

# Human Rights and Technology Sales:

How Corporations Can Avoid Assisting Repressive Regimes

By Cindy Cohn, Trevor Timm, & Jillian C. York

April 2012



## **Background**

For years, there has been ample evidence that authoritarian governments around the world are relying on technology produced by American, Canadian, and European companies to facilitate human rights abuses, and the current indication is that the trend is growing. From software that enables the filtering and blocking of online content to tools that help governments spy on their citizens, many such companies are actively serving autocratic governments as "repression's little helper."

The reach of these technologies is astonishingly broad: governments can listen in on cell phone calls, use voice recognition to scan mobile networks, use facial recognition to scan photographs online and offline, read emails and text messages, track a citizen's every movement using GPS, and can even *change* email contents while en route to a recipient. Some tools are installed using the same type of malicious malware and spyware used by online criminals to steal credit card and banking information. They can secretly turn on webcams built into personal laptops and microphones in cell phones not being used. Other tools and services allow for governments to block entire categories of websites, preventing citizens from accessing vital information. And these tools are being implemented on such a massive scale in some places that they can be used to track and spy on every person in an entire country.

This is a phenomenon that spans the globe and implicates dozens of corporations. Over the past year, and partly in response to the uprisings that have swept the Arab world, concerns about these exports have been amplified in media reports and by digital rights organizations, sparking a debate as to the appropriate course of action.

- For example, Narus, a Boeing subsidiary, was revealed to have sold to Egypt sophisticated equipment used for surveillance.<sup>5</sup> Notably, Narus' technology has also been discovered in use to conduct the illegal mass surveillance of Americans as part of the warrantless surveillance programs that EFF has been suing to stop since 2006.<sup>1</sup>
- California's BlueCoat Systems, Inc. was found to have equipment being used in Syria.<sup>6</sup>
- Germany-based Trovicor has reportedly sold this technology to a dozen Middle Eastern and North African countries, including Bahrain, where dozens of activists were tortured before and after being shown transcripts of their text messages and phone conversations captured from this technology.<sup>7</sup>
- Canadian company Netsweeper's products are used by the governments of Saudi Arabia, Qatar, UAE, and Yemen to censor a variety of content, including political sites. The company has refused to discuss the matter, stating, "There's no good conversation for us to have."

<sup>&</sup>lt;sup>1</sup> For more information on EFF's cases, see: https://www.eff.org/issues/nsa-spying

- SmartFilter, a product of McAfee/Intel, has sold web filtering software to several countries, including Bahrain, UAE, Oman, and Tunisia. In all cases, the software was then used for political censorship.<sup>9</sup>
- Cisco Systems is facing litigation in both Maryland and California based on its alleged sales of surveillance equipment to the Chinese to track, monitor and otherwise facilitate the arrest, detention, or disappearance of human rights activists and religious minorities who have been subjected to gross human rights violations.<sup>10</sup>

And the list goes on and on."

The Electronic Frontier Foundation believes that it's time for technology companies, especially those selling surveillance and filtering equipment, to step up and ensure that they aren't assisting foreign governments in committing human rights violations against their own people.

The issue is complicated because most of these technologies are "dual use." This means that along with the ability to facilitate human rights abuses, nearly all of these technologies can be used for legitimate purposes for both government and nongovernment users. Non-governmental uses include network and computer security investigation, research and protection, which can greatly help users protect their human rights and increase their security. Governmental uses include law enforcement and national security under properly justified circumstances, which can also help protect users. Often the technical functionality for legitimate uses and illegitimate ones is the same. This makes it difficult, if not impossible, to use the design or technical description, or potential use of a tool or service, as the sole basis for determining whether it is being used for human rights abuses. For this reason, EFF believes that any effort to address the facilitation of human rights abuses by technologies or services must focus on use and users, not technology descriptions, and should not reach beyond sales where governments and governmental entities are the ultimate end users. Otherwise, the risk of harming legitimate users, and ultimately decreasing their security and human rights protection, is too great. iii

As a result, EFF proposes companies navigate these difficult issues by adopting a robust *Know Your Customer* program, similar to the one outlined in the current U.S. export controls or a program similar to that required by the Foreign Corrupt Practices Act for

<sup>&</sup>lt;sup>ii</sup> EFF continues to track instances of surveillance technology being sold to authoritarian regimes. See https://www.eff.org/issues/mass-surveillance-technologies.

iii To be clear, based on EFF's experience both in the 1990s to free encryption technologies from export restrictions, and more recently, in working to free communications technologies from the combined effect of export restrictions and sanctions regimes, we have grave concerns about and would likely oppose extending or implementing a solely technology-based regulatory approach in the context of surveillance or filtering technologies.

other purposes. <sup>11iv</sup> Putting the focus on user and potential (or actual) use of the technology for human rights abuses by governments—rather than on the capabilities of the technology itself—presents a more direct path to stopping human rights abuses, and one with fewer collateral risks.

