REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

Submission by Reporters Without Borders (RSF) for the call

"The Surveillance Industry and Human Rights"

by the Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

15th of February 2019

Further information
Elodie Vialle
Head of Journalism & Technology Desk
evialle@rsf.org

Daniel Moßbrucker
Policy Advisor Internet Freedom, RSF Germany
dm@reporter-ohne-grenzen.de

About Reporters Without Borders

Reporters Without Borders is an international human rights organization defending freedom of information, the safety of journalists and fighting censorship online and offline. Founded in 1985, the headquarter is based in Paris. Today, the organization has bureaux, sections or representatives in 18 cities (Berlin, Brussels, Dakar, Geneva, Helsinki, Istanbul, Karachi, Kiev, London, Madrid, Mexico, Rio de Janeiro, San Francisco, Stockholm, Taipei, Tunis, Vienna and Washington) and correspondents in 130 countries. The impact of the digitization on press freedom has been a key priority since the growing importance of the internet for the global communication as well as for the work of journalists. Today, RSF has experts on that field in many areas in the world, for example the Journalism and Technology Desk in Paris, the Desk for Internet Freedom in Berlin and the office in the Silicon Valley, Mountain View. Since the Arabic Spring, RSF follows the discussion about the growing state surveillance against journalists and the use of spy tools developed by the private sector. Therefore, RSF provides assistance to journalists about digital security and works on the question of trade regulations for surveillance technologies.

Topic of the Submission

Given the limited extend of this submission and the perspectives of the experts in the Consultation for this submission in Bangkok, Thailand, in December 2018, RSF will focus especially on improvements for trade regulation of surveillance technology and the need for more business responsibility in that field.

1 Current problems for journalists with government surveillance and the importance of the private sector

Due to their profession, journalists have always been an attractive target for government surveillance. On the one hand, they may have information that have crucial importance for authorities such as intelligence services. On the other hand, they work closely together with sources to gather this information, which can cause legal problems as whistleblowing is often considered illegal. In general, three types of surveillance can be differentiated:

- **interception of communication**, often conducted by giving the private telecommunication or internet service providers the legal obligation to make the communication accessible (targeted surveillance)
- **hacking of terminal devices**, either practiced by state authorities – mostly with tools developed by the private sector – or practiced by private companies who then provide the intercepted data (targeted surveillance)
- **mass surveillance**, mostly practiced by intelligence agencies for (foreign) communication flows by giving private companies such as internet exchange points the legal obligation to mirror the data streams (mass surveillance)

In all cases, a significant problem for journalists is a **lack of attribution** for these surveillance practices. Journalist either do not even know that they are under surveillance, or it is nearly impossible for them or IT forensics to attribute the adversary.[1] However, attribution is essential to have access to remedy.

The common ground of these developments is the strong relation between governments and the private sector in that field. Both democratic and non-democratic states seek to get the latest technology from companies to be able to better control the population. This includes hardware, software, maintenance and consulting.[2] Reporters Without Borders is convinced that the **private sector must take its responsibility more seriously** as technology of companies is widely used for human rights abuses. For that, self-regulatory initiatives may be one piece of the puzzle, but it is not sufficient. Due to the special characteristics of the private surveillance market – great variety of actors in profession, size and nationality, high importance of NDAs, strong relation to intelligence agencies, etc. – a **global, regulatory legal framework for export controls of surveillance technology needs to be developed**. It needs to meet both state responsibilities as well as those from the private sector. It should be the further development of the UN Guiding Principles on Business and Human Rights for the private surveillance sector.

2 Towards a global control regime for surveillance technology

As digitization, the globalisation of trading and state surveillance is evolving, Reporters Without Borders is convinced that an adequate control regime for surveillance technology is necessary to safeguard fundamental rights such as the right to freedom of expression and the right to privacy. Among others, export controls can be one instrument to achieve this goal.

[1] Sven Herpig & Thomas Reinhold (2018): Spotting the bear: credible attribution and Russian operations in cyberspace, URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

[2] Privacy International (2016): The global surveillance industry, URL: https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

With reference to the legal analysis of the UN Special rapporteur in preparation of the expert consultation for that submission, RSF considers the following aspects as the most pressing issues in the export control regulation of surveillance technology.

