Article

No-go zones: Ethical geographies of the surveillance industry

Claire Lauterbach

Privacy International, UK.
claire@privacyinternational.org

Abstract

In an industry as opaque as the surveillance technology industry, any effort to put in place safeguards to prevent human rights abuses using these technologies should be recognised and encouraged. But what happens when those systems fail? For surveillance technology companies, deciding where not to sell in a world full of eager government clients has important ethical and financial implications. The surveillance industry favours a country-agnostic framework that hews to sanctions and export laws. Advocacy and media groups argue to extend the no-sell zone beyond sanctioned governments to ‘authoritarian’ ones. Yet legal compliance is not the only factor influencing surveillance companies’ choices, this article argues. Based on original investigation, this article examines the social responsibility policies of communications surveillance technology vendors and the legal, reputational and normative concerns these demonstrate. The article explores the use of country rankings related to ‘authoritarianism’ and ‘good governance’ by examining the inner workings of a specific company in crisis, Procera Networks. As the cases featured demonstrate, closer attention to be paid processes of corporate responsibility norm-making within companies.

Introduction

In an industry as opaque as the surveillance technology industry, any effort to put in place safeguards to prevent human rights abuses using these technologies should be recognised and encouraged. But what happens when those systems fail?

Since 2012, companies based primarily in Europe but also in Israel, China, and elsewhere have supplied highly invasive electronic surveillance technologies to ‘authoritarian’ governments strongly criticised for abusing human rights. For surveillance technology companies, deciding where not to sell in a world full of eager government clients has important ethical and financial implications. The surveillance industry favours a country-agnostic framework that hews to sanctions and export laws. Advocacy and media groups argue to extend the no-sell zone beyond sanctioned governments to ‘authoritarian’ ones.

Yet legal compliance is not the only factor influencing surveillance companies’ choice of clients globally. A single company can comprise many different ethical geographies determined by legal, reputational, and normative concerns. The cases highlighted in this article give cause to nuance the view of companies common to corporate social responsibility literature as unitary actors and to pay closer attention to processes of corporate responsibility norm-making within companies.

Courting clients

Concern over non-compliance with international sanctions laws is a key factor determining in the business geography of the surveillance industry. ISS World, the premier trade fair of the electronic surveillance, cyber defence and intelligence industry, accepts delegates from everywhere except “any persons residing in or companies from the countries of Iran, Sudan, Syria, North Korea or Cuba”¹ at its events held annually in various locations worldwide (ISS World Training 2017). The five countries governments are all subject to wide-ranging UN, EU and NATO sanctions. Such is the concern with legal compliance—at least what can be discovered by a paper trail—that companies frequently apply for export licenses to trial equipment used for communications surveillance at trade fairs for concern that even testing out such equipment without them would be in violation of local laws.

In an apparent admission that reputational costs do matter to communications surveillance companies, several have inaugurated corporate social responsibility policies. This article closely examines three such ‘policies’ obtained by the author. Together, they reveal a range of ‘corporate social responsibility’ preoccupations—over *legal* compliance, potential *reputational* damage, and broader *normative* concerns.

Trovicor

Munich-based Trovicor is the surveillance spin-off company of the former telecommunications giant Nokia Siemens Network (NSN). Following controversy in 2009 when it was revealed that NSN had sold monitoring centre equipment to Iran in violation of EU sanctions, NSN sold its specialist surveillance unit to a private investment firm based in Munich; the new business was christened Trovicor.

NSN distanced itself from its surveillance business in part by putting in place a corporate social responsibility policy with ‘human rights’ and ‘privacy’ visibly at its core. In internal guidance in 2013, NSN advised its staff to state when asked that NSN “exited [the monitoring centre business] almost two years ago... business because in our view, it can *pose issues related to human rights* that we felt we are not adequately suited to address” (Privacy International 2015: 22). Further it stated that NSN maintained that it had “no ownership interest, no operational control, and no role in the management of Trovicor. Neither do we provide support to any of its products.” Carefully-worded denials aside, NSN nevertheless cooperated closely with Trovicor to execute at least one monitoring centre project in Pakistan in 2013² after the spin-off (Privacy International 2015).

