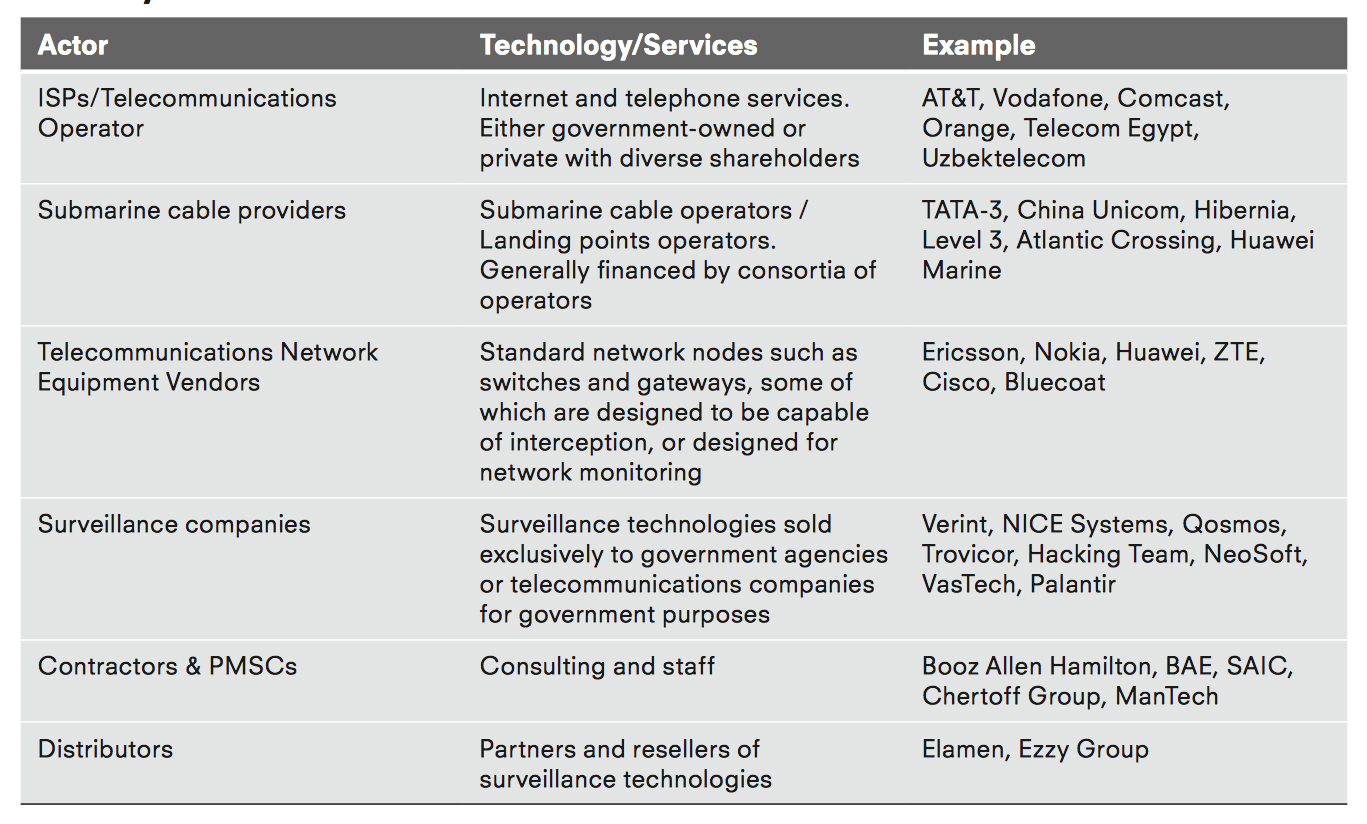
**The Surveillance Industry and Human Rights**

*Privacy International submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*

**February 2019**

Privacy International makes this submission in support of the UN Special Rapporteur's study regarding the obligations and responsibilities of States and businesses to ensure compliance with human rights standards in the procurement, transfer, and use of surveillance technologies.

