COMPANIES AS ACTORS

Robert Faris and Urs Gasser

Companies form the functional core of the Internet. The private sector owns a vast proportion of the physical infrastructure, produces the hardware and software that light up the network, develops innovative services and applications, acts as gateways for residential and business access to the Internet, and hosts the lion's share of content and information. Companies act as merchants, aggregate data and knowledge, serve as media outlets, and house the data and networks that digitally link communities around the globe. In contrast to the pre-Internet commercial world, a prime source of value for much of this activity is based on promoting and leveraging the pro-social urges and voluntary participation of users.

> ***Bringing together companies, rights advocates, investors, and academics to collectively defend against government overreach and advance international human rights standards, GNI aspired to responsible company decision making, collaborative learning, and policy engagement.***
>
> —COLIN M. MACLAY
> Dilemmas and Dialogue: GNI and the Transborder Internet

And while the constellation of businesses that participate in the Internet economy is vast and diverse, a modest number of very large firms dominate the action. Much, if not all, of this can be explained by economies of scale and network effects. Internet enterprises are bolstered by scale. For social networks, search algorithms, social media, content aggregation, advertising, physical infrastructure, and hardware and software development, there are inherent self-reinforcing advantages to being big. And with size comes power, responsibility, and scrutiny. Private companies are caught up in the midst of the most challenging and consequential policy questions facing the Internet: freedom of expression, privacy, surveillance, security, civil liberties online, net neutrality, access to broadband, cybercrime, and law enforcement. As the intermediaries between individuals, civil society, governments, and other companies, technology companies not only provide the playing field but are increasingly being called upon to referee the match. In countries that filter the Internet, ISPs are enlisted to implement the blocking. When governments seek information on Internet users, whether for legitimate law enforcement or to pursue political opposition, they turn to ISPs, cell phone carriers, social media platforms, and content hosts. And when civil society feels that online liberties, privacy protections, and security are not being upheld, they lobby the companies; at times with the support of sympathetic governments and at times demanding that companies provide a layer of protection from governments that are seen as predatory.

While there are segments of the Internet operated by public and non-profit entities—for example municipally-owned networks, government infrastructure, and systems run by schools and universities—these comprise a small portion of Internet traffic. A majority of Internet capacity and data flows are sustained by private owners and operators, and are shaped and maintained by a small number of commercial business models.

Subscription-based models support ISPs that connect businesses and residences to the Internet, as well as commercial software and many media and entertainment services, including news sites (e.g., the New York Times and Wall Street Journal) and video distributors (e.g., Netflix and digital access to cable channels). Online sales of merchandise, for example through Amazon and eBay, constitute a different model. A third model based on advertising revenue supports search engines, a wide range of online media, social media platforms, and other online content hosting services, including many of the biggest players (e.g., Google/YouTube, Yahoo!, Facebook, and Twitter).

While these business models are structurally different, they all rely on access to important personal data about their users. Data collection, aggregation, analysis, and sale is a key part of many companies' value proposition, whether to sell the data to other companies, to increase advertising revenue by better targeting of advertisements, or to provide better services to their customers. These business models, supported by user data and economies of scale, have combined to fuel the rapid growth of the Internet and the many benefits of digital activity, and in doing have also contributed to the tensions and unresolved conflicts that have arisen related to privacy, surveillance, security, and freedom of expression. In each of these areas, companies are brought into the fray. As intermediaries between governments and citizens, and between citizens and citizens, technology companies are drawn into serving several, sometimes competing functions: cooperating with law enforcement, protecting users against security breaches and the excessive prying by governments and others, and setting behavioral and content standards on their platforms (in effect creating their own laws).

In the realm of privacy, persistent unresolved tensions exist between website hosts, social media and social networking companies, and their users. This stems from data that is willingly shared by users—their location; love life; preferences in film, music, or food; and so on—and information that is gathered surreptitiously, for example by quietly tracking a user's web browsing habits. This jumps into the area of state surveillance when governments come looking for this same data. For governments, the cooperation of companies in pursuing criminal activity online is instrumental in their ability to govern digital activity. Companies then find themselves in the awkward position of balancing user privacy against the demands of law enforcement agents. For technology companies that live or die based on the continued participation of users, maintaining trust among their user base is critical. Pointing out to users that their privacy information might be shared with the government has never been a popular option for the marketing department. Pretending this doesn't exist is not viable either. A longstanding strategy for some companies has been to restrict cooperation to requests made with clear and specific legal authority. A more recent strategy is to make the entire process more transparent by publishing the type and quantity of law enforcement requests along with company responses.