However, Trovicor claims to have assumed a proactive approach to anticipating harms. “Our internal specialist team helps draft privacy impact assessments for each Trovicor solution,” it states³ (Trovicor 2015). No countries are named as off-limits, but Trovicor at least tacitly accepts the potentially negative repercussions of its work. However, its primary concern with legal compliance: its ‘internal compliance programme’ is situated within the company’s ‘export and customs control’ department.

VASTech

South African firm VASTech has been providing surveillance technology to government clients since 1999. The company specialises in passive network interception products. In 2011, VASTech was revealed to have provided its Zebra system for communications surveillance to the government of Colonel Muammar Gaddafi but declined to elaborate⁴ on its Libyan operations (Groenewald 2011).

¹ See: https://www.issworldtraining.com/ISS_EUROPE/register.htm.

² See: https://www.privacyinternational.org/sites/default/files/PAKISTAN_REPORT_HIGH_RES_20150721_0.pdf.

³ See: <http://www.ipfli.com/en/newsroom-en.html>.

⁴ See: <https://mg.co.za/article/2011-09-02-sa-firm-helped-gaddafi-spy>.

VASTech's internal compliance policy is more preoccupied with legal compliance; unlike Trovicor's, the policy makes no reference to human rights or privacy. When evidence of VASTech's work in Syria in 2010⁵ hit the media in December 2016, VASTech provided its compliance statement to the author, stating: "VASTech only makes its solutions available to government agencies, and then only to governments that are internationally recognised by the UN and are not subject to international sanctions" (Privacy International 2016: 73). The use of 'international sanctions' leaves VASTech a margin of flexibility in interpretation: the term could refer to UN, NATO, EU or any other sanctions by international bodies.

The one reference to normative considerations that appears in VASTech's policy is that it would "immediately discontinue supplying and supporting its products to a government of which the international status has changed so radically that it does not fulfil the above criteria anymore" (Privacy International 2016: 73). However, it is difficult to see how VASTech could comply with even their own voluntary standard. Both Syria and Libya are and were at the time of contracts with VASTech subject to extensive international sanctions and heavily engaged in quelling political dissent.

Gamma Group

The Anglo-German Gamma Group has gained international notoriety for selling FinFisher, an intrusion malware used to hack devices. Once infected, a person's computer or phone can be remotely monitored in real time. In considering potential sales, Gamma apparently refers to the UK Foreign Office's "published list of countries where there is concern about human rights", and Gamma's 'own human rights policy', as explained in its response to an investigation⁶ on the use of FinFisher against political dissidents (Privacy International 2015: 76). Gamma nevertheless ignored requests for further detail about its policy, leaving there is no basis on which to judge its effectiveness. However, given that technical indicators of FinFisher have been found⁷ in countries ranging from Ethiopia to Saudi Arabia (Citizen Lab 2015), it is doubtful that any such policy, if it exists, can reasonably be considered robust.

No-go zones

The boundaries of companies' *no-go zones* have ostensibly nothing to do with *type* of potential government client, authoritarian or not. They are instead driven primarily by legal concerns; the cases above suggest some attention to reputational costs, but only if such business is published. In an April 2017 undercover investigation,⁸ four companies knowingly offered to sell highly intrusive surveillance technology by falsifying export paperwork, in breach of national regulations. In discussing the deals, one official of an Italian company states that a high level of trust between his company and the proposed Iranian client would be needed to carry out the 'classified' deal and obscure the technology's true nature from regulatory authorities (Al Jazeera 2017).

The human rights community's no-go zones, however, contrast starkly with the industry's. Pressure groups have pushed companies and regulatory authorities to halt exports to countries with 'poor human rights records'. The Coalition Against Unlawful Surveillance Exports, which included human rights heavyweights Amnesty International and Human Rights Watch, called for⁹ "[t]he imposition of export licensing requirements upon strategically chosen, well-defined, surveillance technologies" to ensure "that such items are not used for abuses of human rights".

