Voyages photographiques

O alcance destas tecnologias é incrivelmente amplo: governos podem fazer escutas em chamadas de telefones celulares[1], usar reconhecimento de voz para fazer varreduras em redes móveis, usar reconhecimento facial para fazer buscas em fotografias online e offline, ler mensagens de e-mail e texto, rastrear todos os movimentos de um cidadão utilizando GPS e até mesmo conseguem mudar os conteúdos de e-mails durante sua rota rumo ao destinatário[2]. Algumas ferramentas são instaladas usando o mesmo tipo de malware e spyware perniciosos usados por criminosos online para roubar informações bancárias e de cartões de crédito[3]. Eles podem secretamente ligar webcams embutidas em laptops pessoais e microfones em telefones celulares que não estão sendo usados[4]. Outras ferramentas e serviços permitem que governos bloqueiem categorias inteiras de sítios Web, impedindo que cidadãos acessem informações essenciais. Estas ferramentas têm sido implementadas em uma escala tão massiva em determinados locais, que podem ser utilizadas para rastrear e espionar cada pessoa num país inteiro.

Este é um fenômeno que se espalha pelo planeta e que implica dúzias de corporações. Ao longo do ano passado – e em parte em resposta às insurgências que varreram o mundo árabe – , preocupações sobre este tipo de exportação foram amplificadas em reportagens na mídia e por organizações de defesa de direitos digitais, provocando um debate sobre os cursos de ação mais apropriados.

Por exemplo, foi revelado que a Narus, uma subsidiária da Boeing, vendeu ao Egito sofisticados equipamentos utilizados par vigilância[5]. É notável que a tecnologia da Narus também tenha sido descoberta em uso para conduzir a vigilância massiva e ilegal de norte-americanos, como parte dos programas de vigilância sem garantias contra os quais a EFF vem tomando medidas legais desde 2006.[6]
Descobriu-se que equipamentos da California BlueCoat Systems, Inc. estão em uso na Síria.[7]
A empresa alemã Trovicor supostamente vendeu tecnologia a uma dúzia de países no Oriente Médio e norte da África, incluindo Bahrein, onde dúzias de ativistas foram torturados antes e depois de serem mostradas transcrições de suas mensagens de texto e conversas por telefone, capturadas com esta tecnologia.[8]
Produtos da empresa canadense Netsweeper são usados pelos governos da Arábia Saudita, Qatar, Emirados Árabes e Iêmen para censurar uma série de conteúdos, inclusive sítios Web políticos. A empresa recusou-se a discutir o assunto, afirmando: “Não há nenhuma boa conversa que possamos ter”[9].
O SmartFilter, produto da McAfee/Intel, vendeu software para filtragem de conteúdos na web para diversos países, incluindo Bahrain, Emirados Árabes, Omã e Tunísia. Em todos os casos, o software foi utilizado para censura política.[10]
A Cisco Systems enfrenta litigâncias em Maryland e na Califórnia baseadas em sua suposta venda de equipamentos de vigilância para os chineses – para rastrear, monitorar e desta forma facilitar a prisão ou o desaparecimento de ativistas de direitos humanos e minorias religiosas que têm sido sujeitadas a enormes violações de direitos humanos.[11]
E a lista segue[12]....

A Electronic Frontier Foundation acredita que é hora de as empresas de tecnologia, especialmente aquelas que vendem equipamentos de vigilância e filtragem, tomarem providências e garantirem que não estão ajudando governos de outros países a cometerem violações de direitos humanos contra seus cidadãos.