> *In 2009, Google published the first transparency report; Twitter followed suit in 2012. Nearly a dozen companies are now releasing transparency reports, with more on the way.*
>
> —RYAN BUDISH
> Transparency Reporting

Companies have been lauded as protectors of free speech when pushing back against government content restrictions, criticized for enacting terms of service agreements that prohibit legally protected speech on their sites, faulted for too easily removing content at the request of others, and condemned for not going far enough to eliminate harmful speech from their platforms. Given the range and quantity of discussion on these platforms related to matters of political and social relevance, these private companies are acting as hosts for the networked public sphere. This newfound power instilled in intermediaries has the effect of transferring to them authority that has traditionally resided in the judiciary.

> ***As people are moving information previously hidden in locked file cabinets or safes into their personal clouds, companies have inadvertently gained unprecedented power over who can access and control information about individual citizens.***
>
> —DALIA TOPELSON
> The New Guard

In the area of security, most Internet users rely on a handful of technology companies that provide them with connectivity, serve their email, and host their content to also provide them with protection against online attacks, in an arrangement that Bruce Schneier describes as feudal.

Governments will continue to seek more effective control over cyberspace by enlisting help from companies, whether through coercion or voluntary action. A prime example is the makers of filtering and surveillance tools that have stepped forward to sell their products to governments around the world. Another set of smaller companies occupy the opposite end of the spectrum, developing products meant to prevent governments from accessing user information and helping users circumvent filtering.

> ***From the mid-2000s onwards, the Citizen Lab has documented numerous cases of products developed in North America and Europe being used for censorship and surveillance by governments with poor human rights records, and in some cases under international sanctions.***
>
> —RON DEIBERT AND MASASHI CRETE-NISHIHATA
> The Commercialization of Censorship and Surveillance

In this quasi-borderless world, the importance of the physical location of technology companies' personnel and servers is only growing over time. The social media monitoring apparatus of China is made possible only by having direct jurisdiction over the social media companies that do business there. Subject to filtering that prevents building a meaningful share of the market, foreign-hosted competitors are no longer viable alternatives in China. The United States government enjoys a similarly strong position for law enforcement agencies and regulators given the number of influential technology firms based there. Other countries such as India, Iran, and Vietnam have long pushed for greater control over foreign-based platforms that serve their citizens. For companies, this constitutes a momentous decision: whether to risk being shut out of growing markets or forced into making decisions that infringe on the civil liberties of their users.

There are many other contentious issues in the digital world that we do not take up in this report, some of which pit companies against one another. The debate over the future of copyright protections and digital media is far from resolved. Those that rely on the traditional content licensing and distribution industries are in conflict with online platforms that host user generated content and web-native services whose business models are built not on content licensing but rather on search, indexing, and aggregation. The patent wars continue to rage, touching all corners of the Internet and drawing in device and hardware makers as well as retailers, online platforms, software developers, and others. Interoperability is an ongoing concern as companies and governments continue to wrangle over technology standards. Another set of debates revolves around broadband markets and investments in physical infrastructure. In residential markets, entrants argue for access to last mile infrastructure controlled by incumbent telecommunication providers; the net neutrality debates generally divide broadband providers and content distributors.

The privately controlled core of the Internet generally co-exists amicably with the vast and growing stocks of public knowledge and social capital that reside online. This uneasy equilibrium may not last, particularly as political pressures mount for governments to be more proactive in addressing digital matters.

DILEMMAS AND DIALOGUE: GNI AND THE TRANSBORDER INTERNET

Colin M. Maclay

It has been less than a decade since Shi Tao was sentenced to a decade of hard labor by a Chinese court using data from his Yahoo! email account, Michael Anti's blog was deleted based on an informal law enforcement request to a Microsoft joint venture, and Google removed search results in accordance with Chinese law. These developments, which garnered significant public and private attention and concern, formed part of the inspiration to create the Global Network Initiative (GNI), a multi-stakeholder effort to protect and advance online expression and privacy through principles, implementation guidelines, and external accountability measures.