The modern electronic communications surveillance industry evolved from the commercialisation of the internet and digital telecommunications networks during the nineties, when governments began passing new laws demanding new electronic surveillance powers and technical protocols to guarantee government access to networks. In response, a global industry developed consisting of arms contractors, telecommunications companies, IT businesses, and specialised surveillance companies. The following table summarises various private actors involved in a state’s surveillance architecture.



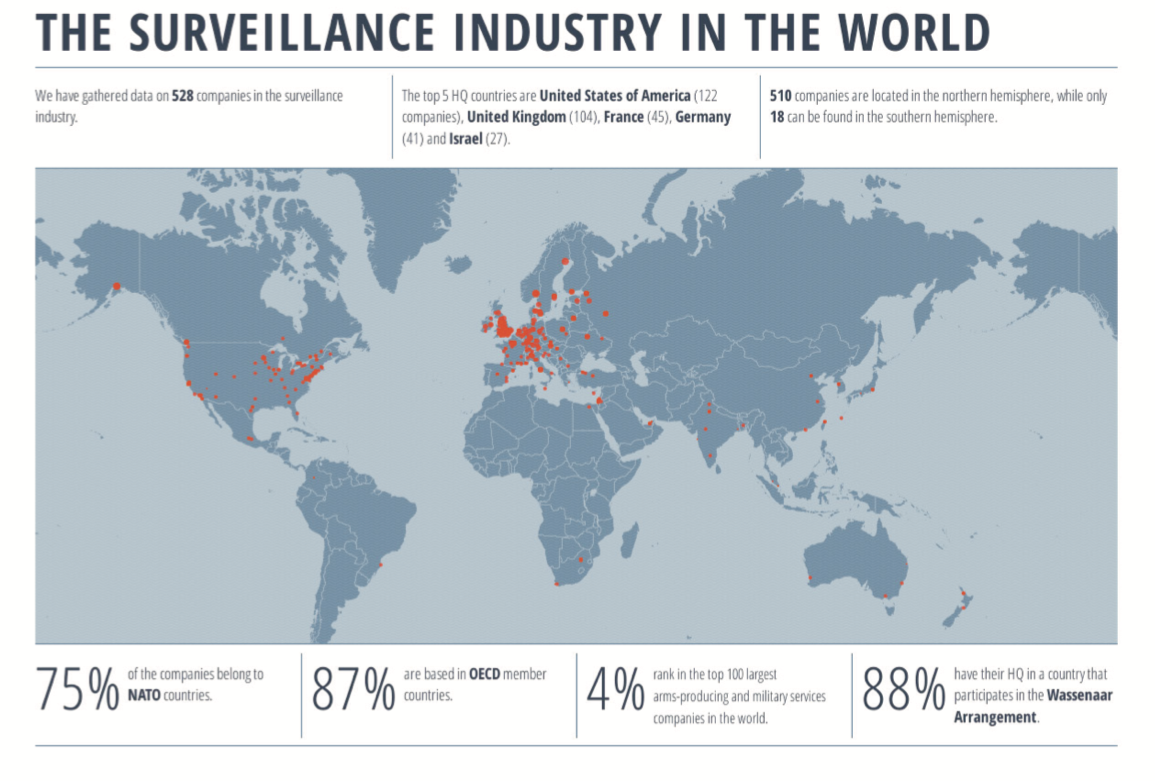
As of May 2016, Privacy International has identified 528 companies which sell one of the following types of surveillance technology.



These companies are overwhelmingly based in large arms-exporting states, with 87% of the 528 companies based in Organisation for Economic Co-operation and Development (OECD) states.