A questão é complicada porque a maioria destas tecnologias é “dual use.” Isso significa que juntamente com a possibilidade de facilitar abusos de direitos humanos, quase todas estas tecnologias podem ser usadas para propósitos legítimos, tanto para os governos quanto para usuários não governamentais. Os usos não governamentais incluem investigação sobre segurança de redes e computadores, pesquisa e proteção, que podem ajudar bastante os usuários a proteger seus direitos e aumentar sua segurança. Os usos governamentais incluem aplicação da lei e segurança nacional sob circunstâncias justificadas, o que também pode ajudar a proteger os usuários. Frequentemente as funcionalidades técnicas para usos legítimos e ilegítimos são as mesmas. Isto torna difícil – se não impossível – usar o design ou descrição técnica, ou o uso potencial de uma ferramenta ou serviço, como a única base para determinar se estas foram usadas para violar direitos humanos. Por esta razão a EFF acredita que qualquer esforço para abordar a facilitação de violações de direitos humanos por tecnologias e serviços deve focar-se nos usos e nos usuários, não em descrições tecnológicas – e não deve ir além dos casos de vendas em que governos e entidades governamentais são os usuários finais. Caso contrário, é muito grande o risco de prejudicar usuários legítimos, e no final das contas fragilizar sua segurança e a proteção de seus direitos humanos.[13]

Como resultado, a EFF propõe que as empresas transitem por estes temas difíceis adotando um robusto programa “Conheça seu Cliente[14]”, similar àquele delineado nos atuais mecanismos de controle de exportação dos EUA, ou um programa similar ao que é requerido, para outros propósitos, pelo Foreign Corrupt Practices Act.[15] Manter o foco no usuário e no potencial (ou real) uso da tecnologia para violações de direitos humanos por governos – mais do que nas capacidades das tecnologias, por si só – representa um caminho mais direto para dar fim às violações de direitos humanos, gerando menos riscos colaterais.

A seguir, nós esboçamos uma proposta básica para que as empresas auditem seus clientes governamentais atuais e potenciais, num esforço para evitar que suas tecnologias e serviços sejam usados para abusos de direitos humanos. Há dois componentes-chave: transparência e padrões de “conheça seu cliente”. A mesma proposta básica poderia ser implementada através de ação voluntária, governamental, ou através de outros incentivos ou marcos regulatórios. A despeito de como seja implementado, nós acreditamos que este arcabouço pode ajudar tanto às empresas quanto ao público a alcançar uma visão mais clara de quem está usando estas tecnologias e como elas estão sendo usadas – e depois dar alguns passos básicos para evitar consequências terríveis como as

que já testemunhamos.[16]

TRANSPARÊNCIA

O primeiro passo é transparência. A indústria de vigilância e censura massivas como um todo tem sido notoriamente silenciosa e opaca, o que, por sua vez, permitiu sua proliferação sem maiores cuidados. Este caráter de opacidade e segredo chegou até mesmo a restringir, no passado, tentativas de fazer estar empresas prestarem contas sobre suas atividades. Por exemplo, o Government Accountability Office dos EUA não foi capaz de identificar quaisquer empresas fornecedoras destas tecnologias ao Irã, em parte porque os negócios são velados, segundo reportagens.[17]

Entretanto, como aprendemos recentemente, somente o fato de esta informação estar acessível ao escrutínio público já ajuda a promover mudanças.

Por exemplo, em agosto de 2011, depois de uma reportagem da Bloomberg sobre a empresa italiana Area SpA – que estava construindo um imenso centro de vigilância na Síria – irromperam protestos do lado de fora do escritório italiano e a Area SpA suspendeu a construção.[18] Fato parecido ocorreu em 2009, quando protestos sobre o envolvimento da Nokia Siemens Networks em venda de equipamentos para o Irã fizera com que a empresa vendesse sua subsidiária, agora chamada Trovicor, que constrói centros de vigilância massiva. Também em 2009 a Websense, empresa baseada na Califórnia que vende software de filtragem, adotou a política de não vender par governos estrangeiros depois que descobriu-se que seus produtos eram usados pelo governo do Iêmen.[19] Mais recentemente, em resposta a uma chamada de propostas publicada pelas autoridades paquistanesas, diversas empresas – incluindo a McAfee SmartFilter, que opera em vários países do Oriente Médio – responderam afirmando sua recusa em vender para o governo.[20]

A atenção da mídia aos mercados destas tecnologias também tem sido crucial. A cobertura midiática do chamado "Wiretapper's Ball," uma série de convenções organizadas pela Intelligence Support Systems (ISS), levou a diretora global de programas da ISS, Tatiana Lucas, a admitir que investigações como as que faz o Wall Street Journal "[fazem] as indústrias de armas norte-americanas intimidarem-se ante a perspectiva de desenvolver, e depois exportar, qualquer coisa que possa de alguma forma ser usada para apoiar a vigilância governamental.[21]„

Entretanto, não há muito mais que a imprensa possa fazer. A vasta maioria destas empresas recusa-se a sequer comentar sobre publicações de notícias. E o que é pior, as vendas destes perigosos sistemas são canalizadas através de subsidiárias e terceiras partes, deixando os jornalistas no escuro e as empresas prontas para negações plausíveis.