The precise relationship between human rights, democracy, authoritarianism and surveillance has never

⁵ See: <https://privacyinternational.org/sites/default/files/OpenSeason.pdf>.

⁶ See: https://privacyinternational.org/sites/default/files/Uganda_Report.pdf.

⁷ See: <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/>

⁸ See: <http://www.aljazeera.com/investigations/spy-merchants.html>

⁹ See: <https://www.privacyinternational.org/node/602>

been rigorously analysed in the advocacy community, however. Instead, this community relies on frequent referencing a potential or actual ‘chilling effect’ of surveillance for other rights including freedom of expression, religion and assembly—all of which are commonly considered necessary components of ‘democratic governance’. Extending the logic of CAUSE’s statement, the question of which governments or agencies within governments should not be able to purchase such technology remains unanswered.

So, too, does the question of what constitutes a rigorous assessment of either human rights or governance. For some exporting countries,¹⁰ human rights assessments are incorporated into the licencing procedure for the export of surveillance equipment which falls in a controlled category (Maurer et al. 2014: 9). The EU common position,¹¹ for example, requires the export agencies of EU countries to review of 8 categories including respect for human rights and international humanitarian law by the recipient country, the country’s internal situation, behaviour of the buyer including “attitude to terrorism” and the “risk of diversion towards an unauthorised end-user or end-use” (European Parliament 2015). However, these only govern export of military technology and equipment. Since 2015, the UK rejected just 7 of 181 applications¹² from UK companies to export dual-use ‘telecommunications interception’ equipment (Campaign Against the Arms Trade 2017).

The advocacy community has called on the EU to adopt a human rights review process in granting export licenses for surveillance technology. This would include a review of the end-user’s ‘human rights record’; an assessment the potential for technology misuse, and an analysis of the robustness of legal framework. However, details of what goes in to a human rights assessment or how it is to be conducted—to the limited extent that it is required by governments of the countries from which surveillance technologies are exported—are entirely unclear. Rigorously assessing a human rights situation is politically sensitive and methodologically difficult; companies and governments are understandably tempted to eschew the hard work of deliberating over the impacts of their sales and rely instead on externally-produced ranking measurements, as the case study of Procera Networks in the next section demonstrates.

Borderline technologies

This article has argued that surveillance companies’ decisions as to where in the world and to whom to refrain from selling their technologies is influenced primarily by concern over *legal* compliance, primarily arising from national country export regimes over ‘dual-use’ goods and international sanctions regimes against a small number of ‘authoritarian’ regimes. To a lesser degree, maintaining a visibly ‘clean’ reputation is another serious consideration. Stated *normative* concerns for the human rights implications of surveillance technologies appears to feature for some companies, though their records of engagement give ample rise to scepticism that these policies are designed to minimise reputational damage rather than prevent human rights abuses using their technologies.

The remainder of this article focuses on the case of Procera Networks. In 2016, the company witnessed an internal crisis over its decision to sell deep packet inspection (DPI) technology in Turkey, particularly over whether to fulfil their client’s request to be able extract personal passwords from unencrypted data streams.

In technology-policy discourses, DPI is separated from more ‘traditional’ tools that ‘make the internet work’, thus making DPI a contested and contentious technology. That is, DPI tools tend to be viewed with

¹⁰ See: https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf

¹¹ See: [http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG\(2015\)572821_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG(2015)572821_EN.pdf)
[http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG\(2015\)572821_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG(2015)572821_EN.pdf)

¹² See: <https://www.caat.org.uk/resources/export-licences/region?item=telecommunications+interception+equipment>

greater politics than tools that enable the internet to route and transmit data. DPI tools enable a form of filtering and inspecting internet traffic. Internet traffic, including communications like email, web browsing, instant messaging, and voice over IP communication, is composed of packets of digital information—these packets consist of payload data and header data (that includes data on addressing and protocols). Routing technologies, being of the ‘traditional’ toolkit, would look at header elements of the packets (e.g. addressing data) for routing purposes and send packets onwards. With DPI technologies, these packets are similarly analysed as they pass inspection points in their transmission across the internet but with an emphasis on the data components of the packets. At inspection points, the packets may be searched for protocol non-compliance, unwanted traffic like viruses and spam, attempts to intrude networks, or other kinds of defined criteria—all of these purposes are useful for the effective running of services. DPI technologies can also determine whether the packet may ‘pass’ onwards to its destination or if it needs to be blocked or routed to a different destination.