Bringing together companies, rights advocates, investors, and academics to collectively defend against government overreach and advance international human rights standards, GNI aspired to responsible company decision making, collaborative learning, and policy engagement. It promised a valuable complement to legislative solutions, which have made little progress and face challenges not only of jurisdiction, but also in responding to the dynamic nature of technology, companies, users, and governments. Rather than expecting compliance with existing laws, however, true success depended in part on companies actually pushing back against government requests for personal information or content removal—first by mitigating risks, but also by resisting demands by law enforcement in some cases, something no other multi-stakeholder initiative had attempted.

Since the GNI's inception, technology has helped topple governments, connectedness and online activity have skyrocketed, and concerns about privacy and freedom of expression have unfurled and deepened. Pressures on and expectations of companies have increased, and attention to their situation has broadened and mounted. Company reactions have varied, including start-ups embracing and established companies adopting expression and privacy issues as part of their identity (Twitter, Google, Yahoo!), joining GNI (Facebook, LinkedIn), denying any role (Cisco), or even closing their doors (Lavabit, Silent Circle). GNI has become more established and completed its first full round of external company assessments, increased substantially in number and diversity of participants, and is directing significant attention to policy engagement. Notably, it has also generated a significant strain of unofficial problem solving through its robust network.

The most recent revelations about widespread warrantless state surveillance with insufficient oversight have added new dimensions to the conversation, calling the activities of robust democracies into question and increasing concerns about the role of the companies that are core to connectivity, physical infrastructure, access to knowledge, collaborative and social networking platforms, and access to user information. The limitations of standard regulatory models for this inherently trans-jurisdictional medium have been further exposed, demonstrating that extending national legal requirements across borders is hard, whether trying to protect civil liberties in other jurisdictions or to enforce domestic laws on foreign platforms. The result of this regulatory patchwork is that security agencies can gather data that would be otherwise legally inaccessible to them.

The limitations to transparency around government collection of user information and constraints on what companies can disclose exacerbate the challenges to policymakers, users, and advocates to developing an empirical understanding of government and company behavior. In addition to encouraging more transparency, GNI has endeavored to compensate for this gap through third-party expert assessments of company processes and their actual practices. The Snowden revelations have added to the challenge of National Security Letters (which include a gag order), sowing frustration and distrust among allies (actual and potential), even as companies and civil society seem to need each other more than ever. Indeed, EFF left GNI in October 2013 citing the inability to carry out a full and honest dialogue given the government constraints on company reporting, an indictment of the legal regime rather than the private sector. In an otherwise forthcoming setting, there is an elephant in the room.

Once the concern of a select (or paranoid) few, privacy is now at the forefront for mainstream users and diverse civil society organizations. Companies are finally improving their own security practices and rethinking—and changing—data collection, transmission, and storage practices. Cloud and other online providers are facing the daunting business implications of user distrust, and governments are exploring nationalization of cloud services, which could either protect their citizens or expose them to even greater risk. Recognizing the fundamental nature of the threat at hand, disparate groups are also working collaboratively for policy reform in coalitions like We Need to Know, which illustrates a range of shared priorities and underscores the benefit of ongoing collaboration across communities. As governments feud (with each other and their citizens) and explore extreme measures (such as the new cloud platform proposal in Brazil), and legislators hold hearings on all sides of the issues, the importance of coalitions is clear. Some feel a palpable risk for Balkanization of the Internet.

While the trajectory of these developments is uncertain, there can be no doubt that that online privacy and free expression are very much at risk globally. NSA and FISA maybe the acronyms of the moment, but other governments are likely to be implicated or to imitate this behavior. Invasive surveillance capabilities are becoming more available and affordable, suggesting wider use and increased oversight challenges (plus a host of non-government surveillance concerns). We are more connected, live more of our lives online, and live them in increasingly interconnected ways, massively increasing the amount and value of information potentially available to prying eyes—and the importance of dealing with that data responsibly from collection to storage, transmission, and disclosure.

In the past, many of the companies who paid the greatest attention to these issues seemed to have been prompted by painful lessons (the telcos remain largely immune to learning, however). Other civic actors blamed the companies for the shortcomings, fairly and not, with incomplete understanding of the issues. It now seems that most parties increasingly understand the dynamic and daunting nature of the challenge before us and the fact that we will continue to need a variety of resources to navigate this terrain, from the law to multi-stakeholder groups like GNI, and technology solutions alongside user norms. From the Internet's inception, bottom-up, multi-sector, participatory standards bodies have played an important role in promoting a robust and vibrant Internet, and, while imperfect, they remain an important part of the tapestry. GNI is a promising approach to developing global standards, advancing good practice, and solving concrete problems around online expression and privacy. With its organizational foundation laid, GNI can (and must) now embody more of that "Internetty" spirit, collaboratively, creatively, and practically taking on these challenges and helping to sustainably protect these human rights, the businesses built atop them, and their potential support for social progress. This is important because everyone can agree that we all need the help in these trying times.

