

Export of Surveillance Technology to MENA Countries



SUMMARY:

Companies around the world—including American, European, and Israeli private firms—are selling sophisticated surveillance technology to countries in the Middle East and North Africa (MENA). Although much of this technology is characterized as “dual use” due to its ostensibly legitimate use for law enforcement, **credible** reports show that, rather than use the technology for lawful purposes, MENA countries weaponize this technology to target citizens and rivals, resulting in **harassment, imprisonment, and torture**. Additionally, some of the surveillance technology acquired in the region (like Deep Packet Inspection technology) is inherently indiscriminate, inevitably violating established legal principles of proportionality and necessity, rendering any legitimate legal use impossible (for more, see TIMEP’s Brief on Use of Surveillance Technology in MENA).

High-profile cases in which surveillance technology use has been linked to human rights violations, **like the murder of Saudi Arabian journalist Jamal Khashoggi and the arrest of UAE activist Ahmed Mansoor**, have fueled recent calls for more regulation, transparency, and corporate responsibility around use and export in this field. However, most states still lack the necessary regulatory controls to prevent such technologies from demonstrable misuse. The only current international export control framework, the **Wassenaar Arrangement**, lists the types of technology that should be regulated, but does not contain stipulations for its enforcement. Furthermore, companies and governments are generally not obligated to share details of exports, making this multimillion dollar market **a highly secretive one**.

Given the lack of a comprehensive legal framework, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, recently **called** for a moratorium on surveillance technology sales.

POLITICAL CONTEXT:

The field of surveillance technology is a rapidly expanding one: Privacy International **reports** that the number of companies in the surveillance industry rose from 246 in 2012 to 528 in 2016. Moreover, 87 percent of the firms are based in countries that are members of the Organization for Economic Co-operation and Development (OECD) and 88 percent have their headquarters in countries that participate in the Wassenaar Arrangement (see details in the Legal Context section). Israel, which has 27 companies on the list, is the country with the **highest per capita ratio** of the market. A variety of these companies export different kinds of surveillance technology to governments in the Middle East (see Table 1).

Spyware—malicious software through which regimes can remotely access phones and computers to listen to calls and read messages—has been prominent. The Israeli company NSO, for example, sold its sophisticated spyware Pegasus to Saudi Arabia and the UAE despite the absence of diplomatic ties between the countries. Saudi Arabia **used Pegasus to spy on civilians in order to target the journalist Jamal Khashoggi**, who was subsequently killed and dismembered in 2018 inside the Saudi consulate in Istanbul.

Table 1: Examples of Surveillance Technology

Country	Technology	Exporting country	Importing countries
Blue Coat	Deep Packet Inspection	United States	Syria, Bahrain, Jordan, Kuwait, Lebanon, Saudi Arabia, UAE, Qatar, Iraq, Palestine, Sudan
NSO Group	Pegasus (spyware)	Israel	Saudi Arabia, UAE, Bahrain, Morocco
Hacking Team	RCS, Crisis, DaVinci (spyware)	Italy	Morocco, Saudi Arabia, Egypt, Oman, UAE, Sudan, Bahrain, Lebanon
Area SpA	Monitoring center	Italy	Egypt, Syria
Gamma	FinFisher Suite (spyware)	United Kingdom, Germany	Bahrain, Morocco, Egypt, Jordan, Lebanon, Saudi Arabia, Oman, Qatar, UAE
Trovicor	Monitoring center	Germany	Oman, Bahrain, Tunisia, Yemen, Egypt, Syria
Nexa / Amesys	Monitoring center	France	Libya, Egypt
Sandvine	PacketLogic (Deep Packet Inspection)	Canada	Egypt

Some of these exporting companies also provide MENA governments with experts to assist them with their surveillance operations. The United Arab Emirates initially hired the Baltimore-based firm Cyberpoint, which employed former NSA agents to conduct cyber-espionage. Some of these workers were later hired by the Emirati company DarkMatter, which mainly conducted surveillance against local citizens, but spied as well on Yemeni activists and hacked an iPhone used by the Emir of Qatar, Sheikh Tamim bin Hamad al-Thani; the company also spied on U.S. citizens.

Some foreign companies install monitoring centers in the region, with which governments can intercept and scan communications. The Italian company Area SpA assisted Syrian authorities in following citizens in real time through the installation of such monitoring centers, raising concerns that the firm may have broken the European Union sanctions regime on Syria. German company Trovicor established similar centers in Bahrain, also amid human rights concerns; local activist Abdul Ghani al-Khanjar was tortured while being shown details of his personal communication, obtained through German technology.