DPI use cases may appear relatively benign. DPI is sometimes considered in policy circles as an interference with the internet to advance an institution’s interests (Chester 2006), notably the institution in a position to place it on the network. DPI is thus far from value-neutral. DPI technologies can be fashioned to perform ‘regulatory analytics’, facilitating both state censorship of digital content as well as passive surveillance of users’ browsing habits and communications including for advertising purposes (Bernal 2011). Procera’s Subscriber Perspectives products, for example, logs records related to the IP addresses of devices like phones and laptops that are connected to the internet, and links this information to other data about the user. This for example enables the internet service provider to know where the subscriber is, their real name and identity, the sites they visit and how often. Procera products can allow the network to decide whether to block access at the micro level by location. “You can do basically anything with that data,” stated one developer linked to Procera, granted anonymity because of the sensitivity of the Turkish case.

Image 1. DPI technologies are used for quality control, but also provide deep insight into individuals' browsing habits (Procera Networks 2015: 13).

Troubleshooting ethics

Conducting research on surveillance sometimes requires digging deeper than what is publicly available or through direct interviews. Much of the information that is now known of government surveillance capabilities, for instance, is now possibly only because of whistle-blowers. No interview or review of government legislation could have revealed what we now know. Similarly, understanding the capabilities of the market in surveillance technology relies on more than queried disclosure through interviews and document searches. Over the years, civil society organisations and journalists have been tracking this surveillance industry using multiple traditional methods—attending conferences, interviewing employees, and relying on open source materials.

Sometimes other methods become available and necessary. Citizen Lab at the University of Toronto, for instance, has been able to peel back the layers of surveillance technology-deployment through technical analysis.

The case study below is based on documents shared with the author by a whistle-blower familiar with Procera. The author verified documentary information through corroborating interviews with several former and current employees. Interviewees were granted anonymity because they are not authorised to speak to researchers or the press. We engaged Procera in a manner that is consistent with investigative research, allowing them a right of reply to the key statements of this article and inviting them to answer further questions. Procera did not respond to repeated requests for comment.

Internal pressure from Procera's engineering corps over a surveillance deal in Egypt first prompted Procera's management to first create a new corporate responsibility mechanism—the ethics committee. In 2011, the Egyptian government's National Telecommunications Regulatory Authority (NTRA) purchased Procera's ScoreCard product, allowing NTRA to profile individuals by correlating IP address, real identities, locations and other metrics. One technology specialist described ScoreCard as very easy to abuse once the data structure built for massive collection is in place.

Following rumblings of discontent from within the company—the Egyptian government was more closed off and repressive than ever—Procera announced to its staff the formation of a new ethics committee in October 2014. The four-person committee would include an engineer who would review the company's commitments.

But the ethics committee was unable or unwilling to deal with the problematic Egyptian contract. Procera was sitting on a serious reputational time bomb. Speaking to the author and in correspondence seen by the author, engineers distilled their concerns as down to fear that their employer was facilitating authoritarianism. But Procera's attempt to address those concerns—through an Ethics Committee—were stagnating. The committee met infrequently. Its decisions were non-binding. "Sometimes they did come to the conclusion that we should probably kind of restrict it, but it was if the customer wanted to buy this, they'd have to sign to say they wouldn't use it for anything bad," reflected one employee. Some attributed the lack of action on a deeper transatlantic 'cultural divide', according to employees and internal documents. "The reason why [the ethics committee] even exists is that it's a bit of Swedish culture," recalls one engineer residing in Sweden. "We have American management. The top people in the company, they don't really share our values". In April 2015, Procera was sold to Francisco Partners, an American technology investment firm headquartered in San Francisco, California. Francisco Partners is reported to have invested in some of the most secretive surveillance technology firms¹³ (Fox-Brewster 2016).