Examples of State use of private surveillance technology against individuals or civil society organizations include:

* [Bahrain Government Hacked Lawyers and Activists with UK Spyware](https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/)
* [Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families](https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html)
* [Snapping up cheap spy tools, nations ‘monitoring everyone’](https://apnews.com/736dd5c3aa644cd499d6f6da8b9e5974)
* [Macedonia: Society On Tap](https://privacyinternational.org/feature/1120/macedonia-society-tap)
* [Torture in Bahrain Becomes Routine With Help From Nokia Siemens](http://www.bahrainrights.org/en/node/4549)
* [The Million Dollar Dissident](https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/)



**Safeguards**

Self-regulation

There is little publicly available evidence that self-regulation by surveillance companies has led to better protections for activists and civil society. In 2014, the UK government and Tech UK, an industry association, produced guidelines for companies to assess the risk to human rights posed by exports of cyber security technologies by conducting due diligence and post monitoring practices.[[1]](#footnote-1) In 2011, the Electronic Frontier Foundation published a “Know Your Customer” guide for surveillance companies.[[2]](#footnote-2) Where human rights concerns do appear to factor in to the calculations of companies within the surveillance industry, it is more likely with companies who do not focus exclusively on surveillance technologies but rather have strong market basis in producing technologies not exclusively used for surveillance purposes, such as network equipment vendors.[[3]](#footnote-3)

Sanctions

Some surveillance technologies have been incorporated into sanctions regimes. The EU has embargoed the transfer of surveillance technologies as part of Restrictive Measures against Syria and Iran. Following a Council Decision in December 2011, Council Regulation (EU) 36/2012 in January 2012 imposed a ban on the sale, supply, transfer or export, directly or indirectly of surveillance equipment, technology or software “whether or not originating in the Union, to any person, entity or body in Syria or for use in Syria.” Similar measures were imposed within Council Regulation (EU) No 264/2012 targeting Iran on a broad range of surveillance technologies, as well as technology and software used for their development and use.

It has been suggested that surveillance technologies could potentially be included within the general scope of restricted items within EU and UN sanctions. In February 2014, Privacy International contacted United Nations investigators monitoring the UN arms embargo on Sudan regarding the fact that Hacking Team’s technology was reported by Citizen Lab to be in use by the country’s military intelligence agency. It was subsequently reported that after the UN Sudan investigators approached the company, Hacking Team replied to say that they had no active business contracts in place. The UN followed up by asking whether there have been any historical contracts. The hack of the company’s internal systems showed that in 2012, Sudan’s National Intelligence and Security Service paid a total of 960,000 euros for their intrusion system, and that Hacking Team cut off the account’s service on November 24, 2014. In response to the UN, Hacking Team stated that its product was not covered by the EU embargo, to which the UN answered that as “such software is ideally suited to support military electronic intelligence (ELINT) operations it may potentially fall under the category of “military... equipment” or “assistance” related to prohibited items.

In 2010, the US prohibited the export of “sensitive technology” to Iran through the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010. Sensitive technology is defined as hardware, software, telecommunications equipment or any other technology used specifically “1) to restrict the free flow of unbiased information in Iran; or 2) to disrupt, monitor or otherwise restrict speech of the people of Iran.” This provision was later expanded to include Syria through the Iran Threat Reduction and Syria Human Rights Act of 2012, Executive Order 13606 (the GHRAVITY E.O.) and Executive Order 13628.

Export licensing controls

Strategic trade controls imposing export licensing requirements on specific surveillance technologies have also been imposed. The Wassenaar Arrangement has for decades controlled the export of cryptography, meaning that some surveillance systems are subject to prior licensing if they contain certain levels of cryptography.

In 2010, “laser microphones” were added to list, which are used to eavesdrop on conversations by monitoring sound vibrations using lasers, for example through glass.[[4]](#footnote-4)

In 2012, phone monitoring technology was explicitly added to the Wassenaar list to target mobile and satellite phone monitoring equipment. Prior to 2012, some states had already controlled the equipment because of controls on ‘Telecommunications systems, equipment, components’, though this was interpreted differently by participating states.