A EFF acredita que muito mais poderia ser feito diretamente pelas empresas para aumentar a transparência nestes mercados nebulosos.[22] As empresas podem começar imediatamente a oferecer informações voluntariamente, como parte de um processo mais amplo de transparência, tais como os que a Global Network Initiative (GNI) já põe em prática com relação a determinados temas, ou como uma iniciativa independente. Mais ainda, no caso de empresas recusarem-se a prestar contas, nós encorajamos o congresso norte-americano, países na União Europeia e autoridades locais a usar seus incentivos (nas contratação de serviços pelos governos, ou de outras formas), bem como seus poderes de investigação, para buscar respostas sobre potenciais cumplicidades em casos de abusos de direitos humanos que possam estar disponíveis em registros públicos. Várias entidades governamentais têm o poder de convocar audiências, emitir petições para obter documentos ou testemunhos e até mesmo conduzir investigações completas. Outras entidades governamentais deveriam considerar requerer transparência em temas de direitos humanos como condição para contratação pelo governo. Por conta de um trabalho importante feito pelas organizações de comunicação e mídia, já existe uma longa lista de empresas que merecem um questionamento mais profundo, embora nós suspeitemos que estas são apenas a ponta do iceberg.[23]

O ARCABOUÇO DA EFF PARA A ANÁLISE DE CLIENTES

[Nota: este esquema usa termos-chave - Tecnologias, Transação, Empresa e Governo - que estão definidos mais adiante e sempre aparecerão no texto iniciados com letras maiúsculas]

O arcabouço da EFF para a política "conheça seu cliente" tem dois componentes básicos:

1. Empresas que vendem Tecnologias de vigilância ou filtragem para Governos devem investiga proativamente e

"conhecer seu cliente" antes e durante uma Transação. Isso inclui, como ressaltamos abaixo, o uso que o cliente faz - ou que parece provável que fará - das Tecnologias. Nós sugerimos que se coloque o foco nos direitos humanos, de maneira similar à que já é requerida da maioria destas empresas sob o Foreign Corrupt Practices Act[24] para evitar suborno, e sob a regulação de exportação para evitar transferências de armas, assim como para outros propósitos;[25]

2. As Empresas devem abster-se de participar de Transações nas quais sua pesquisa para "conhecer seu cliente" revelar provas objetivas ou gerar preocupações plausíveis de que as Tecnologias providas pela Empresa a um Governo serão usadas para facilitar a violação de direitos humanos.

Este arcabouço básico seria mais eficaz se a empresas o implementassem de forma voluntária, assegurando desta forma a abordagem mais flexível possível, conforme as tecnologias mudam e conforme transformam-se as situações ao redor do mundo. A Nokia Siemens Networks já adotou uma Política de Direitos Humanos que incorpora algumas destas orientações.[26] A Websense adotou uma política anti-censura em 2009 e desde então tornou-se membro da Global Network Initiative, um grupo multissetorial cuja tarefa é proteger a liberdade de expressão e a privacidade, que já lida com algumas destas questões.[27]

Se as empresas não agirem por sua própria conta, e não o fizerem logo, com m compromisso convincente, então uma abordagem regulatória provavelmente será necessária. Em 2011, o Parlamento da União Europeia deu um passo rumo à prevenção de vendas de equipamento de vigilância a regimes autoritários. Membros do Congresso dos EUA também estão observando a questão de perto.[28] Na data em que publicamos este artigo, um projeto de lei foi apresentado pelo Congressista Chris Smith chamado "Global Online Freedom Act of 2012" contendo várias provisões positivas, incluindo requerimentos de transparência como parte de um devido processo de auditoria de direitos humanos, analisado de maneira independente por uma terceira parte e reportado publicamente.[29]

Em seguida elencamos as orientações básicas para assegurar que as empresas norte-americanas não sejam cúmplices de violações de direitos humanos ao redor do mundo, quer sejam seus esforços voluntários ou impostos por regulação.