¹³ See: <https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#237a47b3997c>.

Lines in the sand

In April 2016, the company was forced to draw a normative ‘line in the sand’.

That spring, Procera was about to seal a ‘managed services’ contract with Turkey’s main telecommunications service provider, Turk Telekom, with one red flag: the feature request asked specifically to extract personal passwords. The engineers refused to work on it. Even Procera’s CTO could see that fulfilling the password extraction request would be a “really bad idea.” Internet censorship and surveillance is rife in Turkey¹⁴ (Freedom House 2016), and the political situation was deteriorating rapidly in advance of the coup attempt in July 2016. Procera’s Turkey deal was for the Turkish Prime Ministry, according to documents seen by the author. Nevertheless, nothing was done about the engineers’ concerns. In early April, a Procera product manager fired off a resignation email to the company mailing list protesting “Erdoğan’s insanity”.

Procera’s management took the unique step of addressing a strong normative statement to their employees: the password extraction request was the new ‘line in the sand’. “Possible actions range from completely retracting from the deal (incredibly painful to Procera) to some kind of compromise where Procera’s technology will not be used to extract passwords, or whatever is deemed to be the ‘line in the sand’” executives confirmed in an all-hands meeting: “...we want to protect our reputation in media and the market, as well as our employees”.

Procera’s management offered to install a brand new improved ethics committee with a new framework for assessing its human rights impacts based on external standardised country rankings using criteria related to governance. Faced with a crisis, the company effectively outsourced its due diligence, but at least it had a policy. The next section examines the merits and weaknesses of that policy.

Rankings and rancour

Policy Guidance

- Procera will adhere to a Business Ethics Process
- We will make every effort to make sure no deals slip through this process. No loopholes by presenting a deal late in the sales process or trying to masquerade it as something else.
- [The BEC will use a World Bank framework to categorize countries (A, B, C, D) and will take into account any additional facts that are known regarding the the use of our products by the customer
- Sales of any Procera product for a Regulatory use case to B and C countries are submitted to a Business Ethics Council which has the responsibility and authority to review and restrict sale of the product and/or development of product capabilities based on country of use. Sale of Procera products to D countries is prohibited.
- BEC reviews are held early in the sales cycle.
- All customers shall abide by the Acceptable Use policy. In the event the customer does not comply, then their license to use the product terminates.

The BEC has the authority to ask our customer for a Certificate of Compliance with the Acceptable Use. If the customer does not agree to certify then Procera sale of the product is not authorized.

Image 2: Procera’s policy guidance (2016), reproduced from the original by the author.

¹⁴ See: <https://freedomhouse.org/report/freedom-press/2016/turkey>.

On paper, the company's policy guidance is enviable. While never discussing 'authoritarianism' it does refer to a range of 'acceptable use(s)' for its products, requiring customers to sign an acceptable use agreement.

COUNTRY SEGMENT	TRAFFIC MANAGEMENT	POLICY AND CHARGING	ANALYTICS	REGULATORY ANALYTICS
A	OK to sell	OK to sell	OK to sell	OK to sell
B	OK to sell	OK to sell	OK to sell	Review required May require the Customer to certify intended use
C	OK to sell	OK to sell	OK to sell	Review required Customer must certify intended use
D	Will not sell	Will not sell	Will not sell	Will not sell

Regulatory segment definition:

- Sold to a government regulator or other governmental agency
- Sold to a carrier who is compelled by the government to provide bulk data feed export to a regulator or other government agency
- Regulatory filtering use cases are OK to sell, except where explicitly not allowed by EULA

Table 1: An eight-way metric by type of business and country category is supposed to guide Procera's ethics reviews. Reproduced from the original by author.

Procera also created a decision matrix: amalgamating four World Bank country-ranking indices, Procera divides its prospective clients into four categories (A to D).

