fidh

SURVEILLANCE TECHNOLOGIES "MADE IN EUROPE":

Regulation Needed to Prevent Human Rights Abuses

POSITION PAPER

Article 1: All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood. Article 2: Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty. Article 3: Everyone has the right to life, liberty and security of person. Article 4: No one shall be held in slavery or servitude; slavery and the slave trade shall be prohibited in all their forms. Article 5: No one shall be subjected to torture or to cruel,

December 2014 / N°648a

"Innovations in technology have facilitated increased possibilities for communication and freedom of expression, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have also provided new opportunities for State surveillance and interference with individuals' private lives."[1]

Frank la Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression

Introduction

The Amesys case[2] and other recent scandals have recently raised concerns over the growing global trend of the use by governments of sophisticated technological equipment and programmes to systematically persecute human rights defenders, dissidents, and political opponents. Such serious human rights abuses triggered debates on the roles and responsibilities of European information and communication technologies (ICT) companies. These companies provide products and services to oppressive and authoritarian regimes, thereby enabling the monitoring and surveillance of communications. Used as means of repression, the use of these products and services has seen an increase over the last decade and have become powerful tools in the hands of regimes curtailing human rights and disregarding respect for the rule of law. Companies developing and selling surveillance technologies have long been able to avoid the limelight. Several reports by non-governmental organisations (NGOs) and journalists suggest that this trend is now spreading globally, and that surveillance tools are being used as means of repression in diverse countries, including Bahrain, Egypt, Ethiopia, Morocco and Turkmenistan.[3] Most of the technologies used in Northern Africa and the Middle East have been provided by European companies.

"They mentioned things only me and my friends knew about. I believe they got personal messages sent through the Internet."

J. 40 years old, arrested on 10 February 2011 in Benghazi (Libya) and tortured during 11 days

The obligation of States to protect human rights, together with the corporate responsibility to respect human rights as set out in the UN Guiding Principles on Business and Human Rights, are now widely recognised. Gravely concerned about human rights violations resulting from the development and irresponsible sale and export of surveillance technologies, **this paper aims to address the need for stronger regulation at the EU and at the international level to prevent further violations of fundamental human rights resulting from the trade of such technologies and to ensure that victims can obtain justice.** This paper focuses on the trade of surveillance technologies and does not look at broader human rights issues relevant to the ICT sector, such as issues related to censorship. While cases evoked in this paper involve interceptions made on social networks and communication tools such as Facebook and Skype, the role of such ICT companies in these situations is not discussed in this paper.[4]

The first section provides an overview of some of the different types of surveillance and censorship technologies sold by companies that can lead to human rights abuses. The following sections map the current EU legal and policy frameworks; highlight how these are insufficient to ensure that such trade of ICT technologies does not contribute to human rights abuses; and finally, formulate options for regulation in line with the EU's human rights obligations. Recommendations particularly focus on EU member States as "home States" of European ICT

1. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, HRCouncil/ Session23/A.HRC.23.40.
2. See case study chapter 4.
3. See notably Tim Maurer, Edin Omanovic and Ben Wagner, "Uncontrolled Global Surveillance : Updating Export Controls to the Digital Age", Open Technology Institute, Digitale Gesellschaft, Privacy International, March 2014.
4. For FIDH's litigation work around the protection of personal data (re PRISM), please refer to : http://www.fidh.org/Surveillance

companies exporting surveillance technology, and include recommendations to regulate these companies' activities and restrict the trade of surveillance technologies.

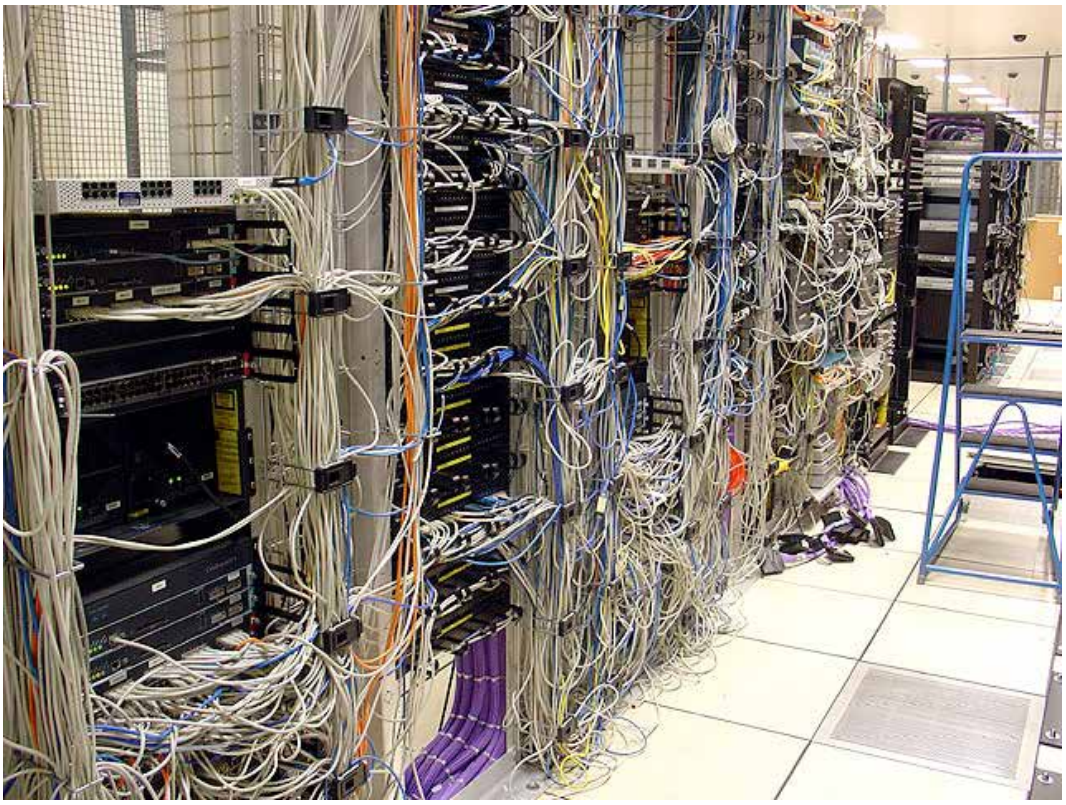
This position paper builds on FIDH's work before French courts[5] representing victims' of abuses allegedly committed by – or with the contribution of – companies selling surveillance technologies and builds on discussions held during an expert seminar organised by FIDH in Brussels (Belgium) in April 2014. Experts from the European Commission, academic experts, and civil society representatives participated in the seminar. It marked the official launch of CAUSE, the Coalition Against Unlawful Surveillance Exports, bringing together non-governmental organisations (NGOs) and experts such as Privacy International, Amnesty International, Human Rights Watch, Digitale Gesellschaft, Open Technology Institute, and Reporters without Borders.[6]

5. See the Amesys and Qosmos cases described below.
6. CAUSE (Coalition Against Unlawful Surveillance Exports), http://www.globalcause.net/

CHAPTER 1

Surveillance technologies and companies: quick overview of the sector

As defined in the EU-commissioned sector guide, the term information and communication technologies (ICT) sector is "an expanded form of the information technology (IT) sector. The sector includes **products** and their **components** for information processing and communication (including transmission and display) using electronic processing to detect, measure, record and control physical processes. This includes products ranging from mobile telecommunication equipment, hardware computing equipment of all types, cabling, transmission towers and masts and other telecommunication infrastructure. The sector also covers **services** intended to enable the function of information processing and communication electronically. This includes service companies ranging from those providing access to networks, securing data in the electronic space, providing space for users to create and share data, images, and other files, providing the software architecture to navigate the world wide web and means with which users can search for information on the Internet, and providing the software and operating systems running these various products themselves. The telephone, cable, and computer networks at the heart of the technology have increasingly converged at a rapid pace, and many companies provide unified services, under single ownership, distribution, or management.[7]"



© Credit Me

7. Institute for Human Rights and Business (IHRB) and Shift, "Corporate Responsibility to Respect Human Rights Sector Guidance Project - ICT Sector Discussion Paper for Public Comment", 24 May 2012. For more, see: http://www.ihrb.org/pdf/roundtable-discussion-papers/ICT-Sector-Roundtable-Discussion-Paper-For-Public-Comment.pdf

Scoping surveillance technology

The spread of ICT surveillance and censorship technology in the past decade has been facilitated by the dramatically reduced costs of massive data storing and processing. Governments can collect data from people's emails, real-time online conversation programmes and calls, telephone calls, webcams, social media profiles, etc., through aggressive surveillance software or requests to Internet and phone providers.

In order to give an overview of known surveillance and censorship technology, this section maps out some of the technology and relating human rights concerns. An amended analytical framework for assessing potential impacts of company activities from the European Commission's Guide for the ICT Sector[8] provides a useful starting point. The framework highlights some sensible categories of ICT technologies. On the **hardware side** of the spectrum there are: **Device Manufacturing** and **Component and Network Equipment Manufacturing and Management**. On the **software side**: **Network Management** and **Management of Connectivity/Access.** The category of **Intrusion Software** could also be added as a category of its own, encompassing surveillance and censorship software, which can aggressively infect computers and devices. This type of spyware or malware acts essentially as a Trojan and makes it easy to bypass encryption. In addition, there are companies which offer to deliver, set-up, and maintain entire monitoring centres or systems, which are a combination of categories.

Device Manufacturers are companies that manufacture or sell cell phones and other mobile devices, computers and related equipment, as well as other consumer electronics, such as digital cameras. The **Component and Network Equipment Manufacturing** category encompasses companies that produce telecommunications components and network equipment, such as semiconductors, cell phone masts, switchers, and routers. **Network management** is the largest category, which includes telecommunications services, wireless and internet service providers, but also provides services which monitor network activity, manage Lawful Interception (LI) interfaces, and that are capable of Deep Packet Inspection (DPI). DPI is a sophisticated method of filtering, used to inspect data packets transmitted over an Internet network (often on a nationwide scale).