In 2013, two further controls were added into the Wassenaar list, one on intrusion software and another on internet monitoring technology. The public statement stated that the controls were aimed at “surveillance and law enforcement/intelligence gathering tools and Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability.”[[5]](#footnote-5)

The category on internet monitoring, known as IP Network Surveillance Systems, was initiated by France after evidence emerged that a French company, Amesys, supplied internet backbone monitoring technology to Gaddafi’s Libya. According to the Wall Street Journal, Amesys’ Eagle monitoring centre, which used a combination of probes using Deep Packet Inspection technology and analysis software, was “deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state” in Libya.141 A criminal case against Amesys for complicity in acts of torture by the Gaddafi regime is ongoing.[[6]](#footnote-6) France implemented the control almost immediately after it was approved by the WA in 2013.

The addition of items related to intrusion software were proposed by the United Kingdom and also agreed at the WA in December 2013. The UK government has stated that these controls were on “Complex surveillance tools which enable unauthorised access to computer systems” introduced “because of real concerns about the use of such tools to breach human rights and the risks that they pose to national security”.[[7]](#footnote-7) The controls distinguished between components used to create and control the malware itself, meaning that the malware component is not targeted, but rather the command and control infrastructure used to generate, install and instruct the malware.

The 2013 additions to the Wassenaar list were added into the EU Dual Use regulation in January 2015. The regulation, which is binding on member states, incorporates decisions to include items for licensing restrictions taken at Wassenaar level, meaning that member states have been controlling the 2013 items since then.

In July 2015, the US Bureau of Industry and Security (BIS) published a proposed implementation of the 2013 additions, causing widespread concern among IT security researchers relating specifically to the implementation of controls on intrusion software. Concerns largely revolved around the fact that the US had interpreted the international agreement too broadly and that the language used by BIS could be interpreted to cover the development of malware and sharing of information about vulnerabilities, meaning that researchers would have to apply for an export license before sharing information about vulnerabilities. Since an open round of submissions, BIS has since agreed to reinterpret the agreement and attempt to update the control language within the Wassenaar Arrangement itself. Efforts to reformulate the control language on intrusion software to protect security research were supported by Privacy International and other NGOs.[[8]](#footnote-8)

Israel is not a participating member of the Wassenaar Arrangement, although it does include items added to the Wassenaar Arrangement’s control list within its own list of strategically controlled goods. In January 2016, the Israeli Defense Exports Control Agency published proposed rules aiming to make a broad range of technologies that can be used for surveillance subject to licensing, going further than any other participating country and far beyond what was decided at the Wassenaar Arrangement, by explicitly stating that the export of exploits would be regulated.[[9]](#footnote-9) Amid significant opposition from Israeli defence contractors, it was reported that the Israeli authorities scaled back many of the proposals.[[10]](#footnote-10)

Since 2011, and around events during the Arab Uprising, the EU has been conducting a review of the Dual Use Regulation. In 2014 the Commission recognised the risk posed by “the emergence of specific ‘cybertools’ for mass surveillance, monitoring, tracking and interception”, while importantly also recognising “the interlinkages between human rights, peace and security”. Privacy International and other NGOs have been campaigning for the regulation to be reformed in line with the recommendations outlined at the bottom of this submission.

The Commission also initiated an impact assessment aimed at informing the policy- making process by quantifying and providing objective data on the industry and the potential cost of any regulatory changes. Ecorys, a European research and consultancy company, in partnership with SIPRI, carried out a data collection project, including a component specificaly focused on surveillance technologies, to inform the impact assessment. The report was submitted to the Commission in November 2015 and provides a broad and detailed analysis of the European market for surveillance technologies and policy issues.[[11]](#footnote-11)

Simultaneously, a Subcommittee, the Surveillance Technology Working Group (STEG), was established within the DG Trade Dual Use Working Group aimed at identifying surveillance technology that poses a risk to human rights and how it can be effectively controlled.