Two main points on which such an approach could be critiqued. The first is the decision to rely on standardised metrics to approximate risk. Procera's matrix uses the World Bank's 'voice and accountability', 'political stability', 'rule of law' and 'control of corruption' indices. The World Bank's indices themselves are themselves an amalgam of indices from media outlets, think tanks, development banks and other sources. Such metrics are often criticised for their blind spots and presuppositions.

The second point of critique is how the countries are divided into categories A to D, and what, practically this means for any safeguards applied to business with them. By this policy, Procera would not generally have to complete an ethics review for 'regulatory analytics' (which engineers called network surveillance mostly for law enforcement agencies) with the A-listers, which include most of Europe and Israel. Category B or C countries would require a further review by the ethics committee. The only difference is that for C countries, the end-user agency would have to self-monitor by signing a statement that it would not use Procera's technology for anything other than 'intended use'. Predictably, D countries—from North Korea to Sudan—are off limits.

Procera did not respond to requests for clarification on how categories A-D are 'scored' using the World Bank indices and what an 'ethics review' would involve. It is unclear, therefore, how often such a country category list would be revised, considering the rapidly deteriorating political situation of many countries in the B and C categories. Crucially, not only are many of the countries with the worst human rights records in the B category, they are also Procera's 'target' market. These include the Philippines—whose government is accused of extra-judicially killing¹⁵ over 1,000 people (Human Rights Watch 2017). Thailand, where insulting the king has been punished by up to 60 years in prison (Privacy International 2017), is also a target country. Procera did not respond to requests to explain their 'target country' programme.

¹⁵ See: <https://www.hrw.org/report/2017/03/01/license-kill/philippine-police-killings-dutertes-war-drugs>.

The essential dilemma of the Procera case is that by dividing up the world into a standardised decision matrix relying on widely-accepted external metrics in an attempt to prevent further scandals over its repressive government clients, Procera has created a rubric with a built-in conflict of interest. This raises questions as to substance of Procera's stated commitment to preventing abuse of its technologies, whether by authoritarian or other governments.

Furthermore, the company has created an internal watchdog mechanism that does not involve the company's most critical employees. In fact, it marginalises those employees—the engineers—who are most likely to understand the 'good' and 'bad' uses of their technologies. In May 2016, the Ethics Committee was rebooted as a 'Business Ethics Committee (BEC)'. This time, however, it comprised only top management and a lawyer with no voting power. There were no engineers. "Which I guess was humorous in the way they put 'Business' before 'Ethics'", chuckled one engineer.

Companies have frequently argued that they can effectively self-regulate. A 2015 European Commission-funded report¹⁶ featuring a survey of 'cyber-surveillance technologies' companies found that respondents attributed strong positive impacts to 'self-regulation' and tools like the use of 'electronic blacklists' of customers (ECORYS and SIPRI 2015). They were also much more likely to favour 'obligatory self-regulation' than either human rights assessments by export authorities or additional EU-level cyber-surveillance technology lists for control.

But will companies self-regulate in a meaningful way? Evidence reviewed in this article, including some companies' willingness to circumvent the law¹⁷ (Al Jazeera 2017) and even to plainly violate their own company policies, suggest that they will not, or at least that current approaches to preventing human rights harms are insufficiently robust.

Ethical geographies

A single company can comprise many different ethical geographies, as the Procera case demonstrates. Policymakers in this arena should pay more attention needed to the risks and influences that companies must manage—legal noncompliance and the potential financial sanctions they incur, as well as reputational risk and a resulting loss of business. Human rights concerns, though largely much less influential, do appear to factor in to the calculations of companies within the surveillance industry—albeit more likely with companies who do not focus exclusively on surveillance technologies (such as the Gamma Group) but rather have strong market basis in producing technologies not exclusively used for surveillance purposes (such as Procera Networks).

The use of 'objective' external rankings and standards is a poor substitute for more involved, comprehensive consideration of human rights issues. No amount of analysis, however, can compensate for a business model that prioritises business with repressive governments. Genuine efforts by any company to improve ethics and corporate social responsibility procedures should be applauded. But these efforts must be based on a political will to abide by these procedures even at a financial cost. Concern over legal compliance and to a lesser degree geopolitical reputational costs is likely to remain the primary concern absent 'harder' repercussions, particularly for companies whose business is exclusively technologies designed primarily for communications surveillance.