Lastly, the category of **Management of Connectivity/Access** are companies that provide web-based services and platforms, such as search engines, social networking, emails, and cloud computing, the latter being the practice of delivering on-demand computing resources over the Internet, by means of data centre services for instance.

Despite the obvious beneficial effects brought by technological developments globally, surveillance technologies potentially

What kind of surveillance do these technologies enable?

- **Device Manufacturing and Network Equipment:** Backdoors into widely-used computer hardware can compromise data and communication**.**
- **Network Management**: Systems can be used to monitor, mediate and modify data traffic in real time, allowing surveillance of communication and the gathering of personal information.
- **Intrusion software**: Real time surveillance of communications and location of those participating in the communication. Can access all stored information and monitor even encrypted communication. Keystrokes can be logged, conversations recorded, and cameras and microphones can be activated remotely.
- **Management of Connectivity/Access:** Critical vulnerabilities in web-based services can allow the monitoring of events and communication.
- **IMSI catcher (International Mobile Subscriber Identity):** Interception of mobile phone traffic and tracking of user.

8. For more, see: "European Commission (EC) ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights". http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

generate direct and indirect human rights abuses. They can therefore directly violate fundamental human rights, such as the right to freedom of expression and opinion, the right to privacy, freedom of assembly, and the right to be free from inhumane, cruel and degrading treatment. As highlighted in the following table, such human rights violations can occur through the use of programmes and services such as spyware and malware programmes enabling surveillance. Furthermore, enhanced surveillance technological capabilities can lead to grave human rights violations. For example, the tracking of activists in Bahrain using the FinSpy toolset led to cases of imprisonment and torture.[9]

The use of intrusive surveillance technologies and network monitoring systems sold by European companies has also been widely documented in Syria and Ethiopia, though it appears that these countries would be no exceptions. A recent report suggests that between 2003 and 2013 German companies alone exported "surveillance technologies to Albania, Argentina, Chile, India, Indonesia, Qatar, Kosovo, Kuwait, Lebanon, Malaysia, Morocco, Mexico, Norway, Oman, Pakistan, Russia, Saudi Arabia, Switzerland, Singapore, Taiwan, Turkey, Turkmenistan, USA, and the UAE".[10]

It appears that numerous European-based companies are engaged in the sale and export of surveillance technologies. These technologies can be used to suppress dissidents both in their home states and abroad, and can lead to extreme self-censoring habits amongst local population. Unfettered surveillance of a person's communications gives a government a hitherto unprecedented control over its citizens, and has led to threats, intimidations, arbitrary detentions, and in some cases, torture.

The following table presents some companies allegedly involved in providing surveillance equipment and/or services which are known to be associated with human rights violations. While documentation shows that there are many more companies involved, this table only offers a brief and incomplete overview.[11]

9. For more on these cases, see: Jamie Doward, UK company's spyware used against Bahrain activist, court papers claim, World News, The Guardian, 12 May 2013; William Marczak, John Scott-Railton, Morgan Marquis-Boire, Vern Paxson "When Governments Hack Opponents: A Look at Actors and Technology", Proc. 23rd USENIX Security Symposium (Sec '14), San Diego, CA, August 2014.
10. Ben Wagner and Claudio Guarnieri, "German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions", Global Voices, September 2014.
11. For a more complete overview see the repository Bugged Planet: http://buggedplanet.info/

Company	Products & services	Category	Allegedly used in (host countries) :	Home States involved
Amesys	EAGLE system (Monitoring Centres, Internet Monitoring, Audio Surveillance and Location Monitoring technology)	Network management	Lybia, Morocco , Qatar, France	France
Bull/Nexa Technologies	Network analysis systems, communications, monitoring technology, lawful interception interface	Network management		France
Qosmos SA	Network analysis systems	Network management	Syria	France
Gamma Group	FinFisher Suite (Monitoring Centres, Communications Monitoring, Technical Surveillance and Intrusion technology)	Intrusion Software	Bahrain, Ethiopia, Indonesia, India, Turkmenistan, Malaysia	Germany - UK
Trovicor	Monitoring Centres	Network Management, Intrusion software	India, Bahrain	Germany
Utimaco	Lawful interception interface, monitoring centres, communications monitoring	Network Management	Iran, Syria, Tunisia	Germany
Elaman	Communication monitoring, intelligence gathering	Intrusion software	Turkmenistan, Oman	Germany
CelarTrail Technologies	Monitoring centres, communications monitoring technology, lawful interception interface	Intrusion software Network Management	India	India
NICE	Monitoring centres, communications monitoring, biometrics and location monitoring technology	Network management	Russia	Israel
Hacking Team	DaVinci : Intrusion technology	Intrusion sofware	Azerbaijan, Kazakhstan, Nigeria, Oman, Saudi Arabia, Sudan, Uzbekistan, Turkey, Morocco, United Arab Emirates, Colombia	Italy
VASTech	Zebra System (Monitoring centres, communications monitoring technology)	Network Management	Libya, Egypt	South Africa
Dreamlab	Internet Monitoring Technology	Network Management	Oman, Turkmenistan	Switzerland
NeoSoft	Training and surveillance equipment	Mobile monitoring systems	Bangladesh	Switzerland
Cobham	Monitoring centres, phone monitoring, technical surveillance and location monitoring technology	Network Management, Intrusion software	Gulf countries	UK
Narus	Internet monitoring technology	Network Management	Egypt, Saudi Arabia, Pakistan	USA
Verint	Monitoring centres, Communications monitoring, video surveillance and location monitoring technology	Network Management, Device manufacturing	Democratic Republic of Congo, the United Arab Emirates, Zimbabwe	USA

For more on the surveillance industry, please refer to the Surveillance Index hosted by Privacy International:

https://www.privacyinternational.org/sii/companies

CHAPTER 2
Current EU Legal and Policy Framework

During the past five years and in the wake of the Arab Springs, the EU has increasingly tackled issues at the crossroads of human rights and ICTs. This section provides an overview of the current EU legal and policy framework related to surveillance technologies, with a view of identifying additional policy and legal measures needed to adequately address challenges posed by the irresponsible trade and export of surveillance technologies.

The No Disconnect Strategy

The EU strategy with regard to communications technologies and human rights is the No Disconnect Strategy (NDS). This strategy was announced by the European Commission in December 2011 to address the restrictions and disruptions through ICTs, including the Internet, employed by authorities during the Arab Springs to control and silence protesters. This strategy is based on four pillars:

1. Supporting the development of technological tools to circumvent surveillance in non-democratic countries.
2. Educating activists and raising awareness on the potential benefits and risks of using ICTs.
3. Providing high quality intelligence on the development of Internet freedom in non-democratic regimes.
4. Strengthening cooperation between all actors involved in this field (companies, third countries, etc.)

With this strategy, it is the first time that the European Commission has attempted to specifically address the issues of human rights defenders facing surveillance and censorship "in third countries". While the strategy intends to assist civil society organisations and individual citizens to circumvent arbitrary disruptions on the Internet, and could be a useful tool to protect individuals, such as human rights defenders, it remains limited and inadequate to address the potential human rights abuses resulting from the sale and use of surveillance technologies. To ensure the coherence and efficiency of its policies, the EU should, as will be explained below, ensure that while it is supporting defenders on digital security and the use of encryption tools, its member States are not providing third countries with sophisticated and unregulated surveillance technologies.

EU Strategic framework and action plan on human rights and democracy

In June 2012, the EU adopted a new strategic framework and action plan on human rights and democracy. One of the main goals of this framework is to promote human rights in all EU external policies, including trade, technology, and the Internet. Article 24 of the Action Plan clearly addresses how the EU intends to address the rising human rights challenges posed by ICTs:

(a) Develop new public guidelines on freedom of expression, both online and offline, which include the protection of bloggers and journalists;
(b) Develop measures and tools to expand internet access; openness and resilience to address indiscriminate censorship or mass surveillance through ICTs; and to empower stakeholders to use ICTs to promote human rights, while taking into account privacy and personal data protection at the same time;

(c) Ensure that a clear human rights perspective and impact assessment is present in the development of policies and programmes relating to cyber security, the fight against cybercrime, internet governance, and other EU policies in this regard;

(d) Include human rights violations as one of the reasons following which non-listed items may be subject to export restrictions by Member States.[12]

Together with the EU regulation on dual-use items, discussed below, article 24 of the Action Plan - most particularly article 24 (c) and (d) - could be useful when it comes to dealing with the protection of defenders, opponents, and journalists targeted by the use of surveillance technologies. The European Commission is increasingly investing financial resources to develop tools for human rights defenders facing surveillance. It is also mobilising considerable resources to fight against cybercrime and to develop cyber-defence programmes, including the development of technologies such as intrusion software and IP surveillance systems. One of the key questions remaining, in addition to the one of how to ensure the effective implementation of the 2013-2014 Action Plan, is how can the EU ensure the effective implementation of its policies while ensuring that its strategies do not lead to human rights violations.

EU CSR Communication: Human rights guidance for ICT companies

In October 2011, the European Commission published its new CSR Communication: "A Renewed EU Strategy 2011-2014 for Corporate Social Responsibility".[13] Adapting its CSR definition to reflect internationally recognised principles and guidelines, the communication **recognises the need for a mix of both voluntary and regulatory measures** to ensure corporate accountability. FIDH, a steering group member of the European Coalition for Corporate Justice (ECCJ), has nevertheless criticised the EU for failing to adopt stronger measures to ensure the EU and its Member States uphold their obligations to protect against human rights abuses involving European businesses.[14] A new communication is expected to be published in 2015.