RECOMENDAÇÕES: O PROCESSO DE DIREITOS HUMANOS "CONHEÇA SEU CLIENTE"

Investigar Afirmativamente a Empresa deve ter um processo, liderado por uma pessoa especificamente designada para isso, par dedicar-se a uma avaliação permanente sobre a possibilidade ou o fato de que as Tecnologias ou Transação sejam – ou estejam sendo – usadas para ajudar, facilitar ou encobrir abusos de direitos humanos, conforme estes são definidos pelo principais instrumentos internacionais das Nações Unidas. Um bom modelo para isso pode ser a atual tendência entre as empresas de designar Diretores de Privacidade, que geralmente são funcionários de alto nível, em posições de poder, que asseguram que a empresa respeita a privacidade de seus clientes e de outras pessoas. Diretores de Direitos Humanos poderiam desempenhar papel similar com respeito aos impactos das atividades da empresa nesta área.[30]

A despeito da forma como é implementado, este processo deve ser muito mais do que simplesmente palavras ditas da boca para fora e precisa ser verificável (e verificado) p pessoas de fora da empresa. Este deve ser um compromisso institucional, com mecanismos reais implementados, incluindo-se aí ferramentas, treinamento e formação de pessoal, bem como a previsão de consequências para os funcionários quando o processo não for cumprido. Ele deve ser incluído na política e nos procedimentos operacionais de toda a empresa e comunicado aos parceiros comerciais, às instituições contratantes e ao público. Além disso, para construir transparência e consolidar uma comunidade mais ampla de empresas agindo para proteger os direitos humanos, uma Empresa que decida recusar (ou dar continuidade a) serviços com base nestes padrões deve, quando possível, tornar sua decisão pública, de modo que outras empresas beneficiem-se desta avaliação.

O PROCESSO DEVE INCLUIR, NO MÍNIMO:

1. REPRESENTAÇÕES. Revisão do que afirma o Governo que faz a compra e do que os agentes de Governo e os funcionários da empresa estão dizendo sobre o uso das tecnologias, tanto antes quanto durante qualquer transação. Isto inclui, entre outras coisas, revisão de materiais de vendas e marketing, discussões e questões técnicas, apresentações, especificações técnicas e contratuais,discussões sobre customização e treinamento, bem como discussões e requisições sobre suporte técnico e atualizações. Algumas das provas mais problemáticas no caso da Cisco são as apresentações que foram feitas pelos funcionários da empresa, que inegavelmente fazem marketing sobre a Tecnologia e o suporte oferecidos ao Governo da China na repressão aos

praticantes do Falun Gong.[31]

2. POSSIBILIDADES E MITIGAÇÃO. Revisão das possibilidades oferecidas pela Tecnologia para a violação de direitos humanos e consideração de possíveis medidas de mitigação, tanto técnicas quanto contratuais.

3. CUSTOMIZAÇÃO E SERVIÇOS A LONGO PRAZO. Revisão de quaisquer requisições (ou demandas) de customização, bem como de serviços de mais longo prazo, atualizações e outros arranjos.

4. PROTEÇÕES LEGAIS. Revisão das leis, regulação e práticas do Governo relativas a vigilância e filtragem, incluindo-se interceptação de comunicação, acesso a comunicações arquivadas, requerimentos quanto ao devido processo legal e outros processos legais relevantes, como parte da análise de risco sobre como as Tecnologias podem ser usadas – para o bem e para o mal. Por exemplo, em sua política de direitos humanos a Nokia Siemens diz que só proverá capacidades para a interceptação legal da rede (i.e. vigilância) que forem requeridas legalmente e "baseadas em padrões claros e em fundamentos transparentes na lei e na prática".