Below, we outline a basic proposal for companies to audit their current and potential governmental customers in an effort to prevent their technologies and services from being used for human rights abuses. It has two key components: transparency and "know your customer" standards. The same basic proposal could be implemented through voluntary action, governmental or other incentives or regulatory or legal frameworks. Regardless of how it is implemented, however, we believe this framework can help both the public and the companies get a clearer picture of who is using these technologies and how they are being used and then take some basic steps to prevent horrible outcomes like the ones we've witnessed."

#### **Transparency**

The first step is transparency. The mass surveillance and censorship industry as a whole has been notoriously secretive, which has, in turn, allowed it to proliferate without meaningful safeguards. This secrecy has even stifled past attempts at holding these companies accountable. For example, the Government Accountability Office in the U.S. was unable to identify any companies supplying the technology to Iran, in part because the business is so secretive, according to the report.<sup>12</sup>

But as we have learned recently, just having this information in the public eye can, by itself, help create change.

For example, in August 2011, after a *Bloomberg* story about Italian company Area SpA—which was constructing a massive surveillance center in Syria—protests sprung up outside their Italian office and Area SpA halted construction. Similarly in 2009, after protests over Nokia Siemens Networks' involvement in selling equipment to Iran, the company sold their subsidiary, now called Trovicor, which builds mass surveillance centers. Also in 2009, Websense, a California-based company that sells filtering software, adopted a policy of not selling to foreign governments after its products were found to be used by the government of Yemen. Most recently, in response to a Request For Proposals (RFP) published by Pakistani authorities, several companies—

**ELECTRONIC FRONTIER FOUNDATION** 

<sup>&</sup>lt;sup>iv</sup> In fact, unlike some of the other places where it is used, "know your customer" is a reasonable idea in the limited context of sales of sophisticated technologies to governments that can be used to facilitate human rights abuses to countries at risk for repression.

v The Global Network Initiative—a multi-stakeholder initiative that works with companies seeking to prevent or minimize censorship—has already started implementing a program that contains some of these same elements in the context of filtering and surveillance technologies.

including McAfee SmartFilter, which is in use in several Middle Eastern countries—responded by stating a refusal to sell to the government.<sup>15</sup>

The media's attention to the marketplaces for these technologies has also been crucial. Coverage of the so-called "Wiretapper's Ball," a series of conventions run by Intelligence Support Systems (ISS), led the world program director for ISS, Tatiana Lucas, to admit that investigations like the *Wall Street Journal*'s "[make] U.S. manufacturers gun shy about developing, and eventually exporting, anything that can remotely be used to support government surveillance." <sup>16</sup>

But there is only so much the press can do. A vast majority of these companies refuse even to comment to news outlets. Worse, the sales of these dangerous systems are funneled through subsidiaries and third parties, leaving journalists in the dark, and the companies with plausible deniability.

EFF believes there is much more that could be done by companies directly to increase transparency into these shadowy markets. Companies can immediately begin to volunteer this information as part of an overall transparency report process, such as the process GNI already runs for certain issues, or as a stand-alone one. In addition, or should they refuse to do so, we encourage the U.S. Congress, individual E.U. countries, and local law enforcement to use their incentives (through government contracting and otherwise) as well as investigatory powers to seek answers about potential complicity in human rights abuses available on the public record. Various governmental entities have the power to hold hearings, issue subpoenas for documents or testimony and even conduct full investigations. Other governmental entities should consider requiring human rights transparency as a condition of government contracting. Because of the important work done by media organizations, there is already a long list of companies worthy of further questioning, although we suspect those are only the tip of the iceberg.

Repressive governments also demand that companies turn over user information that the company gathers as part of providing its services to users. This can can also assist governments in committing human rights abuses, but is not addressed in this paper. Here, we focus solely on companies selling technologies to governments for the purpose of surveillance and censorship.

vii Privacy International's list of surveillance technology providers is the most comprehensive available thus far: https://www.privacyinternational.org/big-brother-incorporated/countries.