TRANSPARENCY REPORTING

Ryan Budish

A pervasive surveillance apparatus for collecting information about the users of services like Gmail and Facebook. I'm not talking about the NSA and the secret programs that Eric Snowden revealed: in the US, personal data is also collected under the legal and non-secretive Stored Communications Act (SCA), and other countries have their own, similar mechanisms. We don't think of this form of collection as extensive or pervasive because accurate aggregate figures are hard to come by. That needs to change.

The US's SCA is an outdated piece of legislation, passed well before we had high-speed Internet or gigabytes of free cloud storage. It gives law enforcement the ability to collect substantial personal data, often with minimal court supervision. For instance, a law enforcement agency can obtain a person's name, physical address, IP addresses, data about when she signs on and off of an online service, and her payment processing information, simply by issuing a subpoena—a demand for information without court approval. If law enforcement notifies the target of the investigation, it can use a subpoena to collect opened emails of any age and unopened emails stored for longer than 180 days. In some circumstances, notice can be postponed. In other words: a tremendous amount of data is available without any court oversight. And law enforcement can use court orders and warrants to collect even more, if necessary.

What we know about this scale of this data collection comes from transparency reports – disclosures that some companies publish about the requests for user data that they've received from governments. In 2009, Google published the first transparency report; Twitter followed suit in 2012. Over a dozen companies are now releasing transparency reports, with more on the way.

These reports give us some information about the scale of governments' criminal surveillance. For instance, we know that in 2012, US law enforcement agencies made 16,407 requests from Google on 31,072 accounts (not including secret foreign surveillance). When combined with similar data from Twitter and Microsoft, the totals are 28,974 requests on 57,730 accounts.

This is helpful information, but it provides only the faintest glimpse into the full scope of lawful domestic surveillance. The utility of transparency reports as an industry-wide measure is limited by three factors:

Obscured Data: Several transparency reports obscure the amount of domestic surveillance. Facebook and Yahoo!, for example, recently released reports that combine national security requests with domestic criminal requests instead of providing criminal requests as a standalone category. This decision, a concession to the Obama administration in exchange for the right to disclose some data relating to national security requests, diminishes the value of the reports in illuminating either of the surveillance categories.

Inconsistent Data: Even the reports that explicitly provide domestic criminal data differ in some significant ways. For instance, how the companies define critical terms such as "user" or "court order" make the reports difficult to compare and aggregate, leaving us with approximations at best.

Weak Internationalization: Some of the companies releasing reports have provided detailed information about US requests, but none provide the same level about other countries' requests. How many countries use warrants? We can't say because we have only US data.

With more consistency in transparency reporting, we'd be able to develop a more complete picture of the scale of data collection in criminal investigations.

THE NEW GUARD

Dalia Topelson

As people are moving information previously hidden in locked file cabinets or safes into their personal clouds, companies have inadvertently gained unprecedented power over who can access and control information about individual citizens. This shift in control over personal data to the private corporate sector has created a new guard of corporate intermediaries that, by circumstance, have unwittingly become arbiters of law. Corporations, rather than individuals and judges, are deciding when and how information should be shared, destroyed, taken down, or concealed. The result is a disconnect between individual citizens and the judicial process that robs individuals of the opportunity to protect their rights and interests in the courts, including their right to free expression and to be free from unwarranted searches and seizures. In light of the revelations regarding the National Security Agency's large scale collection of data from consumer technology service providers, it is imperative that we analyze the role companies play in managing data collected and stored on behalf of individual citizens, including the legal structures that regulate (or don't regulate) what companies can and cannot do with an individual's information. The need is even more urgent in light of the growing investment in "big data" by venture capitalists and the like.

At present, companies in the United States are incentivized both economically and legally to take a passive approach when confronted with a takedown request or a government request for information. Challenging a request creates legal costs and puts companies at risk of direct liability for failing to comply with the request or to exercise their right to safe harbor protections offered by the law. In order to challenge a request, a company must assess its legality, but most companies lack the expertise and authority to make these types of judgment calls. This structure is further reinforced in companies' terms of use and privacy policies, which often give companies sweeping rights to disclose information as they deem necessary. The result is that governments and individuals alike can take advantage of companies' rational apathy and ignorance to obtain or suppress information uploaded by individuals to these services. This rational, yet passive, corporate behavior comes at cost to individuals, who are progressively using online tools for political expression, creating activist networks and generally championing democratic values.