The EU has endorsed the UN Guiding Principles on Business and Human Rights (UNGPs). As part of its agenda for action, the EU commissioned the development of three sector-specific guides on the corporate responsibility to respect human rights under the UNGPs, one of which focuses on the ICT sector.[15]

As per the UNGPs, companies are expected to respect human rights at all times and throughout their operations, including when host States fail to uphold their own human rights obligations. Companies are expected to, through due diligence measures, "[...] identify, prevent, mitigate and account for how they address adverse human rights impacts [...]" which they may "cause or

12. Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy", June 2012. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

13. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A renewed EU strategy 2011-2014 for Corporate Social Responsibility, Brussels, 25 October 2011, COM(2011)681 final, http://ec.europa.eu/enterprise/newsroom/cf/_getdocument.cfm?doc_id=7010

14. ECCJ, "The EU must take further steps to hold companies accountable", 25 October 2011, http://www.corporatejustice.org/csr-communication-eccj-reaction.html

15. EU Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights (2013): http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

contribute to through [their] own activities, or which may be directly linked to their operations, products, or services by their business relationships".[16]

The sector guide identifies a number of human rights risk areas in the ICT sector including the challenges that arise from regulations which lag behind technological developments. If misused, these regulations could have negative impacts on human rights. The guide also addresses the challenge of responding to government requests for information about customers and users that are not in line with international human rights law.

In terms of practical implementation, the guide identifies six core elements of the responsibility to respect human rights under the UNGPs, including public human rights policies, and the assessment of real and potential human rights impacts. Human rights impact assessments should be achieved by understanding the operating context and the remediation of negative impacts the company has caused or contributed to.

However, the guide does not specifically address challenges posed by the trade of surveillance technologies and the related expectations as to how companies should behave in order to comply with their responsibility to respect human rights. At a seminar of experts organised by FIDH in April 2014, while recognising the relevance of such guidance, participants questioned the efficacy of voluntary guidance to prevent human rights abuses in the context of surveillance technologies, given the inherent nature of products and services being sold and the serious human rights risks related to these. In a position paper published in March 2014, FIDH also illustrated, through the Amesys case,[17] how the current international framework on business and human rights, based on the UN Guiding Principles on Business and Human Rights, was insufficient to address human rights violations resulting from the trade and selling of surveillance technologies to repressive regimes.[18]

EU Framework on Trade Restrictive Measures

There are two main ways which the EU uses to impose restrictions on trade: sanctions and exports controls. Recently, the EU has adopted sanction regimes targeting third countries that include surveillance technologies. In January 2012 and March 2012, the Council adopted regulations imposing a ban on the sale, supply, transfer and export of surveillance equipment, technology or software in (or for use in) Syria and Iran. These instances remain, however, two exceptions as these technologies are not systematically included in EU embargoes on equipment that might be used for internal repression, such as the sanctions targeting Belarus, Burma/Myanmar[19] and Zimbabwe. As stated in a recent report published jointly by OTI, Privacy International, and Digitale Gesellschaft, "the fact that surveillance technology has only been included in the regimes targeting Iran and Syria and not across all restrictive measures is problematic. EU embargoes on equipment that might be used for internal repression – a category in which

16. UN Guiding Principles on Business and Human Rights, Principle 17.
17. Explained below.
18. See FIDH, "Business and Human Rights : Enhancing Standards and Ensuring Redress", Briefing paper, March 2014, https://www.fidh.org/en/united-nations/human-rights-council/un-human-rights-council-25th-regular-session/14899-business-and-human-rights-fidh-calls-on-the-international-community-to
19. In 2013, the EU lifted all trade, economic and individual sanctions regarding Burma/Myanmar, except the arms embargo.

surveillance technology should fall but currently does not – have however been adopted more widely, and it is appropriate that this list be expanded to include surveillance technology".[20]

Human rights NGOs are not alone in calling for the ban of surveillance technology exports to other countries than Iran and Syria. The European Parliament has, on several occasions, called for an EU-wide ban on the export of such technologies to countries where they could be used for human rights violations. For instance, the European Parliament adopted a resolution on 17 July 2014 that called for "an EU-wide ban on the export of intrusion and surveillance technologies to Egypt which could be used to spy on and repress citizens". In line with the Wassenaar Arrangement, it also called for a ban on the export of security equipment or military aid that could be used to suppress peaceful protests.[21]

Beyond sanctions policies, the EU aims to control the spread of surveillance technologies through dual-use export controls.

EU export control through dual-use technologies

Dual-use items are goods, software, and technology normally used for civilian purposes but which may also have military use, or may contribute to the proliferation of weapons of mass destruction. The EU Dual-Use Regulation implements the control lists of dual-use items that are agreed by the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG), the Australia Group, the Chemical Weapons Convention (CWC), and the Wassenaar Arrangement. The EU export controls regime is governed by Council Regulation (EC) N°428/2009. This Regulation was originally designed from an engineering standpoint to prevent the construction of nuclear, chemical, and biological weapons. Similarly as in these cases, digital technologies normally used for civilian purposes can also be used for malicious purposes.

The recent proliferation of surveillance technologies and software, which can be as harmful as weapons and often originate in the EU, has sparked some promising initiatives for more specific dual-use legislation.

The Wassenaar Arrangement

The Wassenaar Arrangement is a voluntary export regime whose 41 parties,[22] among which the US, Russia and all the EU Member States (except Cyprus), exchange information on the transfer of conventional weapons and dual-use goods and technologies. This Arrangement consists mainly of two different lists, one of them being the List of Dual-Use Goods and Technologies, on which export controls are based.

20. Maurer, Tim, Edin Omanovic, and Ben Wagner. 2014. Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age. Washington D.C.
21. For more, see : http://www.europarl.europa.eu/document/activities/cont/201409/20140930ATT90282/20140930ATT90282EN.pdf
22. Austria, Canada, Costa Rica, Czech Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Kenya, Latvia, the Republic of Maldives, Mexico, Moldova, Mongolia, The Netherlands, Sweden, Tunisia, the United Kingdom, and the United States.

© r2hox

While the Wassenaar Arrangement is a voluntary instrument, it has implications on the EU Dual-Use Regulation as well as on its Member States, expected to align their legal requirements with the list of items to the Regulation. The challenge, therefore, remains the implementation of new provisions by the EU and by the national legal systems of Member States.

In the early 2000s, surveillance technologies such as surreptitious listening devices as well as IMSI catchers began to be controlled through this Arrangement. More recently, at the 19th plenary meeting of the Wassenaar Arrangement in Austria in December 2013, new export controls were adopted by all participating states on two types of surveillance technologies: "intrusion software" and "IP network surveillance system". It must be noted that these new provisions originated respectively from the British and French governments. In the case of France, the decision to propose the inclusion of a new category was partly motivated by debates triggered after FIDH and its member organisation LDH filed two complaints against French ICT companies: one against Amesys for alleged complicity in acts of torture against opposition politicians, citizens and journalists in Libya, and one against Qosmos for allegedly supplying telecom surveillance systems to the Syrian regime.[23] Alluding directly to these two cases, Fleur Pellerin, the then Deputy Minister for the Digital Economy in France, expressed the intention of the French government to tighten regulations on the export of surveillance technologies.

On 22 October 2014, the European Commission finally announced the update of the EU list of dual-use items, in line with the latest Wassenaar amendments and which "reflects growing security concerns regarding the use of surveillance technology and cybertools that could be misused in violation of human rights or against the EU's security"[24]. The updated list introduces controls for new categories of items such as IT intrusion software ('spyware') and IP surveillance equipment. Provided there are no objections from the European Parliament or the Council, it should enter into force in December 2014.

23. See Section V. Avenues for holding ICT companies accountable through litigation and/or non-judicial mechanisms.
24. For more, see : http://trade.ec.europa.eu/doclib/press/index.cfm?id=1166&title=Commission-updates-EU-control-list-on-dual-use-items

The EU Dual-Use Regulation

The EU Regulation (EC) N°428/2009, the EU Dual-Use Regulation, currently leaves it to each of the EU Member States to implement the Regulation at the national level, which explains why it can create legal fragmentation.

Since the adoption of the Lisbon Treaty, the Council and the European Parliament share co-decision powers over any updates to the EU Dual-Use Regulation. Under the leadership of Dutch MEP Marietje Schaake, the European Parliament has recently adopted amendments and resolutions favouring stricter export controls for surveillance technology.[25]

The European Commission and Council have at times been reluctant to take up proposals from the European Parliament to include the digital technologies in question in the EU Dual-Use Regulation. By doing so, the Commission has created a stark discrepancy between the EU's human rights strategy and the real human rights implications resulting from the application of these technologies.

The EU dual-use export control system is currently undergoing a major review, as a result of the recent empowerment of the European Commission to unilaterally update the Dual-Use Regulation, without waiting for the two co-decision powers, the Council and the European Parliament, to legislate when new dual-use items are included to international control lists. Part of the current review aims at integrating the enforcement and the oversight of dual-use export controls between Member States.[26]

In Article 8 of the Dual-Use Regulation, Member States are allowed to impose an authorisation requirement on the export of non-listed dual-use items for reasons of public security or human rights considerations. If they make use of such provision, Member States must inform the EU Commission. These "catch-all clauses" are significant, but have rarely been used by Member States.[27] In order to avoid fragmentation between different EU countries, the application of such authorisation requirements should not remain limited to one single country, but should apply to all Member States. The efficiency of the "catch-all" clauses to control the export of technologies requires the establishment of an EU-wide ad-hoc licensing requirement (see recommendations below). Developing the use of these catch-all clauses in the EU would also require looking more closely at the technological specifications of digital goods, combined with the context in which they are going to be used. For now, the EU should be reminded that Syria and Iran are the only countries to which Member States are no longer exporting surveillance and monitoring technologies, in addition to a plethora of other goods.[28]

---

25. European Parliament resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI)); Regulation (EU) No 599/2014 of the European Parliament and of the Council amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

26. See Council conclusions on the Review of Export Control Policy, Foreign Affairs Council, 21 November 2014, Brussels. See also "MEP Schaake: more must be done for effective export controls dangerous technologies", http://www.marietjeschaake.eu/2014/11/mep-more-must-be-done-for-effective-export-controls-dangerous-technologies/

27. For examples of the use of such catch-all clauses in countries like Italy and the UK, refer to: Tim Maurer, Edin Omanovic, and Ben Wagner. 2014. Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age. Washington D.C.