So far, there are **only very few export control regimes for surveillance technology in place**. Regarding to the Wassenaar Arrangement[3] and the EU regulation[4], surveillance technology is legally considered as dual use items. These regimes were historically created for completely different items such as nuclear goods or components of weapons of mass destruction. This is problematic as it is today **hard to define a balanced legal language** that fits for both surveillance technology and "traditional dual use items".

⇒ *A global control regime, that only deals with surveillance technology or at least has the flexibility to exclude non-digital goods in some areas of a regulation, would be an immense improvement.*

A consequence of broad legal language in the existing regulations such as Wassenaar is a **high pressure from industry on lawmakers**[5] – even from those who do not provide surveillance technology. As they are afraid that their non-digital goods fall under the regulation, they oppose it.

⇒ *A regulation that deals with the specifics of surveillance technology – immaterial, often usable for consumer products, hard to attribute etc. – is coercible.*

Another consequence of the broad language in the regulation is that it opens loopholes for companies to **legally circumvent export control requirements**. For example, in 2018 Access Now reported[6] that spyware of the German company FinFisher has still been used in Turkey, but the German government never received a request for an export warrant. It remains unclear whether the company used a legal way or whether it made criminal deals.

⇒ *National states have to improve the ability to investigate cases of export control circumvention when there is evidence that products "somehow found their way" to a critical destination. To achieve that, states may have to adjust their obligations in the criminal code and companies have to cooperate with state investigators. If there is evidence that a company's products is used in critical environments, the company has to explain how the technology came there.*

As there is no international binding regulation in place, the existing **multilateral regimes may be in conflict with the business structure of international operating companies**. For the regulatory practice, this causes two problems: First, companies make the argument of a "level playing field" that is in their view necessary for their business.[7] Second, a regulation cannot be enforcement in countries that are not part of the regimes, although they may receive surveillance technology. This is especially important for so-called end-use-controls that exist for the control of weapons. They might be effective for the control of surveillance technology as well, but exporting countries so far have no rights to exercise

[3] Wassenaar Arrangementon Export Controls for Conventional Arms and Dual-Use Goods and Technologies, URL: https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf

[4] COUNCIL REGULATION (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0428&from=EN

[5] Daniel Moßbrucker (2018), Surveillance exports: How EU Member States are compromising new human rights standards, URL: https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/

[6] Access Now, FinFisher changes tactics to hook critics, see: https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/

[7] BDI The voice of German industry (2018): For a Balanced Reform of the EU Regulation on Dual-Use Export Controls, URL: https://english.bdi.eu/article/news/for-a-balanced-reform-of-the-eu-regulation-on-dual-use-export-controls/

these end-use-controls as it is considered as a violation of the national sovereignty of the importing state.

- ⇒ *A regulation has to open the possibility for exporting countries to control the end-use of surveillance technology in the destination country. An export has to be denied if a destination country refuses to this.*

In regulating exports of the surveillance technology, states have to regulate their own business partners. Also democratic states are customers of these companies, sometimes for decades. The result is a **strong relationship between government and the surveillance industry**.[8] This influence of the private sector hinders both an improvement of regulations as well as stricter decision about export licenses. Moreover, the authorities that have to make the decisions about export controls often have **not enough staff** to make intensive research.

- ⇒ *A regulation has to safeguard the independence of the decision making process. It needs a system with enough resources as well as checks and balances within an authority, but also transparency about warrants and denies as it holds the government publicly accountable for their behaviour.*

There is a **lack of intergovernmental information sharing** and a **lack of international standards** about export license decisions. For example, even within the EU, which has a common regulation regime, the EU member states fell different decisions about certain technologies and countries. [9]As there are no standards that provide orientation for the authorities, the decisions about export controls often do not reflect the human rights situation in the countries, but follow more geopolitical and strategic deliberations. Also, the decision-making in the exporting process often relays on **non-public information gathered by the national intelligence agencies**. These are considered secret, which is in conflict with intergovernmental intelligence sharing.