Large online service providers are starting to address this problem head on by challenging these types of requests in the courts. Twitter has gained a reputation for protecting its users against unwarranted government requests,[1] and Yahoo has recently gained some praise for quietly challenging the legality of a government order requesting information under the Protect America Act.[2] Other service providers are offering encrypted email, texting, phone, and video chat services to help individuals proactively protect online communications from being intercepted. Still, most companies lack the legal resources and expertise to challenge these types of requests, and as a society, we should ask ourselves whether we want to relinquish control over the judicial process to intermediaries whose interests may be at odds with our own. This is not to say that companies should stop implementing policies and processes to help protect their customers from unwarranted intrusions of privacy or suppression of protected speech. Rather, we should revisit existing legal mechanisms and structures to ensure that we as citizens are capable of exercising our right to due process to protect the civil rights and liberties that create the foundation for a free democratic society.

Notes

1. Kim Zetter, “Twitter Fights Back to Protect ‘Occupy Wall Street’ Protester,” Wired, August 27, 2012, http://www.wired.com/threatlevel/2012/08/twitter-appeals-occupy-order/. See also Rachel Weiner, “Twitter earns plaudits for privacy amid NSA controversy,” The Washington Post, June 7, 2013, http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/07/twitter-earns-plaudits-for-privacy-amid-nsa-controversy/.

2. Mark Rumold, “Yahoo’s Fight for its Users in Secret Court Earns the Company Special Recognition in Who Has Your Back Survey,” Electronic Frontier Foundation, July 15, 2013, https://www.eff.org/deeplinks/2013/07/yahoo-fight-for-users-earns-company-special-recognition.

THE COMMERCIALIZATION OF CENSORSHIP AND SURVEILLANCE

Ron Deibert and Masashi Crete-Nishihata

The commercial market for Internet filtering and surveillance technologies is rapidly growing. This market consists of a range of products capable of content filtering and both passive and targeted surveillance, which, depending on the end use, can serve legitimate purposes or result in human rights violations. For example, products used for managing network traffic and restricting access to web content in private enterprise and institutional settings can also be used by governments to censor content on the national level or engage in passive surveillance.[1] Other technologies such as "lawful intercept" products are designed to provide passive and targeted surveillance capabilities, and are typically marketed directly to government agencies.

There are numerous examples of such technologies in the current marketplace. The US-based company Blue Coat provides network management appliances including PacketShaper and ProxySG, which are capable of network filtering and surveillance.[2] The Canada-based company Netsweeper develops products specifically designed to filter web content. The UK-based company Gamma International sells FinFisher, "governmental IT intrusion" software that can exfiltrate data, intercept email and instant messaging communications, and spy on users through webcams and microphones.[3]

These technologies have come under increased scrutiny over their use by regimes with dubious human rights records. Following the 2011 the Egyptian revolution, protestors retrieved a document from state security offices outlining an offer to the Egyptian State Security Investigations Service for the Finfisher surveillance software package. Similarly, in 2011 the *Wall Street Journal* reported that the French company Amesys sold deep packet inspection systems to the Gaddafi regime, and that the Gaddafi regime purchased technology from China's ZTE and South Africa's VASTech capable of tapping international phone calls. Bloomberg reported that Sweden's Ericsson, the United Kingdom's Creativity Software, and Ireland's AdaptiveMobile all provided Iranian law enforcement and state security agencies with surveillance technology. Privacy International believes that at least thirty British companies and at least fifty US companies sold surveillance technologies to countries that have committed human rights violations. [4]

From the mid-2000s onwards, the Citizen Lab has documented numerous cases of products developed in North America and Europe being used for censorship and surveillance by governments with poor human rights records, and in some cases under international sanctions.[5]

In more recent work, the Citizen Lab has revealed evidence of Netsweeper's filtering products in Pakistan, Qatar, the UAE, and Yemen.[6] The Citizen Lab has also found Blue Coat devices on public networks in 83 countries, including those with questionable human rights records, such as Burma, Cote d'Ivoire, and United Arab Emirates; and countries subject to sanctions, including Iran, Syria, and Sudan.[7] These findings raise questions around the sale of "dual-use" information and communication technologies to national jurisdictions where the implementation of such technology has not been publicly debated or shaped by the rule of law. These issues go beyond any one company and underscore the imperatives of addressing the global public policy implications of internationally marketed communications infrastructure and services.