5. INFORMAÇÃO EXTERNA. Revisão dos relatórios de direitos humanos do Departamento de Estado dos EUA[32], de relatórios relevantes das Nações Unidas, e de outros relatórios plausíveis sobre o Governo, incluindo notícias ou outros relatos de fontes não governamentais ou de fontes locais que indiquem se o Governo utiliza recursos de vigilância para conduzir violações de direitos humanos. Onde for possível, isso deve incluir a criação de um processo através do qual os indivíduos impactados pela Tecnologia e aqueles que fazem denúncias possam prover informação direta à empresa –, garantindo assim segurança àqueles que reportarem questões e um caminho para que a informação possa ser revisada e ações possam ser tomadas.

Abster-se de Participação: a Empresa não deve participar – ou continuar sua participação – em uma Transação, ou prover a Tecnologia, se for razoavelmente previsível que a Transação ou Tecnologia vai facilitar a violação de direitos humanos pelo Governo direta ou indiretamente, incluindo-se:

1. USO. A parte da Transação na qual a Empresa está envolvida ou a Tecnologia específica a ser provida inclui construção, customização, configuração o integração em um sistema que é sabidamente usado para violações de direitos humanos, ou quando este uso for razoavelmente previsível.

2. USUÁRIO ESPECÍFICO. O setor do Governo que está envolvido na Transação ou que esteja supervisionando as Tecnologias tenha sido identificado como violador de direitos humanos usando ou baseando-se em Tecnologias similares, direta ou indiretamente.

3. HISTÓRICO GERAL DO GOVERNO. O histórico geral do Governo na área de direitos humanos gera preocupações legítimas de que a Tecnologia ou Transação será utilizada para facilitar violações de direitos humanos.

4. AÇÕES DO GOVERNO. O Governo recusa-se a incorporar termos contratuais confirmando o uso pretendido das Tecnologias, recusa-se a permitir a inspeção suficiente sobre seu uso ou dá sinai sobre a utilização – pretendida ou em curso – das Tecnologias para a violação de direitos humanos.

Definições-chave e escopo do processo quem deve seguir estes passos? O escopo é, de fato, bem estreito – Empresas envolvidas em Transações para vender, alugar ou prover de qualquer outra forma Tecnologias a Governos, definidos como segue:

1."Transação" inclui todas as vendas, leasings, aluguéis ou outros tipos de arranjo onde uma Empresa, em troca de qualquer tipo de pagamento ou outra recompensa, incluindo-se a possibilidade de operar naquele país, provê ou assiste no provimento de Tecnologias, recursos humanos ou apoio não tecnológico a um Governo. Isto também inclui o provimento de qualquer tipo de suporte tais como atualizações de software ou hardware, consultoria ou serviços similares.

2. "Tecnologias" inclui todos os sistemas, serviços, hardware, software, consultoria e suporte passíveis de serem utilizados para vigiar terceiros ou fazer filtragem, incluindo-se, ma não limitando-se, a tecnologias que interceptam comunicações, registram atividades do usuário e suas informações, farejam pacotes ou fazem inspeção profunda de pacotes, aparatos e sistemas de biometria, sistemas de votação e medidores de uso. "Tecnologias" inclui especificamente qualquer serviço, customização, apoio ao cliente e paths ou componentes para atualizações.

3. "Empresa" inclui subsidiárias, joint ventures (incluindo-se joint ventures diretamente com entidades governamentais), e outras estruturas corporativas nas quais a Empresa tem partes significativas ou controle operacional.

4. "Governo" inclui governos formais, reconhecidos, englobando também Estados membros das Nações Unidas. Também inclui entidades governantes ou com status de governo, como o Partido Comunista da China ou o Talibã – e outras entidades não governamentais que efetivamente exercem poderes de governo sobre um país ou parte de um país. Para estes propósitos, "Governo" inclui vendas indiretas através de um agente, contratante ou outro intermediário (ou múltiplos intermediários) se a Empresa está ciente ou devesse saber que o receptador final, usuário ou beneficiário da tecnologia é um Governo. A Export Administration Regulations[33] (EAR) e a FCPA[34] podem prover orientação mais específica sobre estas determinações.