- ⇒ *States have to install a mechanism of intergovernmental information sharing about the human rights situation in destination countries, previous decisions for certain technologies and countries and about the previous use of surveillance technology in the country. Common databases for information sharing could be one option. It is important to not only rely on intelligence information, but also seek for information from civil society organisations and affected people in the destination countries.*
- ⇒ *If an authority comes to the conclusion, that human rights violations are likely, the export needs to be automatically denied. A human rights concern cannot be balanced with a business calculation.*

In almost every country, companies have a **right to business secrecy**. This stands in conflict with transparency obligations for export controls of exporting countries, e.g. the name of companies, the products they are selling etc. Moreover, the importing countries often have to sign **Non-Disclosure-Agreements (NDA)** in order to use the products for the states purposes. This could, for example, serve as an argument for governments to not disclose information under a Freedom of Information Request.

- ⇒ *States have to periodically publish information about exports of surveillance technology, at least quarterly and in an easily accessible manner, on each license*

[8] see 2.

[9] European Commission (2016): Report on the EU Export Control Policy Review, URL: https://trade.ec.europa.eu/doclib/docs/2016/october/tradoc_155008.pdf

with regard to the type of license, the value, the volume, nature of equipment, a description of the product, the end user and end use, the country of destination, as well as information regarding approval or denial of the license request. A NDA must not stand in conflict with these obligations, as these information do not touch sensitive information.

Although the protection of human rights is first and foremost an obligation of states, also the private sector has to meet its responsibilities. This is especially crucial in a field in which the private sector develops products that are by definition designed to interfere with human rights such as the right to privacy, the right to freedom of expression or the right to free assembly. However, most of the surveillance companies today only make a contract with a government in which both sides agree that the technology will only used for legitimate purposes. **Many businesses of the surveillance industry consider that they are not bound by law to exercise due diligence in the human rights field**. In the EU regulation, for example, an exporter only needs to "be aware" of potential human rights violations, but not to "become aware" of them.[10]

⇒ *Following the business principles on business and human rights, also companies of the surveillance industry have to implement an internal due diligence process to identify potential human rights violations with their products.*

3 Arising challenges for export controls of surveillance technology

As technology is constantly evolving, however, there are already new dangers for journalists arising apart from these three "traditional" types of governmental surveillance. For example, the growing existence of **CCTV cameras** in the public space combined with **facial recognition technology**, often practiced with machine learning technology, makes it more and more impossible for journalists to move without being monitored and meet sources privately. Moreover, **data mining** programs mark a new trend in the underlying purpose of governmental surveillance. In analysing huge amounts of data and combining them with data gathered by secret surveillance actions, governments do not only want to prove behaviour with surveillance (e.g. on courts), but to use surveillance to **predict behaviour**. This is a slow, but dangerous development for journalists as they rely on an environment that allows themselves and their sources to act without a general suspicion. If this trend of predictive data mining due to surveillance continues, it would be a next step in limiting the working conditions for free media. In an extreme case, whistleblowing would become impossible, because authorities would be aware of this before it actually occurred. In this context, it is worth to note that both in the EU[11] and in den USA[12] lawmakers at least already considered to add certain groups of "new technologies" that go beyond the list of Wassenaar, such as "digital forensics" or even artificial intelligence systems to existing export control regimes.

[10] see 4.

[11] European Commission (2016): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items, URL:

https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF

[12] Bureau of Industry and Security (2018): Review of Controls for Certain Emerging Technologies, URL:

https://www.regulations.gov/document?D=BIS-2018-0024-0001

While this shows the relevancy of this development, it remains unclear in both cases whether there will be a majority for these improvements in the ongoing negotiations.

Attention should also be drawn on the **grey markets for vulnerabilities**, in which again private companies sell weaknesses in software or hardware to government authorities. While it might be pretty easy now for governmental agencies to build their own exploit, the new product of private companies is nowadays "only" knowledge about vulnerabilities. From a regulatory perspective, this poses completely new questions about how to control these international, non-official markets.