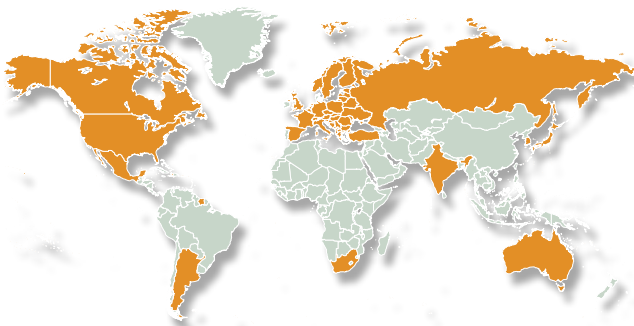
Firms sell also Deep Packet Inspection (DPI) technologies to the Middle East, allowing authorities to monitor



and redirect internet traffic. Egypt authorities have **blocked more than 34,000 pages in a single shot** using the technology sold by the Canadian company Sandvine. There are also reports that the governments of Syria and Turkey have used DPI solutions to redirect users to download spyware. The American company Blue Coat provided the Syrian regime with tools to filter internet traffic, **potentially violating the U.S. sanctions regime**.

LEGAL CONTEXT:

The Wassenaar Arrangement, created in the wake of the Cold War to set broad standards for the export of military and “dual-use” technologies by its **41 (now 42) members** (see Figure 1), was expanded to apply to surveillance technologies through a series of amendments,



most recently adopted in 2013. The arrangement includes a list of technologies which require export licenses but does not lay out parameters under which a license should be approved or denied, nor does it lay out any enforcement mechanism for member states that do not adhere to the conditions of the arrangement. Therefore, it is up to each member country to develop a domestic export control regime that is consistent with the terms of the Wassenaar Arrangement.

This has led to great variety in the domestic export control regimes that have been established (see Table 2). For example, the U.S. Department of Commerce’s Bureau of Industry and Security oversees the licensing of exports, which is implemented in accordance with the Export Administration Regulations. Exports can be controlled based on their functionality, end-use, end-user, and country of end-use. Items can be controlled for purposes of **“antiterrorism, regional stability, or crime control.”** Generally, the agency has discretion to approve or deny a license as long as it is “consistent with national security and foreign policy interests.”

In 2013, the European Union began a **review of its export control system**, noting the importance of “taking into consideration human rights” in order to create a “Europe that protects.” Since the review began, the European Commission and Parliament have been moving towards stricter export controls on surveillance technologies, but have met resistance from member states; in May 2019, Germany and other member states were reported to have **prevented** reform measures that would restrict export from being adopted by the EU. Nevertheless, individual member states may already impose laws which provide safeguards over the trade: British law, for example, states that the government cannot approve an export if there is a “clear risk” that it might be used for internal repression or would violate international humanitarian law. In the Department for International Trade’s **United Kingdom Strategic Export Control Lists**, there is a list of capital punishment and torture goods that implements controls based on the potential abuse of human rights and fundamental freedoms that was formulated in conjunction with the EU Human Rights Lists. While this equipment is currently subject to licensing restrictions, activists argue that the criteria which governs how the licenses are assessed are permissive, not suited for surveillance technology, and set an overly high bar for an application to be refused. As a result, out of 284 license applications made between 2015 and September 2018 in the UK for the export of surveillance technologies, only nine have been rejected because of a risk of use for internal repression. Only 21 percent of the destinations for these exports are considered “free” by Freedom House’s 2018 global report on political rights and civil liberties; 44 percent are considered “partly free”, while 35 percent of all approved licenses of surveillance equipment are to destinations considered “not free”.

A lack of transparency is fairly consistent across export regimes, particularly regarding decisions to allow or deny an export of a specific technology. Although there are procedures in place across government agencies, the reasons why exports are ultimately approved are not publicized, and data about licensing decisions—which would allow people to see which equipment has been approved for export and where—is not made publicly available. Currently, the UK and Switzerland are the only countries that proactively provide detailed licensing data about surveillance technology within their domestic export control regimes.

Some lawyers and policy experts have argued that **domestic export controls** should be better defined and should include reporting requirements for states. Additionally, they argue that export controls should be developed with input from the larger security sector, including organizations from civil society, in order to ensure that international human rights obligations are taken into account.