Products used by law enforcement and government agencies for "lawful interception" become problematic in countries with weak rule of law and where dissident activities can be viewed as criminal. In 2012, the Citizen Lab found evidence of FinFisher being used to target Bahraini activists. Since that initial finding, we further revealed evidence of FinFisher campaigns with political content relevant to Ethiopia and Malaysia. In our most recent research, we detected FinFisher command and control servers (C2s) in 36 countries. The presence of a Finfisher C2 in a country does not necessarily imply that law enforcement or government agencies of that country are clients and operators of FinFisher. However, the global proliferation of Finfisher raises questions regarding how the product is being used, particularly in countries with problematic human rights records.

Lawmakers at national and regional levels and civil society organizations have called for greater regulation of sensitive technologies through industry self-regulation or legislative measures, such as export controls and sanctions. In December 2012, the European Union passed a resolution on a "Digital Freedom Strategy" that *inter alia* called for "a ban on exports of repressive technologies and services to authoritarian regimes" and "the establishment of a list, to be regularly updated, of countries which are violating freedom of expression in the context of human rights and to which the export of the above 'single-use' items [technologies that inherently threaten human rights, such as jamming, surveillance, monitoring and interception technology] should be banned."[8]

Civil society groups, policymakers, and others have pressured the private sector to better control the end uses of their products, leading to new frameworks for corporate social responsibility. To this end, civil society has developed a number of frameworks to encourage corporate social responsibility. For example, the Electronic Frontier Foundation's "Know Your Customer" framework encourages companies to investigate customers before and during transactions.[9]

Multi-stakeholder efforts have also emerged, such as the Global Network Initiative, a group of companies, civil society organizations, academics, and investors that provides a framework based on commitments to freedom of expression and privacy principles.[10] Some companies have developed their own corporate social responsibility policies. For example, Websense has a policy of not selling to "governments or Internet service providers that are engaged in any sort of government-imposed censorship."[11]

Ongoing research and monitoring of these technologies for censorship and surveillance is vital for informing policymakers and vendors who many not be aware that their products are being used to violate human rights. In 2009, after the OpenNet Initiative informed Websense that its products were being used to filter political content in Yemen (and thus violating the company's anti-censorship policy), Websense withdrew software update support. In 2011, the company joined the Global Network Initiative.[12] Similarly, media attention and pressure from government and civil society organizations in the wake of findings by Citizen Lab and others that Blue Coat devices were active in Syria[13] prompted the company to withdraw support, updates, and other services to active Blue Coat devices in the country.[14]

Addressing this growing market and the potential of human rights violations stemming from the use of Internet filtering and surveillance products requires dialogue between the private sector, government, and civil society. Bringing together perspectives from these stakeholders is crucial for moving towards effective options for intelligently controlling these technologies and ensuring companies can fulfill their moral and ethical obligations while also protecting them from liabilities that could arise from knowledge gaps and / or partner malfeasance in their global operations.

Notes

[1] For research on Internet filtering products being used in institutional settings, see: Peacefire: Open Access for the Net Generation, http://peacefire.org/info/about-peacefire.shtml; “Seth Finkelstein’s Anticensorware Investigations - Censorware Exposed,” http://sethf.com/anticensorware/; and Benjamin Edelman, “Expert Report of Benjamin Edelman,” Multnomah County Public Library et al., vs. United States of America, et al., http://cyber.law.harvard.edu/archived_content/people/edelman/pubs/aclu-101501.pdf.

[2] “Blue Coat PacketShaper Application List,” Blue Coat, http://www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf.

[3] Gamma International, “Remote Monitoring & Infection Solutions,” FinFisher IT Intrusion, http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf.

[4] See Gamma International, “Remote Monitoring & Infection Solutions,” FinFisher IT Intrusion, http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf; Margaret Coker and Paul Sonne, “Firms Aided Libyan Spies,” *Wall Street Journal*, August 30, 2011, http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html; Ben Elgin, Vernon Silver, and Alan Katz, “Iranian Police Seizing Dissidents Get Aid Of Western Companies,” *Bloomberg*, October 30, 2011, http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html; and Jamie Doward and Rebecca Lewis, “UK ‘Exporting Surveillance Technology to Repressive Nations’,” *The Guardian*, April 7, 2012, http://www.theguardian.com/world/2012/apr/07/surveillance-technology-repressive-regimes.