## **EFF's Framework for Auditing Customers**

[Note: This framework uses key terms — Technologies, Transaction, Company and Government — which are defined at the bottom and capitalized throughout]

EFF's substantive framework for "know your customer" has two basic components:

- Companies selling surveillance or filtering Technologies to Governments must affirmatively investigate and "know your customer" before and during a Transaction. This includes, as noted below, the use the customer makes or seems reasonably likely to make of the Technologies. We suggest focusing on human rights in a similar way to what most of these companies are already required to do under the Foreign Corrupt Practices Act to prevent bribery and the export regulations to prevent arms transfers as well as for other purposes,<sup>17</sup> and
- 2. Companies must refrain from participating in Transactions where their "know your customer" investigations reveal either objective evidence or credible concerns that the technologies provided by the Company to a Government will be used to facilitate human rights violations.

This basic framework would be most effective if companies implement it voluntarily, thereby ensuring the most flexible approach as technologies change and situations around the world shift. Nokia Siemens Networks has already adopted a Human Rights Policy that incorporates some of these guidelines. Websense adopted an anticensorship policy in 2009 and has since become a member of the Global Network Initiative (GNI), a multi-stakeholder group tasked with protecting freedom of expression and privacy that is already tackling some of these questions. ix

But if companies don't act on their own, and don't act soon and with convincing commitment, then some regulatory approach is likely going to be necessary. In 2011, the EU Parliament took a step toward preventing sales of surveillance equipment to authoritarian regimes. Members of the U.S. Congress are watching closely as well. As of the date of this white paper, a bill introduced by Representative Chris Smith called the Global Online Freedom Act of 2012 contains numerous good provisions, including transparency requirements as part of a human rights due diligence process independently assessed by a third party and reported publicly.

viii Nokia Siemens Networks adopted a human rights policy in August 2010. See PDF: http://ecfr.gpoaccess.gov/cgi/t/text/text-

 $idx?c = ecfr\&sid = b598042103e95c10c396b0140e0620b7\&rgn = div9\&view = text\&node = 15:2.1.3.4.21.\\0.1.7.22\&idno = 15.$ 

ix Websense's anti-censorship policy: https://www.websense.com/content/censorship-policy.aspx; the Global Network Initiative: http://globalnetworkinitiative.org/.

The following are basic guidelines to ensure that U.S. companies aren't complicit in the abuse of human rights around the world, regardless of whether efforts are voluntary or through regulation.

# Recommendations: "Know Your Customer" Human Rights Process

Affirmatively Investigate: The Company must have a process, led by a specifically-designated person, to engage in an ongoing evaluation of whether Technologies or Transaction will be, or are being used to aid, facilitate or cover up human rights abuses, as defined by the core international human rights instruments of the United Nations. A good model for this may be the trend to appoint Chief Privacy Officers, who are generally empowered, high-level employees who ensure that the company respects the privacy rights of its customers and others. Officers could perform a similar role with respect to the human rights impacts of the companies activities.

Regardless of the form, this process needs to be much more than lip service and needs to be verifiable (and verified) by outsiders. It needs to be an organizational commitment, with real mechanisms in place including tools, training and education of personnel and career consequences for personnel when the process is not followed. It must be included in the operational policy and procedures throughout the company and communicated to business partners, contractors, and the public. In addition, in order to build transparency and a broader community of companies acting to protect human rights, a Company that decides to refuse (or continue) further service on the basis of these standards should, where possible, report that decision publicly so that other companies can have the benefit of their evaluation.

The process should include, at a minimum:

1. Representations. Review of both what the purchasing Government and Government agents and the Company personnel and agents are saying about the use of the Technologies, both before and during any Transaction. This includes, among other things, review of sales and marketing materials and discussions, technical discussions and questions, presentations, technical and contractual specifications, customization and training discussions and technical support and upgrade conversations or requests. Some of the most troubling evidence in the Cisco case are the presentations made by Cisco employees that are plainly marketing Technology and giving technical support to the Government in repressing the Falun Gong.<sup>21</sup>

- 2. <u>Capabilities and Mitigation.</u> Review of the capabilities of the Technology for human rights abuses and consideration of possible mitigation measures, both technical and contractual.
- 3. <u>Customization and Ongoing Services.</u> Review of any customization requests (or requirements) and ongoing service and upgrade and other arrangements.
- 4. <u>Legal Protections.</u> Review the Government's laws, regulations and practices regarding surveillance and filtering, including interception of communications, access to stored communications, due process requirements, and other relevant legal process as part of the assessment of risk of how the Technologies may be used or misused. For instance, in the company's human rights policy, Nokia Siemens says that it will only provide core lawful intercept (i.e. surveillance) capabilities that are legally required and are "based on clear standards and a transparent foundation in law and practice."
- 5. Outside Information. Review U.S. State Department annual human rights reports, <sup>22</sup> relevant U.N. Reports, and other credible reports about the Government, including news or other reports from nongovernmental sources or local sources that indicate whether the Government engages in the use or misuse of surveillance capabilities to conduct human rights abuses. Where possible, this should include the creation of a process by which individuals impacted by the Technology and whistleblowers can provide direct information to the company, including security for those reporting issues and a path for that information can be reviewed and acted upon.