28. Council Regulation (EU) No 264/2012 of 23 March 2012 amending Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran and introducing export restrictions on ICTs and monitoring tools. Council Regulation (EU) No 36/2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011 of 18 January 2012 and introducing export restrictions on ICTs and monitoring tools

The necessity to ensure legal harmonisation throughout the Member States is further reinforced by the fact that companies are currently able to circumvent controls by using subsidiaries from countries where regulations are less strict. This situation was highlighted in 2013 by the London-based NGO Privacy International, which exposed how surveillance companies were increasingly turning to Switzerland in order to export their products.[29] After facing intense scrutiny from the media and members of the Swiss Parliament, the government changed its position and recently referred the Swiss company Neosoft for prosecution after Privacy International and the national media uncovered evidence that the company may have been involved in selling mobile phone surveillance equipment, as well as training programs for a governmental unit in Bangladesh which were then implicated in wide-scale human rights abuses.[30]

Moreover, the provision excluding the requirement of an export license for equipment intended for marketing use should be cautiously scrutinised. For instance, when it was revealed that pro-democracy activists in Bahrain had been targeted by FinSpy (a malware sold by the company Gamma International), the company claimed it was not responsible for these attacks, by laying the blame on an old demonstration version.[31]

Finally, and despite the fact that research shows "many of the surveillance tech services […] are systems that require a lot of maintenance and technical support",[32] the regulation of services is currently explicitly excluded from the EU Dual-Use Regulation.

Increasingly aware of the weaknesses of current export controls, the EU has recently initiated an export control policy review to update the EU Dual-Use Regulation. In this context, the EU adopted on April 2014 a Communication to set out policy options for improving current controls on the export of dual-use items, such as surveillance technologies.[33] These options will now be subject to an impact assessment, with a view of presenting a proposal for a revised regulation in 2015.[34] Among the three key review areas on which the impact assessment will focus, it is encouraging to see included as a major focus "the impact of the introduction of a new dimension in EU export control in the form of new controls on Information and Communication Technologies (ICTs) that may be used in violation of human rights or against the EU's security".[35] On 21 November 2014, the EU Foreign Affairs Council recognized that the export of certain ICT technologies "could be used in connection with human rights violations as well as to undermine the international security, particularly as regards technologies used for mass-surveillance, monitoring, tracking, tracing and censorship. […]". The Council notes that controls on non-listed dual-use items are an essential part of controls. Member States should

29. Privacy International, "After Gamma revelations, Switzerland begins to debate export of surveillance tech", blog, 4 October 2014, https://www.privacyinternational.org/news/blog/after-gamma-revelations-switzerland-begins-to-debate-export-of-surveillance-tech

30. For more, see : https://www.privacyinternational.org:4443/blog/surveillance-company-neosoft-referred-for-prosection-by-swiss-authorities-over-deal-with-brutal

31. Gamma International spokesperson said: "it is unlikely that it was an installed system used by one of our clients but rather that a copy of an old FinSpy demo version was made during a presentation and that this copy was modified and then used elsewhere," For more see: http://www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-maybe-stolen-copy.html

32. See Tim Maurer, Edin Omanovic and Ben Wagner, "Uncontrolled Global Surveillance : Updating Export Controls to the Digital Age", Open Technology Institute, Digitale Gesellschaft, Privacy International, March 2014.

33. For more, see: http://trade.ec.europa.eu/doclib/docs/2014/april/tradoc_152446.pdf

34. Joint answer given on 13 June 2014 by High Representative/Vice President Ashton on behalf of the Commission, to the parliamentary question (2 April 2014) of MEP Marietje Schaake. For more see: http://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2014-004120&language=EN

35. For more, see: http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152697.pdf

consider whether the application of "catch all" controls council be further developed, while acknowledging at the same time that the instrument is aimed at specific cases.[36]

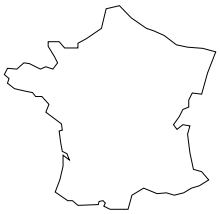
All the above highlights the necessity for a concerted and coordinated international response to address challenges posed by transnational companies operating within global structures and with global supply chains across different jurisdictions. As illustrated below through the examples of the French, British and German export control regimes, and despite some interesting developments, national export control regimes vary and remain inadequate.

© Steven Kreuzer

36. See Council of the European Union, Foreign Affairs Council (Trade), Council Conclusions, Brussels, 21 November 2014, http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/145903.pdf

CHAPTER 3

A look into the French, British and German export control regimes



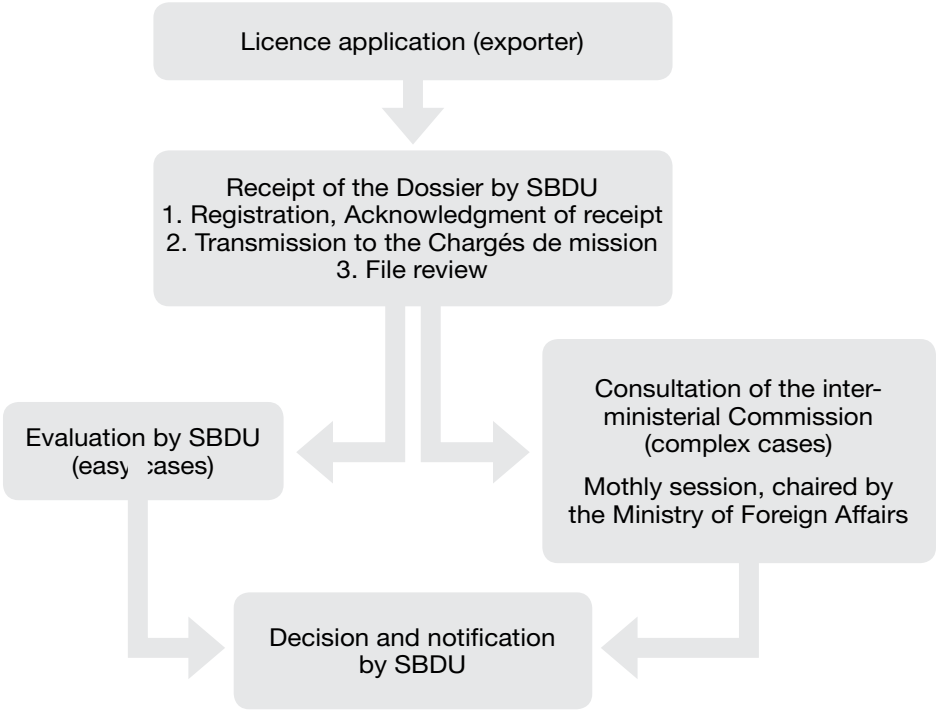
France

In the wake of the addition of the two new categories of surveillance technologies into the dual-use goods and technologies control list of the Wassenaar Arrangement, the Minister for industrial renewal (*Ministère du Redressement Productif*) issued on 6 December 2013 a Notice to the exporters of equipment allowing the interception of mobile telecommunications and IP network communications surveillance.[37]

According to this notice, exporting such technologies outside the EU requires the same prior authorisation of the French government that was already required for exporting dual-use technologies outside the EU. The export licensing procedure of this national export control regime is detailed in Decree No 2010-292 of 18 March 2010 defining procedures for obtaining export, transfer, brokering and transit authorisations for dual-use goods and technologies, and introduces the transfer of competences from the General Directorate of Customs and Direct Taxation to the General Directorate for Competitiveness, Industry and Services.[38]

The Dual-Use Goods Control Office (in French *Service des Biens à Double Usage,* SBDU) is the administrating body responsible for dual-use export licensing and the instruction of license applications. It is also in charge of channelling most sensitive files through the Inter-Agency Committee on Dual-Use Items (in French *Commission Interministérielle des Biens à Double Usage,* CIBDU), from within the Ministry of Industry.

Export licensing procedure for dual-use goods and technologies outside the EU:[39]



37. "Avis aux exportateurs d'équipements d'interception de télécommunications mobiles et de surveillance de communications sur réseau IP".
38. Décret n° 2010-292 du 18 mars 2010 relatif aux procédures d'autorisation d'exportation, de transfert, de courtage et de transit de biens et technologies à double usage et portant transfert de compétences de la direction générale des douanes et droits indirects à la direction générale de la compétitivité, de l'industrie et des services.
39. Décret n° 2010-292 du 18 mars 2010 relatif aux procédures d'autorisation d'exportation, de transfert, de courtage et de transit de biens et technologies à double usage et portant transfert de compétences de la direction générale des douanes et droits indirects à la direction générale de la compétitivité, de l'industrie et des services.

In the notice to the exporters of equipment allowing the interception of mobile telecommunications and IP network communications surveillance (December 2013), the technologies needing export authorizations from the Dual-Use Goods Control Office are termed as:

➜ Equipment used for the interception of mobile telecommunication:
Systems or equipment specifically designed or modified to intercept and analyse the aerial electromagnetic signals of mobile communications (and their specifically designed components), excluding those intended for mobile telephone operators, or those designed for the development or the production of mobile telecommunications equipment or systems.

➜ IP network communications surveillance systems or equipment, and their specially designed components, that have all of the following characteristics, excluding those intended to be used for marketing purposes or the application of quality of service or experience's measurement:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
   a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
   b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
   c. Indexing of extracted data; and

2. Being designed to specifically carry out all of the following:
   a. Execution of searches on the basis of 'hard selectors'; and
   b. Mapping of the relational network of an individual or of a group of people.[40]

The language of the second provision is taken directly from one of the new provisions of the Wassenaar Arrangement. However, the two recent amendments adopted by the French government (along with forty other States) through the Wassenaar Arrangement did not only refer to IP network communications surveillance systems, but also to "intrusion software". The notice to exporters therefore failed to reflect the engagements taken by the French government in the context of the Wassenaar Arrangement. With the recent update of the EU Dual-Use Regulation, the French government is expected to adapt its regulation to comply with the Arrangement by December 2014, including with regard to intrusion software.