[5] See: “Tunisia,” OpenNet Initiative, 2005, http://opennet.net/studies/tunisia; “Saudi Arabia,” OpenNet Initiative, 2009, http://opennet.net/research/profiles/saudi-arabia; “United Arab Emirates,” OpenNet Initiative, 2009, http://opennet.net/research/profiles/united-arab-emirates; “Yemen,” OpenNet Initiative, 2009, http://opennet.net/research/profiles/yemen; and Jakub Dalek, Bennett Haselton, Helmi Noman, Adam Senft, Masashi Crete-Nishihata, Phillipa Gill, and Ronald Deibert, “A Method for Identifying and Confirming the Use of URL Filtering Products for Censorship,” IMC’13, October 23-25, 2013, Barcelona, Spain.

[6] Helmi Noman, “When a Canadian Company Decides what Citizens in the Middle East Access Online,” OpenNet Initiative, May 16, 2011, https://opennet.net/blog/2011/05/when-a-canadian-company-decides-what-citizens-middle-east-can-access-online; and Citizen Lab, “O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper’s Role in Pakistan’s Censorship Regime,” June 2013, https://citizenlab.org/2013/06/o-pakistan/.

[7] “Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma,” Citizen Lab, November 9, 2011, https://citizenlab.org/2011/11/behind-blue-coat; Morgan Marquis-Boire et al., “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” Citizen Lab, January 15, 2013, https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools; and Morgan Marquis-Boire et al., “Some Devices Wander by Mistake: Planet Blue Coat Redux,” July 9, 2013, https://citizenlab.org/2013/07/planet-blue-coat-redux/.

[8] European Parliament, *Report on a Digital Freedom Strategy in EU Foreign Policy*

(2012/2094(INI)), November 15, 2012, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN&language=EN. The US State Department also issued a guide on the export of "sensitive technology" to Iran and Syria pursuant to applicable sanctions, and the British government invoked an existing international export control regime—the Wassenaar Arrangement—to assert that FinFisher was subject to export controls. See: "State Department Sanctions Information and Guidance," US Department of State, November 8, 2012, http://www.state.gov/e/eb/tfs/spi/iran/fs/200316.htm; and "British government admits it has already started controlling exports of Gamma International's FinSpy," Privacy International, September 10, 2012, https://www.privacyinternational.org/press-releases/british-government-admits-it-has-already-started-controlling-exports-of-gamma .

[9] Cindy Cohn and Jillian C. York, "'Know Your Customer' Standards for Sales of Surveillance Equipment," Electronic Frontier Foundation, October 24, 2011, https://www.eff.org/deeplinks/2011/10/it's-time-know-your-customer-standards-sales-surveillance-equipment.

[10] Global Network Initiative, http://www.globalnetworkinitiative.org.

[11] "Anti-Censorship Policy," Websense, http://www.websense.com/content/censorship-policy.aspx.

[12] Jillian C. York, "Websense Bars Yemen's Government from Further Software Updates," OpenNet Initiative, 2009, https://opennet.net/blog/2009/08/websensebars-yemens-government-further-softwareupdates.

[13] "Web Censorship Technologies in Syria Revealed," Reflets.info, August 12, 2011, http://reflets.info/opsyria-web-censorship-technologies-in-syria-revealed-en; "Blue Coat's Role in Syria Censorship and Nationwide Monitoring System," Reflets.info, September 1, 2011, http://reflets.info/bluecoats-role-in-syrian-censorship-and-nationwide-monitoring-system; "#OpSyria: Syrian Censorship Logs (Season 3)," Reflets.info, October 4, 2011, http://reflets.info/opsyria-syrian-censoship-log; "Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma," November 9, 2011, https://citizenlab.org/2011/11/behind-blue-coat/.

[14] "Update on Blue Coat Devices in Syria," Blue Coat, December 15, 2011, http://www.bluecoat.com/company/news/update-blue-coat-devices-syria; and Citizen Lab, "UPDATE: Are Blue Coat Devices in Syria "Phoning Home?," Citizen Lab, January 14, 2013, https://citizenlab.org/2011/11/behind-blue-coat/#update.