¹⁶ See: <https://www.sipri.org/publications/2015/other-publications/final-report-eu-dualuse-review>.

¹⁷ See: <http://www.aljazeera.com/indepth/features/2017/04/spy-merchants-spying-dissent-illegal-means-170409073619770.html>.

References

- Al Jazeera. 2017. "Spy Merchants". Accessed April 10, 2017. <http://www.aljazeera.com/investigations/spy-merchants.html>.
- Bernal, Paul. 2011. "Rise and Phall: Lessons from the Phorm Saga". In *Computers, Privacy and Data Protection: An Element of Choice*, eds Serge Gutwirth et al. 269-283. Houten, The Netherlands: Springer.
- Campaign Against the Arms Trade. 2017. "telecommunications interception equipment". In *UK Arms Export Licenses, 2015-2017 database*. Accessed April 10, 2017. <https://www.caat.org.uk/resources/export-licences/licence?item=telecommunications+interception+equipment&rating=Dual+Use>.
- Chester, Jeffrey. 2006. "The End of the Internet?" *The Nation*, 13 February. Accessed April 28, 2017. <https://www.thenation.com/article/end-internet/>.
- Citizen Lab, The. 2015. "Pay No Attention to the Server Behind the Proxy: Mapping Fin-Fisher's Continuing Proliferation", October 15. Accessed April 10, 2017. <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/>.
- ECORYS and SIPRI. 2015. "Data and information collection for EU dual-use export control policy review", November. Accessed November 20, 2017. <https://www.sipri.org/publications/2015/other-publications/final-report-eu-dualuse-review>.
- European Parliament. 2015. "At a glance: EU rules on control of arms exports." December 10. Accessed April 10, 2017. [http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG\(2015\)572821_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/572821/EPRS_ATAG(2015)572821_EN.pdf).
- Fox-Brewster, Thomas. 2016. "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text". *Forbes*, August 25. Accessed April 10, 2017. <https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#39ee40703997>.
- Freedom House. 2016. "Turkey". In *Freedom of the Press 2016*. Accessed April 10, 2017. <https://freedomhouse.org/report/freedom-press/2016/turkey>.
- Groenewald, Yolandi. 2011. "SA firm 'helped' Gaddafi spy on the people of Libya." *Mail and Guardian*, September 2. Accessed April 10, 2017. <https://mg.co.za/article/2011-09-02-sa-firm-helped-gaddafi-spy>.
- Human Rights Watch. 2017. "'License to Kill': Philippine Police Killings in Duterte's 'War on Drugs'". 1 March. Accessed April 10, 2017. <https://www.hrw.org/report/2017/03/01/license-kill/philippine-police-killings-dutertes-war-drugs>.
- ISS World Training. 2017. "Registration". Accessed April 10. https://www.issworldtraining.com/ISS_EUROPE/register.htm.
- Maurer, Tim, Omanovic, Edin and Ben Wagner. 2014. "Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age." March. Accessed April 10, 2017. https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf.
- Privacy International. 2015. "Tipping the Scales: Security & surveillance in Pakistan". Accessed April 25, 2017. https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf.
- Privacy International. 2016. "Open Season: Building Syria's Surveillance State." Accessed April 10, 2017. <https://privacyinternational.org/sites/default/files/OpenSeason.pdf>.
- Privacy International. 2017. "Friends, Followers, Police Officers, and Enemies: Social Surveillance in Thailand". Accessed April 10, 2017. <https://www.privacyinternational.org/node/935>.
- Prodera Networks. 2015. "Mobile Subscriber Experience for Dummies." May 28. Accessed April 10, 2017. <https://www.slideshare.net/proceranetworks/mobile-subscriber-experience-for-dummies-v23>.
- Trovicor. 2015. "The challenge of balancing national security with individual privacy." Accessed April 10, 2017. <http://www.ipfli.com/en/newsroom-en.html>.