Table 2: Examples of Relevant Export Controls

Country	Controls
United States	According to the Export Controls Act of 2018 , the Department of Commerce's Bureau of Industry and Security oversees the licensing of these exports. The Departments of Commerce, Defense, State, and Energy may approve or deny a license as long as it is "consistent with national security and foreign policy interests."
Israel	According to the Import and Export Order of 2006 , a license is required by the Ministry of Defense to export "dual-use goods, technology and services." Both the Ministry of Defense and the Ministry of Foreign Affairs shall review the license application for its "security implications, or implications on the foreign relations policy."
France	According to the Decree No. 2001-1192 , the Ministry of Defense and the Ministry of Economy's Dual Use-Goods Service (SBDU) oversee France's export license process, consistent with European Union Community Regulation No 428 of 2009 , which sets out the general licensing framework for EU member states to follow. Licenses are granted based on the character of the technology and its end destination.
Germany	According to the War Weapons Control Act , the Federal Office of Economics and Export Control (BAFA) is in charge of export licensing, consistent with European Union Community Regulation No 428 of 2009 . For dual-use items, licenses are granted if they do not "impair the foreign policy and security interests" of the country. Information on the intended use of the item and the exporter's reliability are taken into consideration when evaluating a license application.
United Kingdom	The Export Control Joint Unit (EJCU) is in charge of granting export licenses for dual-use items. The EJCU includes a variety of reasons for requiring export licenses , including "concerns about internal repression, regional instability or other human rights violations," in addition to national security.
Italy	According to Legislative Decree No. 221 of 2018 , the Ministry of Economic Development (MISE) is tasked with granting export licenses for dual-use technologies. Anti-torture regulations are taken into account when granting certain types of authorizations, in addition the "public security and the protection of human rights."



International human rights legal obligations also mandate that states protect against human rights abuses within their territory and jurisdiction and stipulate that states have the duty to protect against abuses by third parties, including businesses. The [UN Guiding Principles on Business and Human Rights](#) further expands on this duty for states, as well as on the duties of companies. When companies export surveillance technology that is used to perpetuate human rights abuses, both the companies and states involved may arguably be liable if sufficient action was not taken to conduct due diligence to prevent such abuses.

Given the absence of a comprehensive international framework that would set forth binding rules for the export of surveillance technology, in a [recent report](#), United Nations Special Rapporteur David Kaye called for a moratorium on surveillance technology sales until the international community finds new ways to regulate it.

TREND ANALYSIS:

Having witnessed the transformative potential of web technology in the past decade, authoritarian regimes have stepped up their efforts to discipline and punish non-violent actors in cyberspace. This trend has [opened up a lucrative market](#) for firms in the field of surveillance technology, with a proliferation of companies in the past several years.

While there is a growing call for greater regulation from civil society organizations and some regional and international bodies, such as the European Parliament and the United Nations, there appears to be insufficient political will to [go beyond the Wassenaar Arrangement](#) and treat surveillance technology with sufficient rigor to ensure that abuses are prevented or that perpetrators are held to account.

The [lack of transparency](#) on the exports and use of surveillance technology, in the meantime, makes it hard to properly assess the scope and trajectory of this crisis. Most of the information currently available is anecdotal, coming from journalists and organizations such as the Citizen Lab, and there is a sense that much of surveillance activity, as well as its impact, still goes unnoticed.

IMPLICATIONS:

The export of surveillance technology to MENA governments has led to violations of the rights to life, privacy, and freedom of speech, among others, imperiling journalists, activists, and researchers. The growing awareness around the use of surveillance technology also leads to concerns around feelings of intimidation and self-censorship in the MENA region. This dynamic has already caused individuals to become [more reluctant to talk to journalists](#), discouraged research initiatives, and contributed to a climate of fear and mistrust, all of which carry reverberating negative implications for the vitality of a free press, active civil society, and individual and societal well-being. This situation further impedes a clear and critical global understanding of developments in the whole region.

The fact that these technologies ostensibly have [legitimate uses](#), among them law enforcement, makes regulation particularly complicated. Because the Wassenaar Arrangement is not binding, countries are left to determine domestic export licensing processes, which creates an inherent [asymmetry](#). The few existing domestic export control regimes are vague and do not include stipulations for punishing transgressions, even in cases in which these technologies are clearly linked to human rights violations.

This absence of a binding international legal framework to clearly outline obligations and ensure transparency has led to a regulatory “Wild West” where there are little to no controls over use of technology once a company has already made the transaction, and in which states that implement stricter regulations risk the

flight of those companies to states with lower barriers in a potential “race to the bottom.” These concerns risk exacerbation as the market for surveillance technology continues to expand, seeing a proliferation of companies and an entrenchment of corporate interest in maintaining an unregulated environment.

Finally and most immediately, measures to guarantee transparency are of the utmost importance in order to clarify the role that governments and corporations play in the export process, in order to understand how these surveillance technologies are being used by importing countries to propagate human rights abuses, and in order to hold exporting governments and corporations accountable for their role in any abuses.

TIMEP COVERAGE:

- “Use of Surveillance Technology in MENA” (TIMEP Brief)
- “Social Media and Online Surveillance: Egypt and Abroad” (Commentary by Ahmed Ezzat)
- “In the Era of ‘Fake News,’ Egypt Monitors and Silences” (Commentary by Mai el Sadany)