Este arcabouço, evidentemente, não é a única opção razoável para abordar o problema. Se levarmos em conta os passos que estas grandes empresas que competem nestes mercados já precisam dar – sob leis de exportação, o Foreign Corrupt Practices Act, entre outras – esta é uma inclusão relativamente pequena. Mesmo que algumas pessoas possam argumentar que pressionar empresas tecnológicas norte-americanas e as multinacionais sobre as quais os EUA têm jurisdição para que tenham sólidos programas de direitos humanos dará uma vantagem competitiva a empresas que não têm tal programa, o mesmo é verdade no que diz respeito às leis anti-suborno. Se podemos esperar que estas grandes empresas não façam negócios através de subornos – mesmo que algumas de suas concorrentes o façam – , também é razoável pedir que elas não façam negócios que resultem no favorecimento da repressão.

CONCLUSÃO

Nenhuma empresa razoável, e certamente nenhuma no Vale do Silício, quer ser conhecida como uma empresa que ajuda a facilitar violações de direitos humanos. Há numerosas maneiras pelas quais as empresas podem assegurar que as ramificações dos direitos humanos sejam consideradas em suas decisões de negócios. Enquanto a EFF defende a adoção de um marco que primeiramente garanta transparência e depois coloque o foco da tomada de decisões na abordagem "conheça seu cliente", pode haver outras formas de assegurar que empresas assumam responsabilidade pelos usos que governos fazem de suas tecnologias. Quaisquer que sejam os passos que elas deem, com ou sem a pressão de legisladores e reguladores, é hora de as empresas de tecnologia adotarem medidas reais para assegurar que não sirvam como "pequenos ajudantes da repressão".

Este artigo foi originalmente publicado pela EFF em: https://www.eff.org/node/70462

---

1. Ben Elgin e Vernon Silver, "The Surveillance Market and Its Victims," Bloomberg, 20 de dezembro de 2011 - http://www.bloomberg.com/data-visualization/wired-for-repression/

2. Vernon Silver, "Post-Revolt Tunisia Can Alter E-mail With 'Big Brother' Software," Bloomberg, 12 de dezembro de 2011 - http://www.bloomberg.com/news/ 2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html.

3. Jennifer Valentino-DeVries, "Surveillance Company Says It Sent Fake iTunes, Flash Updates," Wall Street Journal, 21 de novembro de 2011 - http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent...

4. Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear,"Bloomberg, novembro de 2011- http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm...

5. Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," Huffington ost, 28 de janeiro de 2011 - www.huffingtonpost.com/timothy-karr/one-us-corporation-role_b_815281.html

6. Para mais informações sobre os casos da EFF, ver: https://www.eff.org/issues/nsa-spying

7. Jillian C. York, "Government Internet Surveillance Starts With Eyes Built in the West," Electronic Frontier Foundation, 2 de setembro de 2011, https://www.eff.org/deeplinks/2011/09/government- internet-surveillance-starts-eyes-built

8. Vernon Silver e Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," Bloomberg,

22 de agosto de 2011 - http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-rout...

9. Nicki Thomas and Amy Dempsey, “Guelph-based software censors the Internet in the Middle East,” Toronto Star, 12 de junho de 2011 - http://www.thestar.com/news/article/1007399-guelph-based-software-censor...

10. Paul Sonne and Steve Stecklow, “U.S. Products Help Block Mideast Web,” Wall Street Journal, March 27, 2011, http://online.wsj.com/article/SB10001424052748704438104576219190417124 22...

11. Rainey Reitman, “Cisco and Abuses of Human Rights in China: Part 1,” Electronic Frontier Foundation, August 22, 2011, https://www.eff.org/dee-plinks/2011/08/cisco-and-abuses-human-rights-chi...

12. A EFF continua a monitorar casos de venda de tecnologias de vigilância a regimes autoritários. Ver em https://www.eff.org/issues/mass-surveillance-technologies.

13. Falando claramente, com base na experiência da EFF – desde os anos 90, quando atuou para liberar de restrições às exportações tecnologias de encriptação,e mais recentemente, no seu trabalho para libertar as tecnologias de comunicação do efeito combinado de medidas restritivas à exportação e regimes de sanção, nós temos graves preocupações sobre este tema, e provavelmente nos oporíamos à extensão ou implementação de uma abordagem regulatória baseada unicamente em aspectos tecnológicos, no contexto das tecnologias de vigilância e/ou filtragem de conteúdos.