**Refraining from Participation:** The Company must not participate in, or continue to participate in a Transaction or provide a Technology if it appears reasonably foreseeable that the Transaction or Technology will directly or indirectly facilitate human rights violations by the Government, including:

- 1. <u>Use.</u> The portion of the Transaction that the Company is involved in or the specific Technology provided includes building, customizing, configuring or integrating into a system that is known or is reasonably foreseen to be used for human rights violations.
- 2. <u>Specific User.</u> The portion of the Government that is engaging in the Transaction or overseeing the Technologies has been recognized as committing human rights abuses using or relying on similar Technologies, either directly or indirectly.
- 3. Overall Government Record. The Government's overall record on human rights generally raises credible concerns that the Technology or Transaction will be used to facilitate human rights abuses.
- 4. <u>Government actions.</u> The Government refuses to incorporate contractual terms confirming the intended use or uses of the Technologies, refuses to

allow sufficient auditing of their use, or indicates an intent to or actual use of Technologies for human rights abuses.

**Key Definitions and the Scope of the Process:** Who should undertake these steps? The field is actually pretty small: Companies engaging in Transactions to sell, lease or otherwise provide Technologies to Governments, defined as follows:

- "Transaction" includes all sales, leases, rental or other types of arrangements where a Company, in exchange for any form of payment or other consideration, including the ongoing ability to operate in that country, either provides or assists in providing Technologies, personnel or non-technological support to a Government. This also includes providing of any ongoing support such as software or hardware upgrades, consulting or similar services.
- 2. "Technologies" includes all systems, services, hardware, software, consulting, and support that are reasonably likely to be used to surveil third parties or filter, including but not limited to technologies that intercept communications, log user activities and information, packet-sniff or engage in deep packet inspection, biometrics devices and systems, voting systems, and smart meters. "Technologies" specifically includes any service, customization, customer support or upgrade paths or components.
- 3. "Company" includes subsidiaries, joint ventures (including joint ventures directly with government entities), and other corporate structures where the Company has significant holdings or has operational control.
- 4. "Government" includes formal, recognized governments, including State parties to the United Nations. It also includes governing or government-like entities, such as the Chinese Communist Party or the Taliban and other nongovernmental entities that effectively exercise governing powers over a country or a portion of a country. For these purposes "Government" includes indirect sales through a broker, contractor, or other intermediary or multiple intermediaries if the Company is aware or should know that the final recipient, user or beneficiary, of the Technology is a Government. The Export Administration Regulations (EAR), 23 and FCPA 24 can provide more specific guidance for these determinations.

This framework isn't the only reasonable option for addressing the problem, of course. Yet given the steps that these large companies who compete in these markets already have to take—under the export laws, the Foreign Corrupt Practices Act and otherwise—this is a relatively small addition. While some may argue that pushing U.S. and multinational tech companies over which the U.S. has jurisdiction to have a strong human rights programs will give a competitive advantage to companies that don't institute one, the same is true about the anti-bribery laws. If these big companies can be

expected not to get business through bribes even though some of their foreign competitors do, it's reasonable to ask them not to conduct business that would result in enabling repression either.

#### Conclusion

No reasonable company, and certainly none in Silicon Valley, wants to be known as the company that helps facilitate human rights abuses. There are numerous ways in which companies can ensure human rights ramifications are considered in their business decisions. While EFF advocates for a framework that first ensures transparency and then centers decision-making on a "know your customer" approach, there may be other ways to ensure companies take responsibility for the uses that governments make of their technologies. Whatever steps they take, and with or without push from lawmakers or regulators, it's time for tech companies to take real steps to ensure that they aren't serving as "repression's little helpers."

#### **Notes**

<sup>&</sup>lt;sup>1</sup> Ben Elgin and Vernon Silver, "The Surveillance Market and Its Victims," *Bloomberg*, December 20, 2011, http://www.bloomberg.com/data-visualization/wired-for-repression/.

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

<sup>&</sup>lt;sup>3</sup> Jennifer Valentino-DeVries, "Surveillance Company Says It Sent Fake iTunes, Flash Updates," *Wall Street Journal*, November 21, 2011, http://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/.