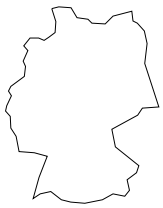
Furthermore, the notice does not specifically refer to sanctions in case of non-compliance with the export licensing procedure. However, according to the Article 414 of the French Customs Code, exporting controlled items without the proper license are considered to be a criminal offence. It constitutes a first class customs offence, punishable with up to three years imprisonment, confiscation of the goods, and a fine that can be up to twice the value of the goods.

One of the other obvious flaws of the notice is the limited scope of the technology requiring an export license. For instance, to obtain an export license, a technology needs to possess five characteristics to be recognized as an IP network communications surveillance system. Therefore, exporters could easily choose to export technologies that omit one of these five characteristics in order to bypass the licensing procedure.

40. For original version see: "Avis aux exportateurs d'équipements d'interception de télécommunications mobiles et de surveillance de communications sur réseau IP". http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?

Thus, the current notice should take into account the actual functioning of these systems which require the integration of services and technologies, and which can be provided by different companies and sub-contractors. Indeed, the sub-division of tasks and the integration of capabilities between these companies are commonplace. This situation is well highlighted by the Qosmos case, in which the French company claimed that it only provided "one piece" of a larger system, and therefore could not control the way their technology could be eventually used. The scope of controlled items should therefore be broadened to take into account the specificities of the ICT sector.

The French export licensing procedure in itself also raises concerns. As highlighted by the recent parliamentary question of Isabelle Attard to the Ministry for renewal of industrial licensing,[41] very little is known about the criteria used by the French government to grant export licenses to exporters of equipment that allow the interception of mobile telecommunications and IP network communications surveillance.


Germany

In Germany, the key legal instruments for export control are the *Aussenwirtschaftsgesetz* (AWG) and the associated administrative implementation agreement *Aussenwirtschaftsverordnung* (AWV). As of September 1, 2013, revised versions of both of have been passed into law in order to reflect the changes in the EU Dual-Use Regulation. The AWV provides a long list of goods to be regulated and goes beyond both the EU dual-use regulation and Wassenaar dual-use regulations. However, national legislation is not necessarily required in Germany, as the EU regulation is directly enforceable and binding in Germany, and overrides all national laws on the same subject. Although the German government has the ability to restrict exports through Article 8 EU Dual-Use ((EU) No 428/2009) it is not included in the German AVG or AVW due to either human rights or public safety concerns. This is a significant loophole, which could be amended by simply updating the relevant articles of the AWV to include Article 8 of the EU Dual-Use Regulation.

Other sections of the German export control law could be used to address the export of intrusive surveillance technologies. Indeed, several provisions of German law specifically aim to regulate services, such as maintenance and technical support, for critical technologies. Though surveillance technologies are not yet included in the list of products and services currently controlled through these provisions, extending export controls to "services" could offer an effective way for the German government to control the trade of these technologies.

In 2014, the German government has given several signals that it seemed willing to pay closer attention to these issues, given the increasing spread of surveillance technologies at the global level. For instance, in May 2014 Germany declared a ban on the sale of surveillance technologies to Turkey, with the justification that countries who want to defend Internet freedom cannot provide technology to those regimes that monitor Internet users and thereby breach fundamental human rights. This decision was followed by a declaration of the German Minister of the Economy Sigmar Gabriel stating that: "authoritarian regimes oppress their population not only with tanks and machine guns, but also increasingly with Internet surveillance technology. We want to stop the export of such technology to countries that suppress the civil rights movement

41. Question parlementaire de Isabelle Attard (Ecologiste – Calvados) au Ministère du Redressement Productif le .... décembre 2013, Assemblée Nationale. See: http://questions.assemblee-nationale.fr/q14/14-45855QE.htm

and don't accept human rights".[42] Even if these recent declarations must be acknowledged, it has to be kept in mind that Germany remains as of today one of the largest exporters of surveillance technologies in the world. On 24 November 2014, Germany took unilateral steps to address what it felt was an easily exploitable framework within the EU for the near unaccountable export of surveillance technologies. The German government announced that it was now active in leading on the issue in the EU through the formation of a Working Group on Surveillance Technology, which will meet regularly with members of the European Commission and the Member States, identifying gaps and ways to remediate to such gaps.[43]


United Kingdom

In the UK, exports controls are based on lists of items which are set up both at national (UK Military List), European (EU Dual-Use List and the EU Human Rights List) and international levels (Wassenaar Arrangement), which combined together form the Consolidated List.[44] Licensed exports of military and dual-use goods are considered on a case-by-case basis against eight criteria, defined as Consolidated EU and National Arms Export Licensing Criteria.[45] Some surveillance equipment is currently explicitly subject to licensing, and is thus automatically considered against these criteria. However, the majority of surveillance equipment is either not explicitly controlled, or inadequately so.

As is the case in Germany and France, some types of surveillance systems are directly controlled in the UK as a result of being subject to specific EU Restrictive Measures, or because they are on the EU Dual-Use list. Although items that are used to identify mobile telecommunications details such as MSI numbers were added to the Wassenaar Dual-Use list in 2011, the delay taken by the EU to update its Dual Use Regulation to reflect this means that these items, as of 2014, were still not explicitly included in the UK Consolidated List.

Surveillance equipment can be brought within the scope of UK export controls either by adding items to one of the pre-existing lists within the Consolidated List, or by adding a new list, through the use of "catch-all" controls, through the use of sanctions, or through the use of interim measures.

When introducing new "ad hoc" national export controls, EU Member States are required to ensure that they are consistent with EU law, proportionate to the desired outcome, do not impose unnecessary costs on legitimate trade, and capable of being effectively enforced. In fact the UK has implemented controls on specific dual-use items within the UK Dual Use List based on Article 8 within the EU Dual-Use Regulation (human rights concerns) and made in exercise of powers conferred in Section 3 of the Export Control Order. The UK has made use of Article 8 for several types of goods, including 'Telecommunications and related technology' – which includes "tropospheric scatter communication equipment using analogue or digital modulation techniques for export to Iran".

42. For more, see: http://www.sueddeutsche.de/politik/internetueberwachung-gabriel-plant-exportstopp-von-spaeh-software-1.1969189
43. For more http://bmwi.de/DE/Presse/pressemitteilungen,did=671052.html
44. There are six lists that make up the Consolidated List – National: UK Military List, UK Dual Use List, UK Radioactive Source List, UK Security and Human Rights List. – EU: EU Human Rights List, EU Dual Use List.
45. For more on the Consolidated EU and National Arms Export Licensing Criteria, see: http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140325/wmstext/140325m0001.htm#14032566000018

One issue in the UK process is that the assessment of exports does not sufficiently take into account the human rights record of the end-user, and in fact human rights are only examined if there is a "clear risk" the technology might be used for internal repression. This essentially allows strategic goods to be exported from the UK to States it considers having poor human rights records because the item itself may not directly be used for internal repression, or for human rights abuses.

© Louish Pixel

CHAPTER 4

Accountability of ICT companies: initial lessons learned from the use of recourse mechanisms

Given the current weaknesses of existing policy and legal frameworks in preventing human rights violations linked with the sale and export of surveillance technologies, victims together with civil society organisations are turning both to judicial and non-judicial mechanisms to hold companies accountable and to seek appropriate remedies.

Non-judicial mechanisms: the OECD complaint mechanism

"The Organisation for Economic Cooperation and Development (OECD) Guidelines for Multinational Enterprises (the Guidelines) are part of the OECD Declaration on International Investment and Multinational Enterprises. The Guidelines – a non-binding instrument – are a set of recommendations addressed to MNEs operating in or from OECD member countries and other states that are signatories to the Declaration. The Guidelines therefore apply to companies present in all adhering states, and also covers operations in countries that have not adhered to the Guidelines.[46] They were updated in 2011. In addition to containing general principles which include the principle of due diligence, they provide guidance for responsible business conduct in different areas, including human rights and information disclosure. Governments adhering to the Guidelines must establish a National Contact Point (NCP) to promote the Guidelines and to handle complaints (referred to as "specific instances") against companies that have allegedly failed to respect the standards comprised in the Guidelines. NCPs are governmental agencies organised in various forms and essentially are mediation mechanisms focused on conciliation and the resolution of disputes.[47] Complaints have been referred to NCPs to address human rights violations allegedly committed by surveillance companies.

In February 2013, a number of human rights organisations[48] jointly filed complaints before the British and German NCPs against two surveillance companies, Gamma International and Trovicor, with regards to both companies' alleged complicity in serious human rights abuses in Bahrain. The British NCP accepted the complaint against Gamma International. On its part, the German NCP was only willing to consider Trovicor's due diligence procedures, and refused to consider the role the company would have played in the abuses that were committed. Complainants therefore did not believe the mediation process would be successful in these conditions.[49]

Non-judicial mechanisms, while more easily accessible than judicial procedures, are alternate avenues victims can turn to. However, NCP complaint procedures remain focussed on mediation and are therefore unlikely to provide an effective remedy to victims, particularly in cases of grave human rights abuses. Such mechanisms are also largely criticised for their inability to effectively ensure that companies respect the spirit and content of the OECD Guidelines with regard to human rights standards. More specifically, they are criticised by both rights-holders and supportive civil society organisations for their lack of ability to investigate, their lack of independence, and their restrictive interpretation of the admissibility criteria (as illustrated

46. OECD Guidelines for Multinational Enterprises, 25 May 2011, Chapter I, §3.
47. See FIDH, Corporate Accountability for Human Rights Abuses : A Guide for Victims and NGOs on Recourse Mechanisms, Update in March 2012, Section III, http://www.fidh.org/en/globalisation-human-rights/business-and-human-rights/Updated-version-Corporate-8258
48. Privacy International, the European Center for Constitutional and Human Rights, the Bahrain Center for Human Rights, Bahrain Watch and Reporters Without Borders
49. "German OECD NCP unwilling to investigate role of German company in human rights violations in Bahrain", Privacy International, 21 December 2013. For more, see: https://www.privacyinternational.org/press-releases/german-oecd-national-contact-point-unwilling-to-investigate-role-of-german-company-in

above with the case of Trovicor in Germany) and the Guidelines, etc.[50] NCPs' ability to provide effective remedies in cases of human rights violations resulting from the sale of surveillance technologies can indeed be seriously questioned.