Any changes to the Regulation will need to be agreed upon by all member states, as well as by the European Parliament. In April 2015, the Foreign Affairs Committee of the European Parliament adopted a report by MEP Marietje Schaake on Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries, which was approved by the parliament in Autumn 2015. However, reaching a position across different member states has proved difficult, and the regulation is now unlikely to be reformed until after the European parliamentary elections in 2019. Without these reforms, outlined at the bottom of this submission, export controls will continue to be limited in use in preventing the unlawful use of surveillance technology. For example:

* Of over 330 export license applications for controlled surveillance technology made to 17 EU authorities since 2014, 317 have been granted and only 14 have been rejected; 11 member states, including France and Italy, refuse to make any licensing data available to public scrutiny, meaning that the actual amount of surveillance equipment being licensed for export is likely to be significantly more ([The Correspondent](https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153)).
* BAE Systems, the UK’s largest arms manufacturer, has been exporting controlled internet surveillance systems capable of carrying out mass surveillance to countries where human rights abuses are common, including to Saudi Arabia, UAE, Qatar, Oman, Morocco, and Algeria ([BBC and Dagbladet Information](http://www.bbc.co.uk/news/world-middle-east-40276568)).
* Italy approved then subsequently revoked an export license for an internet surveillance system to Egypt ([IlFattoQuotidiano](http://www.ilfattoquotidiano.it/2017/06/30/software-spia-il-ministero-revoca-la-licenza-di-vendita-in-egitto-di-area-spa-dopo-le-indagini-della-procura/3697495/)).
* A French company has been exporting similar internet surveillance equipment to Egypt and has received nine other export licenses in 2016 ([Telerama](http://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer%2C160452.php)).
* Companies based in Italy were filmed admitting to be willing to skirt existing export regulations to sell surveillance technology to potential clients around the world, including to countries under EU restrictive measures ([Al Jazeera](http://www.aljazeera.com/investigations/spy-merchants.html)).
* Between 2015 and September 2018, 281 license applications have been made for telecommunications interception equipment and internet monitoring systems in the UK; only nine have been rejected because of a risk of use for internal repression. Only 21% of the destinations for these exports are considered “Free” by Freedom House’s 2018 global report on political rights and civil liberties; 44% are considered “Partly Free”, while 35% of all approved licences of surveillance equipment are to destinations considered “Not Free”. ([Privacy International](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/committees-on-arms-export-controls/2017-arms-export-annual-report/written/95815.html))

In August 2015, Germany unilaterally announced a Federal amendment to its laws seeking “to stop the use of [surveillance] technology for internal repression in countries of destination.” Germany also added new surveillance items to its list of technologies which require export authorisation, covering monitoring centres and lawful interception technologies. In announcing the new regulations, the Vice Chancellor of Germany, Sigmar Gabriel, stated that “human rights violations can not only [occur] with weapons, but ultimately with technologies for example, wiretapping. So far the European regulations for the export of such technologies to other countries is sketchy. The Federal Government is therefore closing the gaps, [which are] still under discussion in Brussels. We will work in Brussels, as well as internationally, for speedy European and global regulations.”[[12]](#footnote-12) No surveillance items currently subject to unilateral control in Germany have since been added to the Wassenaar control list.

Switzerland has also taken unilateral steps. In May 2015, the Swiss Federal Council added an amendment to their export regulations which for the first time compels the export control authorities to deny all license applications for internet and phone monitoring technology if there is “a reason to believe” that the export may be used “as a means of repression”.[[13]](#footnote-13) After an investigation by Privacy International in conjunction with Swiss magazine WOZ, it was uncovered that representatives from a Bangladeshi unit dubbed a “death squad” by Human Rights Watch were being hosted in Zurich by a manufacturer of IMSI Catchers, NeoSoft. Additional Director General of RAB, Colonel Ziaul Ahsah, subsequently reported to Bangladeshi media that the export had been stopped “just before the shipment of the materials” by Switzerland after “a human rights organisation reported against RAB.”[[14]](#footnote-14) Bangladeshi government forces have since put out multiple tenders for the procurement of surveillance equipment amid a crackdown on protestors.[[15]](#footnote-15)