<sup>&</sup>lt;sup>4</sup> Ben Elgin and Vernon Silver, "Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear," *Bloomberg*, November 3, 2011, http://www.bloomberg.com/news/2011-11-03/syria-crackdowngets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

<sup>&</sup>lt;sup>5</sup> Timothy Karr, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," *Huffington Post*, January 28, 2011, www.huffingtonpost.com/timothy-karr/one-us-corporations-role-\_b\_815281.html.

<sup>&</sup>lt;sup>6</sup> Jillian C. York, "Government Internet Surveillance Starts With Eyes Built in the West," *Electronic Frontier Foundation*, September 2, 2011, https://www.eff.org/deeplinks/2011/09/government-internet-surveillance-starts-eyes-built.

<sup>&</sup>lt;sup>7</sup> Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," *Bloomberg*, August 22, 2011, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

<sup>&</sup>lt;sup>8</sup> Nicki Thomas and Amy Dempsey, "Guelph-based software censors the Internet in the Middle East," *Toronto Star*, June 12, 2011, http://www.thestar.com/news/article/1007399--guelph-based-software-censors-the-internet-in-the-middle-east.

<sup>9</sup> Paul Sonne and Steve Stecklow, "U.S. Products Help Block Mideast Web," *Wall Street Journal*, March 27, 2011,

http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html.

- <sup>10</sup> Rainey Reitman, "Cisco and Abuses of Human Rights in China: Part 1," *Electronic Frontier Foundation*, August 22, 2011, https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1.
- <sup>11</sup> United States Department of Justice, *Foreign Corrupt Practices Act*, http://www.justice.gov/criminal/fraud/fcpa/ (accessed February 9, 2012).
- <sup>12</sup> Ben Elgin, Vernon Silver, and Alan Katz, "Iranian Police Seizing Dissidents Get Aid of Western Companies," October 30, 2011, *Bloomberg*, http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html
- <sup>13</sup> Vernon Silver and Ben Elgin, "Torture in Bahrain Becomes Routine With Help From Nokia Siemens," *Bloomberg*, August 22, 2011, http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.
- <sup>14</sup> Websense blog, "Websense Issues Statement on Use of its URL Filtering Technology by ISPs in Yemen," August 17, 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.
- <sup>15</sup> Maira Sutton, "Companies Respond to Pakistan's Internet Censorship Proposal," *Electronic Frontier Foundation*, March 13, 2012, https://www.eff.org/deeplinks/2012/03/companies-respond-pakistans-national-censorship-proposal.
- $^{16}$  Jennifer Baker, "Surveillance companies should not sell to despots says EU," IDG, December 10, 2011,

http://www.pcworld.idg.com.au/article/409841/surveillance\_tech\_companies\_should\_sell\_despots\_says\_eu/.

- <sup>17</sup> Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=b598042103e95c10c396b0140e0620b7&rgn=div9&view=text&node=15:2.1.3.4.21. 0.1.7.22&idno=15 (accessed February 9, 2012).
- <sup>18</sup> Vernon Silver, "EU Curbs Export of Surveillance Systems," *Bloomberg*, September 27, 2011, http://www.bloomberg.com/news/2011-09-27/eu-curbs-export-of-surveillance-systems.html. See also EFF's commentary: https://www.eff.org/deeplinks/2011/10/eu-parliament-takes-first-step-bans-sales.
- <sup>19</sup> H.R. 3605: Global Online Freedom Act of 2011, http://www.govtrack.us/congress/bills/112/hr3605.
- <sup>20</sup> Kenneth A. Bamberger and Deirdre K. Mulligan, "New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States," *Law and Policy* (2011), papers.ssrn.com/sol3/papers.cfm?abstract\_id=1701087.
- <sup>21</sup> 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/.
- <sup>22</sup> U.S. Department of State, Human Rights Reports, http://www.state.gov/j/drl/rls/hrrpt/ (accessed February 9, 2012).
- <sup>23</sup> Bureau of Industry and Security U.S. Department of Commerce, Export Administration Regulations, http://www.bis.doc.gov/policiesandregulations/index.htm#ear.
- <sup>24</sup> Electronic Code of Federal Regulations, Title 15: Commerce and Foreign Trade, http://ecfr.gpoaccess.gov/cgi/t/text/text-

 $idx?c = ecfr\&sid = b598042103e95c10c396b0140e0620b7\&rgn = div9\&view = text\&node = 15:2.1.3.4.21.\\0.1.7.22\&idno = 15 (accessed February 9, 2012).$