Judicial mechanisms

EU Member States have the obligation to protect human rights, including from violations committed by third-parties operating abroad, and to provide for an effective remedy in case of violations. EU Member States' courts can have jurisdiction for human rights violations committed abroad by multinational corporations. The primary instrument EU Member States' courts use to establish the civil liability of multinational corporations for human rights violations committed outside of the EU is Regulation 44/2001 of December 2000 (Brussels I). This regulation sets out, *inter alia*, the rules of international jurisdiction in civil and commercial matters which are common to the various EU Member States.

This regulation applies for corporations that are domiciled in an EU Member State. In addition, Rome II regulation, which aims at standardising rules on conflicts of law applicable to non-contractual obligations and ensure that courts of all Member States apply the same law in cross-border civil liability disputes, will apply.

Numerous obstacles nevertheless remain for victims in order to hold multinational companies accountable in EU Member States courts,[51] even more so for victims of violations committed by European companies in third countries. In all jurisdictions, victims face legal obstacles, including issues such as the doctrine of *forum non conveniens,* time limitations, immunities doctrine, in addition to practical obstacles such as costs and access to legal aid. Corporate law – such as the doctrine of "separate legal liability" also create significant legal obstacles, making it difficult to meet the required threshold to demonstrate the level of control European corporations, as parent companies, can have on their subsidiaries operating abroad. The European Coalition for Corporate Justice (ECCJ), of which FIDH is a steering group member, is calling on the EU to undertake a series of reforms to lift barriers victims may face, and ensure access to judicial remedies for abuses of human rights by transnational companies.[52]

Another judicial avenue worth exploring at the national level is that of criminal law. Direct extraterritorial jurisdiction on the basis of the nationality of the offender is accepted in some countries, and recent studies have shown that many states, much more so than a decade ago, are exercising extraterritorial jurisdiction in relation to crimes under international law.[53] The difficulty then lies on proving how such surveillance has led to crimes against humanity or

50. See OECD Watch (coalition of which FIDH is a member), http://www.oecd-watch.org/

51. See notably recommendations for reforms formulated by NGOs and legal experts. See for instance the work of the European Coalition for Corporate Justice (ECCJ) of which FIDH is a member. See Gwynne Skinner, Robert McCorquodale, Olivier de Schutter, Andie Lambe, "The Third Pillar: Access to Judicial Remedies for Human Rights Violations by Transnational Business", commissioned by ECCJ, CORE, ICAR, December 2013. See also, FIDH, Corporate Accountability for Human Rights Abuses : A Guide for Victims and NGOs on Recourse Mechanisms, Update in March 2012, Section II, http://www.fidh.org/en/globalisation-human-rights/business-and-human-rights/Updated-version-Corporate-8258

52. See recommendations at the end. See also : Gwynne Skinner, Robert McCorquodale, Olivier de Schutter, Andie Lambe, "The Third Pillar: Access to Judicial Remedies for Human Rights Violations by Transnational Business", commissioned by ECCJ, CORE, ICAR, December 2013, http://www.corporatejustice.org/The-Third-Pillar-Access-to

53. FIDH, Extraterritorial Jurisdiction in the European Union" (2010): http://fidh.org/IMG/pdf/Extraterritorial_Jurisdiction_In_the_27_Member_States_of_the_European_Union_FINAL.pdf

other crimes, such as torture, for which many EU legislations provide for extraterritorial jurisdiction. FIDH has used this route in two strategic litigation cases in which it is involved in France. As illustrated below and while such cases are progressing, important hurdles remain.

Amesys case[54]

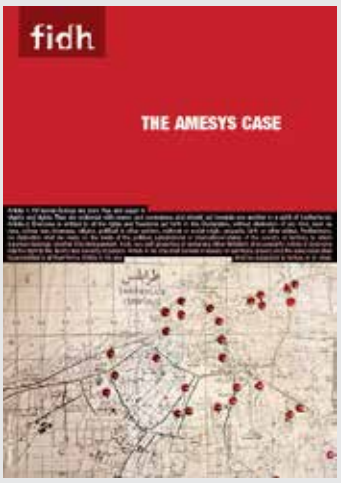
In the context of the Arab Spring, information published in the *Wall Street Journal i*n August 2011 (see Annex below) brought to light the business relationship of the French company Amesys with the Libyan intelligence services resulting from a contract to supply a sophisticated communications surveillance system. It raised profound concerns.

The sophisticated surveillance technology used in the context of the Arab Spring by repressive regimes proved to be a formidable weapon that facilitated the targeting, arrest and oppression of anyone participating in peaceful uprisings.

Information circulated by the media shed light on a previously unheard of business sector – that of surveillance technology. For FIDH, who supported human rights defenders during the uprisings on a daily basis, putting such technology into the hands of regimes that practice unbridled repression raises serious issues of corporate responsibility for companies involved in this sector. To what extent does supplying computer programmes that allow regimes such as those of Muammar Gaddafi or Bashar Al-Assad to repress peaceful demonstrators more efficiently constitute involvement in an act punishable by law? Can companies be seen as complicit in the resultant international crimes perpetrated? And, in this case, are they accomplice to torture?

On 11 November, 2011, FIDH and its member organisation in France French Human Rights League (*Ligue française des droits de l'Homme* - LDH) filed a complaint for alleged complicity of the French company Amesys and its executive managers in acts of torture, for having signed and executed a commercial agreement for the provision of surveillance technology to the Libyan regime in 2007.

FIDH and its Litigation Action Group (LAG) lodged the complaint in France on the basis of the principle of extraterritorial jurisdiction. FIDH's LAG is a network of lawyers, magistrates, and academics who represent the victims of international crimes before national, regional and international courts in proceedings aimed at proving the legal liability of persons, businesses, or states believed to have perpetrated such serious offences.



For FIDH, complaints for serious international crimes should, as a priority, be lodged in the country where the crimes are perpetrated. However, the specific details of this case, and the state of the Libyan judicial system, led FIDH and its LAG and LDH to lodge the complaint in France. Indeed, in this case a French magistrate is also better able to conduct the investigations required on French territory.

54. Extracts from FIDH Report, "The Amesys case", November 2014, www.fidh.org

The agreement signed in 2007 between Amesys and the Libyan regime covered the supply of a communications interception system called EAGLE. The system sold by Amesys allegedly permitted the interception of all country-wide, on-line and off-line exchanges, and the subsequent processing of collected data to target and identify a given group within the civilian population on the basis of criteria established by the system's user.

In an interview published in the French newspaper *Figaro* in September 2011, a former official of the Libyan External Security Organisation explained that the system was able to find "targets within the country's massive flow" and to identify "individual suspects using key words". This witness summed it up as follows: "We listened in on the entire country". The system was subsequently used to create data analysis methods that were applied to the collected data in order to hone in on key words used for queries and to monitor the findings obtained collaboratively with Libyan authorities, in particular the Libyan military high command.

In the complaint, FIDH and LDH concluded that the system supplied by Amesys effectively enabled the Libyan regime to perfect their methods of oppressing the Libyan people. Given the sinister reputation of Muammar Gaddafi and his security structures –regularly criticised by international human rights organisations – Amesys must have known that the Libyan regime would use the technology as a means of oppression.

The serious breaches of fundamental liberties committed by the regime, which had been widely covered by the media and by international human rights organisations, must have been known to the Amesys Group and to all those who participated in the cooperation programme between Amesys and Libyan authorities. That programme was specifically aimed at modernising, perfecting, and extending the durability of the system used for the identification, surveillance, and elimination of opponents by intelligence authorities.

The opening of a criminal investigation has been met with opposition from the Prosecutor of the Paris Tribunal. The Prosecutor officially asked that the case be closed and appealed the order issued by the investigating judge who had chosen to disregard the arguments put forward by the Prosecutor and proceeded with the judicial investigation. On 15 January 2013, the Criminal Investigations Tribunal of the Paris Appeals Court (*Chambre de l'instruction de la Cour d'appel de Paris*) denied the Prosecutor's request for a reversal of the investigative judge's decision to formally open a criminal investigation, thus confirming the opening of an investigation.

In December 2012, FIDH organised a mission to Libya.

In January 2013, with the support of FIDH and LDH, five Libyan victims joined ongoing proceedings as civil parties (*parties civiles*). In December 2012, the members of the FIDH mission had recorded these victims' accounts of their respective experiences. All of the victims had been arrested and tortured during the uprising against Muammar Gaddafi after having been identified through the monitoring of their electronic communications. In June and July 2013, with support from FIDH, the five victims went to France to testify before the investigating judge in charge of the criminal investigation opened in January 2013 before the newly created Specialised War Crimes Unit within the Paris Tribunal (*Tribunal de Grande Instance*).

The following is testimony from a civil party represented by FIDH in the proceeding:

"Mrs. A was 32 years old and a student in Tripoli at the time she was arrested at 9:00 am on 16 February 2011. The arrest took place after she had been asked to report to the headquarters of the Internal Security Services in Tripoli. This was not the first time she had been asked to report to the headquarters to provide information on her activities, which had been qualified as "incitement to demonstrate." It was for this reason that she had decided to go ahead and report. She was interrogated by officers working for Internal Security from the morning of February 16 February until 2:00 am on the following day, without a break. The officers asked her about the content of Skype conversations that had been recorded by the security service, and also asked about emails exchanged via her Yahoo account and conversations on Facebook. The interrogators showed Mrs. A the contents of all of her private communications printed on sheets of paper and asked her to identify her interlocutors, and the people hiding behind the user names. Mrs. A was tortured during the interrogation. The following day she was transferred to the Abu Salim prison. On several occasions she witnessed summary executions in the prison courtyard. She was threatened, insulted, and beaten on several occasions".