14. Na realidade, diferente de alguns dos outros lugares onde é usado, o “know your customer” é uma ideia razoável, no contexto específico das vendas de tecnologias sofisticadas para governos, em que pod ser usadas para facilitar violações de direitos humanos em países onde a repressão é uma possibilidade concreta.

15. Ver : United States Department of Justice, Foreign Corrupt Practices Act, http://www.justice.gov/criminal/fraud/fcpa/

16. A Global Network Initiative - uma iniciativa multissetorial que trabalha com empresas buscando evitar ou minimizar censura - já começou a implementar um programa que contém alguns destes mesmos elementos no contexto das tecnologias de vigilância e filtragem

17. Ver Ben Elgin, Vernon Silver, e Alan Katz, “Iranian Police Seizing Dissidents Get Aid of Western Companies,” 30 de outubro de 2011, Bloomberg, http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissiden...

18. Vernon Silver e Ben Elgin, “Torture in Bahrain Becomes Routine With Help From Nokia Siemens,” Bloomberg, Augusto de 2011, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-rout...

19. Blog da Websense, “Websense Issues Statement on Use of its URL Filtering Technology by ISPs in Yemen,” 17 de agosto de 2009, http://community.websense.com/blogs/websense features/archive/2009/08/17/websense-issues-statement-on-use-of-its-url-filtering-technology-by-isps-in-yemen.aspx

20. Maira Sutton, “Companies Respond to Pakistan’s Internet Censorship Proposal,” Electronic Frontier Foundation, março de 2012, https://www.eff.org/deeplinks/2012/03/companies-respond-pakistans-nation...

21. Jennifer Baker, “Surveillance companies should not sell to despots says EU,” IDG, 10 de dezembro de 2011, http://www.pcworld.idg.com.au/article/409841/surveillance_tech_companies...

22. Governos repressivos também podem demandar que as empresas entreguem as informações de seus clientes obtidas na prestação de seus serviços e nas relações com os usuários. Isto também pode ajudar governos repressivos a cometer violações de direitos humanos, mas não é um fato abordado neste artigo. Aqui nos focamos unicamente na venda de tecnologias aos governos para fins de vigilância e censura.

23. A lista da Privacy International de provedores de tecnologias de vigilância é o documento mais elucidativo até o momento: https://www.privacyinternational.org/big-brother-incorporated/countries

24. N.E.: legislação anti-corrupção implementada pelo governo dos EUA em 1977. Ver em http://www.justice.gov/criminal/fraud/fcpa/

25. Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/textidxc=ecfr&sid=b598042103e95c10c... (acessado em 9 de fevereiro de 2012).

26. A Nokia Siemens Networks adotou uma política de direitos humanos em agosto de 2010. Ver: http://ecfr.gpoaccess.gov/cgi/t/text/text-idxc=ecfr&sid=b598042103e95c10...

27. Política anti-censura da Websense: https://www.websense.com/content/censorship-policy.aspx e Global Network Initiative: http://globalnetworkinitiative.org/

28. Vernon Silver, “EU Curbs Export of Surveillance Systems,” Bloomberg, 27 de setembro de 2011, http://www.bloomberg.com/news/2011-09-27/eu-curbs-export-of-surveillance.... Ver também o comentário da EFF: https://www.eff.org/deeplinks/2011/10/eu-parliament-takes-first-step-ban...

29. H.R. 3605: Global Online Freedom Act of 2011, http://www.govtrack.us/congress/bills/112/hr3605

30. Kenneth A. Bamberger e Deirdre K. Mulligan, “New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States,” Law and Policy (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087

31. Sarah Lai Stirland, “Cisco Leak: ‘Great Firewall’ of China Was a Chance to Sell More Routers,” Wired, May 20, 2008, http://www.wired.com/threatlevel/2008/05/leaked-cisco-do/

32. U.S. Department of State, Human Rights Reports, http://www.state.gov/j/drl/rls/hrrpt/ (acessado em 9 de fevereiro de 2012).

33. Bureau of Industry and Security U.S. Department of Commerce, Export Administration Regulations, http://www.bis.doc.gov/policiesandregulations/index.htm#ear

34. Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/textidx?c=ecfr&sid=b598042103e95c10...

Categoria:

- poliTICs 12