**Recommendations**

For governments regarding export controls regulations:

* Human rights protections should be strengthened and have definitive impact
  + Regulations should clearly specify that states are required to deny export licenses where there is a substantial risk that those exports could be used to violate human rights, where there is no legal framework in place in a destination governing the use of a surveillance item, or where the legal framework for its use falls short of international human rights law or standards. Without such criteria, states will continue to authorise licenses for export to destinations where surveillance will be used to unlawfully target civil society and others.
* All relevant surveillance technology should be covered
  + A mechanism to update the EU and other national control lists should be agreed, which will decide on updates to the control list in a transparent and consultative manner, taking into account the expertise of all stakeholders, including civil society, researchers, and international human rights law. Such a method would minimise the concerns caused by the inclusion of intrusion software in the Wassenaar list in 2013 by opening decisions to public and expert scrutiny.
* Greater transparency and reporting should be made mandatory
  + Greater transparency in export licensing data is needed. Such transparency is crucial in enabling parliaments, civil society, industry, and the broader public — both in the exporting and in recipient countries — to meaningfully scrutinise the human rights impact of the trade in dual-use items.
* Security research and security tools should be protected
  + To reinforce the protection of research (as, for example stated in the preamble of the Eruopean Commission’s proposal), regulations should include clear and enforceable safeguards for the export of information and communication technology used for internet security research.

Companies should:

* Develop a policy commitment to respect human rights, approved at the most senior level, and made publicly available.
* Carry out due diligence on any potential customers to identify, prevent and mitigate adverse human rights impact prior to agreeing to a potential transaction.
* Stipulate clear end-use assurances in contractual agreements with strong human rights safeguards that prevent against arbitrary or unlawful use of the technology.
* Carry out a periodic review of states’ use of the technology, and refuse to carry out maintenance, training, or updates if the end-use does not conform to these contractual obligations.

1. https://www.techuk.org/images/CGP\_Docs/Assessing\_Cyber\_Security\_Export\_Risks\_website\_FINAL\_3.pdf [↑](#footnote-ref-1)
2. https://www.eff.org/deeplinks/2011/10/it’s-time-know-your-customer-standards-sales-surveillance-equipment [↑](#footnote-ref-2)
3. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6616 [↑](#footnote-ref-3)
4. http://www.wassenaar.org/wp-content/uploads/2015/06/Revised-Summary-of-Changes-to-Control-Lists.pdf [↑](#footnote-ref-4)
5. https://www.wassenaar.org/app/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf [↑](#footnote-ref-5)
6. https://www.wsj.com/articles/SB10001424052970203961204577269391401776590 [↑](#footnote-ref-6)
7. https://webarchive.nationalarchives.gov.uk/20170110100622/http://www.blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf [↑](#footnote-ref-7)
8. https://medium.com/privacy-international/rights-organisations-urge-export-control-body-to-change-control-list-997c209c6aa4 [↑](#footnote-ref-8)
9. https://www.gkh-law.com/cyber-update-february-2016/ [↑](#footnote-ref-9)
10. https://www.defensenews.com/2016/01/26/israeli-govt-reaches-out-before-clamping-down-on-cyber-exports/ [↑](#footnote-ref-10)
11. https://www.sipri.org/publications/2015/other-publications/final-report-eu-dualuse-review [↑](#footnote-ref-11)
12. http://www.bmwi.de/DE/Presse/pressemitteilungen,did=719188.html [↑](#footnote-ref-12)
13. https://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=de&msg-id=57261 [↑](#footnote-ref-13)
14. http://www.newsbangladesh.com/english/Switzerland%20holds%20back%20shipping%20of%20intelligence%20gears%20for%20RAB/482 [↑](#footnote-ref-14)
15. https://privacyinternational.org/feature/2226/amid-crackdown-bangladesh-government-forces-continue-spytech-shopping-spree [↑](#footnote-ref-15)