One of countless files from Libya's internet surveillance centre. *The Wall Street Journal.*

Qosmos Case

On 17 July 2012, FIDH and LDH lodged a similar complaint against French company Qosmos for its alleged implication in the selling of hardware to the Syrian government. This complaint led to the opening of a judicial investigation after the Paris Prosecutor undertook a preliminary investigation conducted by the Paris Prosecutor within the Specialised War Crimes Unit within the Paris Tribunal (*Tribunal de Grande Instance*). After 18 months of preliminary investigation monitored by the Prosecutor, during which important evidence was collected by the French investigators, a formal judicial enquiry was opened in April 2014.[55]

55. FIDH, Opening of a judicial investigation targeting Qosmos for complicity in acts of torture in Syria, 11 April 2014, http://www.fidh.org/en/europe/france/15116-france-opening-of-a-judicial-investigation-targeting-qosmos-for-complicity

Many companies selling mass monitoring or censorship equipment, including Amesys and Qosmos, have argued that they do not have responsibility for how their tools are used once sold, and have denied that they are complicit in any human rights abuses that may be committed with the help of their technology. These two cases are an opportunity to reassess corporate liability in such cases, and could send out a strong warning to other firms that they can, and will be, held to account.

In other cases, the use of administrative judicial mechanisms, together with criminal complaints, can also represent an interesting legal avenue to hold ICT companies accountable.

Cases involving British-German ICT company Gamma International

In November 2012, Privacy International provided a 186-page dossier of evidence against UK-based Gamma International to the HM Revenue and Customs (HMRC), the UK body responsible for enforcing export regulations, regarding a potentially criminal breach of the export control regime. On behalf of victims who were targeted by Gamma's FinFisher, Privacy International called for an urgent investigation into Gamma's export practices. FinFisher is one of the most notorious and controversial suites of surveillance software. It is "designed to siphon off and intercept all kinds of data from a target's computer or cell phone, including Skype calls, emails, and chat conversations".[56]

HMRC's response was to categorically refuse to provide details on any of Gamma's export practices, arguing it is statutorily barred from releasing information to victims or complainants. The agency further denied that it had any obligation to be transparent about any activities relating to the potentially illegal exports of British surveillance technology by Gamma International. In April 2013, Privacy International instituted judicial review proceedings before an Administrative Court of Justice, asserting that HMRC acted unlawfully.

In May 2014, the Administrative Court declared that HMRC acted unlawfully and "irrationally" in issuing blanket refusals into the status of any investigation into the potentially illegal export

of the spyware FinFisher by Gamma International to repressive regimes. The Administrative Court also ordered HMRC to reconsider Privacy International's request.

Shortly before this positive decision, Privacy International filed, on February 2014, a criminal complaint before the National Cyber Crime Unit of the National Crime Agency urging them to investigate the potentially unlawful interception of the communications of an Ethiopian political refugee living in the UK, as well as the role Gamma played in developing and exporting an invasive commercial surveillance software called FinSpy.[57]

56. "Wikileaks exposes countries that use controversial FinFished surveillance Tech", 16 September 2014, Mashable.com. For more see: http://mashable.com/2014/09/15/wikileaks-finfisher-customers-surveillance/
57. For more on the case, see: https://www.privacyinternational.org/resources/legal-action/criminal-complaint-to-national-cyber-crime-unit-on-behalf-of-tadesse-kersmo

A similar criminal complaint was also made in October 2014 before the National Cyber Crime Unit of the National Crime Agency, urging the immediate investigation of the unlawful surveillance by Bahraini authorities of three Bahraini activists living in the UK using the same technology supplied by Gamma. This complaint came after the recent leak of Gamma's internal documents demonstrating that it was "both aware of, and actively facilitating, the Bahraini regime's surveillance of targets located outside Bahrain through the provision of intrusion technology".[58]

Several ongoing cases in both the EU and the US, using innovative legal strategies, demonstrate the need for a better regulation controlling the activities of ICT companies selling surveillance technology.

On 17 September 2014, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced that Area S.p.A. (Area), located in Italy agreed to a $100,000 civil penalty settling charges that it knowingly sold U.S.-origin network monitoring equipment to the Syrian Telecommunications Establishment (STE) without the required U.S. Government authorization. This penalty is both welcome, because it is almost unprecedented, and timid, in the sense that the penalty fine does not even come close to the amount at which Area purchased, and then sold, the network monitoring equipment valued at approximately $140,000.

The StealthGenie case is another promising case underway in the United-States. As stated by Kim Zetter, a journalist from Wired, the StealthGenie case could be "the criminal indictment that could finally hit spyware makers hard".[59] The FBI arrested the CEO of StealthGenie, another UK company, in the end of September 2014 for allegedly conspiring to advertise and sell StealthGenie, a spyware application that could monitor and collect communications on mobile phones without detection. This programme was designed to secretly monitor phone calls and text messages, as well as allowing "users to read email sent and received through a phone, turn on the phone's microphone to monitor conversations up to 15 feet away, and view the address book, calendar entries and photos and videos". This marks the first-ever criminal case involving the advertisement and sale of a mobile device spyware app[60]. In this case, it is troubling that the StealthGenie programme is actually very similar to others sold by other European-based companies, such as Gamma International, which are deemed lawful and appropriate.

In Switzerland, "Swiss company Neosoft has been referred in September 2014 for prosecution after uncovered evidence that the surveillance company was trying to equip and train a brutal government unit in Bangladesh implicated in wide-scale human rights abuses with state of the art mobile phone surveillance equipment".[61]

58. For more on this case, see : https://www.privacyinternational.org/news/press-releases/privacy-international-files-criminal-complaint-on-behalf-of-bahraini-activists
59. For more, see: http://www.wired.com/2014/10/stealthgenie-indictment
60. For more, see : http://www.fbi.gov/washingtondc/press-releases/2014/pakistani-man-indicted-for-selling-stealthgenie-spyware-app
61. For more, see: https://www.privacyinternational.org/news/blog/surveillance-company-neosoft-referred-for-prosecution-by-swiss-authorities-over-deal-with

CHAPTER 5
Proposals for a sound and evolving EU regulatory framework

To ensure that the trade of ICT technologies, such as those surveillance technologies discussed in this paper, do not lead to human rights violations, and to further ensure access to justice for victims, there is an urgent need to strengthen the European and international regulatory and policy frameworks that control the trade of these technologies through a coordinated and concerted approach.

FIDH calls on the European Union and its Member States to:

On the sale and export of surveillance technologies

➜ Ensure the development of effective international and European regulation of dual-use surveillance technologies in close co-operation with all relevant stakeholders, including civil society organisations, within and beyond the Wassenaar Arrangement;

➜ Consider ways to improve the EU Dual-Use Regulation by tackling the fragmented national export control legislation in EU Member States and by ensuring appropriate monitoring and oversight mechanisms are in place;

Centralising oversight and enforcement of the Regulation would improve the level-playing field and could be a way to improve accountability at the European level. Furthermore, conflicts of interests between certain ICT companies and Member States exist in many EU countries. Member states are indeed responsible for the licenses that businesses need to export certain technologies, but have also an interest in the commercial success of these companies. This could be avoided by placing the licensing authority at the European level;

➜ Ensure the inclusion of new categories of surveillance technologies to EU and international export control lists to broaden the scope of the controlled items, in line with the real scope of products and services sold in this sector;

➜ Establish an EU-wide ad-hoc licensing requirement[62];

"Catch-all" controls should be made more efficient and effective by extending their application to all Member States. Improving the coherence and the efficiency of the catch-all controls for technologies that are instrumental in human rights violations would require the establishment

➜ For IP Network Communication Surveillance Systems and Intrusion Software, introduce controls including case-by-case screening for all destinations with a provisional presumption of denial;[63]

62. See notably recommendation formulated by MEP Marietje Schaake, Written submission to the public consultation on the European Commission's Gron the dual-use export control system of the European Union, 31 October 2011. For more, see: http://www.marietjeschaake.eu/wp-content/uploads/2012/07/MarietjeSchaakeMEP-SubmissionGreenPaperDualUse-2011.10.31-def.pdf

63. See Access Now, Collin Anderson, Internews, Reporters Without Borders, and the Open Technology Institute, "Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding "Intrusion Software" and "IP Network Communications Surveillance Systems", May 2014.

The license consideration process for Intrusion Software and IP Network Communications Surveillance Systems must include examination of the human rights and privacy concerns that prompted their control, and exporters should have to prove that the goods or products in question do not pose a significant risk to human rights and national security";[64]

➜ Integrate specific recommendations regarding the trade of ICT technologies in the EU's next CSR communication as well as in the EU's tools, guidelines and strategies regarding the implementation of the UN Guiding Principles on Business and Human Rights;

➜ Call on Member States to include regulatory measures regarding the trade of surveillance technologies in their national action plans on the implementation of the UN Guiding Principles on Business and Human Rights;

➜ Implement conditions, triggers, benchmarks and reporting procedures to ensure the EU financial and technical support to the development of new technologies in third states are not used in a way that infringe human rights;

European financial support for communications infrastructure could be made conditional on its capacity to effectively contribute to the realisation of human rights.

➜ Include human rights clauses in public procurement processes;

➜ Require Members States to conduct human rights impact assessments of these technologies, including by introducing human rights impact assessment in the R&D phase of technological development;

On this issue, the Dutch MEP Marietje Schaake has provided valuable input on how these human rights impact assessments could be conducted: "The EU should explore possibilities of incorporating human rights impact assessments at an earlier stage: the R&D phase or when registering a new item for an EU patent. Thus, items that are potentially harmful outside the EU can be identified and flagged at an early stage, and ad-hoc probes can be carried out to check compliance. […] The human rights impact assessments or 'flagging' could be performed by a European regulator, e.g. the Body of European Regulators for Electronic Communications (BEREC).[65]

➜ Include surveillance technologies in EU embargoes on equipment that might be used for internal repression;

➜ Ensure relevant regulatory authorities possess the necessary resources and technological expertise to enforce these export controls;

64. See Access Now, Collin Anderson, Internews, Reporters Without Borders, and the Open Technology Institute, "Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding "Intrusion Software" and "IP Network Communications Surveillance Systems", May 2014

65. Written submission of Marietje Schaake – Member of European Parliament (ALDE / D66) - to the public consultation on the European Commission's Green paper on the dual-use export control system of the European Union: ensuring security and competitiveness in a changing world, 31 October 2011.

➜ Increase transparency and access to information for the general public on the use of such technologies, including by publicly disclosing licences requests, licences granted, the list of companies supplying surveillance technologies and its suppliers.

➜ Ensure greater scrutiny from democratic bodies to ensure trade regulations are effectively implemented;

➜ Implement import licenses for private companies that wish to use these technologies[66];

➜ Ensure judicial supervision of the use of surveillance technologies by the police, military and intelligence services;

➜ Require ICT companies to disclose information on surveillance activities undertaken, including the time period and location;

General recommendations for access to justice by victims

➜ Request Member States to introduce mandatory human rights due diligence for companies in their national legislation [67] ;

➜ Proceed with legal reforms to enable victims of abuses committed by European-based surveillance companies to bring cases in companies' home States[68];

➜ Address obstacles in accessing justice posed by the principles of limited liability and the separation of legal personality by ensuring parent companies can be held liable for human rights violations caused by their subsidiaries[69];

➜ Adopt the necessary legal and policy measures to lift financial and practical barriers that can discourage or prevent victims from bringing a case[70];

➜ Ensure, at the national level, the swift and impartial investigation of cases alleging human rights violations by surveillance companies. Prosecutorial policies should include, as a matter of priority, the issue of surveillance comapanies ;

➜ Support efforts to enhance democratic control and judicial oversight of the intelligence services, law enforcement and military intelligence in the EU and third countries;

➜ Ensure the establishment of review processes allowing for civil society expertise to be included at both national and EU levels;

---

66. Digital Rights, "What transparency standards should we demand from States using surveillance technologies?", Digital Rights Latin America and The Caribbean, 30 September 2014. For more, see: http://www.digitalrightslac.net/en/que-estandares-de-transparencia-debemos-exigir-a-los-estados-que-usan-tecnologias-para-la-vigilancia/

67. For detailed recommendations see Gwynne Skinner, Robert McCorquodale, Olivier de Schutter, Andie Lambe, "The Third Pillar: Access to Judicial Remedies for Human Rights Violations by Transnational Business", commissioned by ECCJ, CORE, ICAR, December 2013, http://www.corporatejustice.org/The-Third-Pillar-Access-to

68. For detailed recommendations see Gwynne Skinner, Robert McCorquodale, Olivier de Schutter, Andie Lambe, "The Third Pillar: Access to Judicial Remedies for Human Rights Violations by Transnational Business", commissioned by ECCJ, CORE, ICAR, December 2013, http://www.corporatejustice.org/The-Third-Pillar-Access-to

69. *ibid*

70. *ibid*

➜ Support the development of a binding legal framework at the international level to address the sale and trade of surveillance export technologies contributing to human rights violations;

➜ Support the creation of a UN special procedure (Special Rapporteur) on the right to privacy and ensure that its mandate addresses the use and export of surveillance technologies by private companies and related human rights abuses;

➜ Support the work of human rights defenders by ensuring the establishment and adequate functioning of prevention mechanisms, in line with the EU Guidelines on Human Rights Defenders and the EU No disconnect strategy;

➜ For high-risk countries, take into account potential human rights abuses linked with the sale and export of surveillance technologies in bilateral dialogues and human rights country strategies.

FIDH echoes recommendations formulated by CAUSE members and calls on companies to:

➜ **Adopt, with the support of the top-management, a human rights policy** targeted at the human rights risks associated with this sector of business activities, and include references to uphold human rights in case the company receives governmental requests for activities such as illegal surveillance and requests for censorship;

➜ **Exercise due diligence to identify potential human rights risks** linked with their business activities and relationships, including by conducting human rights impact assessments prior to concluding any contract to ensure that the use of surveillance technologies does not lead to human rights violations. In particular, ICT companies should pay specific attention to potential risks of violations of the rights to privacy, freedom of expression and freedom of association. Such due diligence processes should aim at ensuring that companies refrain from selling technologies or selling and/or providing maintenance, updates and/or any other types of services that could cause or contribute to human rights violations;

➜ When negotiating a contract**, identify clearly the end use and end users** of the products or services being provided. Avoid selling such technology if there is no clear legal framework controlling its use or if there is a documented record of human rights abuses within the country of destination;

➜ To avoid complicity in any misuse of products or services, **stipulate clear end-use assurances in contractual agreements** with customers encompassing strong human rights safeguards and protecting against their arbitrary and unlawful use[71];

➜ **Adopt policies and procedures to stop or address misuse of products and services**, including contractual provisions that designate end use and end users, the violation of which would allow the company to withdraw services or cease technical support or upgrades[72];

71. Privacy International,"Private Interests: Monitoring Central Asia", Privacy International, November 2014, https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privateinterests.pdf
72. Human Rights Watch, 'They Know Everything We Do': Telecom and Internet Surveillance in Ethiopia", Human Rights Watch, 25 March 2014. For more, see: http://www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights

➔ As part of a tender or contract negotiation process, **inquire about both the end-use and end-users** of the products or services being provided, especially for "dual use" products, including "lawful intercept" surveillance software and equipment[73];

➔ Commit to **independent and transparent third-party monitoring** to ensure compliance with human rights standards;

➔ **Investigate any misuse of products or services and engage with business partners, resellers and distributors** to ensure human rights compliance. The "multi-layered sales structure"[74] that is prevalent in this sector imposes companies to proactively prevent adverse human rights impacts that are directly linked to their operations.

"While concerns about national security and criminal activity may justify the exceptional and narrowly-tailored use of surveillance programmes, surveillance without adequate safeguards to protect the right to privacy actually risk negatively impacting the enjoyment of human rights and fundamental freedoms."

UN High Commissioner for Human Rights, Navi Pillay

73. *ibid*

74. Citizen Lab's public submission to the UN Working Group on Human Rights and Transnational Corporations and Other Business Enterprises. Munk School of Global Affairs, December 2011. See more at: http://www.ohchr.org/Documents/Issues/TransCorporations/Submissions/AcademiaAndIndependentResearchers/CitizenLabUniversityTorontoMunkSchoolGlobalAffairs.pdf

75. UN, "Mass surveillance: Pillay urges respect for right to privacy and protection of individuals revealing human rights violations", 12 July 2013, Geneva, www.ohchr.org

fidh

Keep your eyes open

Establishing the facts

investigative and trial observation missions

Through activities ranging from sending trial observers to organising international investigative missions, FIDH has developed, rigorous and impartial procedures to establish facts and responsibility. Experts sent to the field give their time to FIDH on a voluntary basis.
FIDH has conducted more than 1 500 missions in over 100 countries in the past 25 years. These activities reinforce FIDH's alert and advocacy campaigns.

Supporting civil society

training and exchange

FIDH organises numerous activities in partnership with its member organisations, in the countries in which they are based. The core aim is to strengthen the influence and capacity of human rights activists to boost changes at the local level

Mobilising the international community

permanent lobbying before intergovernmental bodies

FIDH supports its member organisations and local partners in their efforts before intergovernmental organisations. FIDH alerts international bodies to violations of human rights and refers individual cases to them. FIDH also takes part in the development of international legal instruments.

Informing and reporting

mobilising public opinion

FIDH informs and mobilises public opinion. Press releases, press conferences, open letters to authorities, mission reports, urgent appeals, petitions, campaigns, website… FIDH makes full use of all means of communication to raise awareness of human rights violations.

FIDH - International Federation for Human Rights
17, passage de la Main-d'Or - 75011 Paris - France
CCP Paris: 76 76 Z
Tel: (33-1) 43 55 25 18 / Fax: (33-1) 43 55 18 80
www.fidh.org

Director of the publication: Karim Lahidji
Editor: Antoine Bernard
Authors: Clément Perarnaud, Adrian Klocke, Geneviève Paul
Coordination: Geneviève Paul
Design: Bruce Pleiser

Imprimerie de la FIDH - Dépôt légal décembre 2014 - FIDH (English ed.) ISSN 2225-1804 - Fichier informatique conforme à la loi du 6 janvier 1978 (Déclaration N°330 675)

FIDH represents 178 human rights organisations on 5 continents

inhuman or degrading treatment or punishment. Article 6: Everyone has the right to recognition everywhere as a person before the law. Article 7: All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination. Article 8: Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law. Article 9: No one shall be subjected to arbitrary arrest, detention or exile. Article 10: Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him. Article 11: (1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty

ABOUT FIDH

FIDH takes action for the protection of victims of human rights violations, for the prevention of violations and to bring perpetrators to justice.

A broad mandate
FIDH works for the respect of all the rights set out in the Universal Declaration of Human Rights: civil and political rights, as well as economic, social and cultural rights.

A universal movement
FIDH was established in 1922, and today unites 178 member organisations in more than 100 countries around the world. FIDH coordinates and supports their activities and provides them with a voice at the international level.

An independent organisation
Like its member organisations, FIDH is not linked to any party or religion and is independent of all governments.

fidh

Find information concerning FIDH's 178 member organisations on **www.fidh.org**