



Carlo Calenda, Ministro dello Sviluppo Economico
Ministero dello Sviluppo Economico
Via Molise 2
00187 Roma
Italy

Sent by email: segreteria.ministro@mise.gov.it

23 January 2016

Dear Minister Calenda,

Privacy International (“PI”) is a UK-based non-governmental organisation which campaigns to protect the right to privacy across the world. In doing so, PI investigates covert government surveillance to raise public awareness about technologies and laws that place privacy at risk.

Coalizione Italiana per le Libertà e i Diritti civili (CILD) is an Italian non-governmental organisation that supports and empowers civil society groups working on the most pressing human rights issues faced by the country today, including the right to privacy of every citizen.

Hermes Center for Transparency and Digital Human Rights is an Italian non-governmental organisation that operates internationally to promote and develop the awareness and the attention to transparency and accountability, as well as to boost the active participation of workers and employees to the correct management of companies they work for.

We are writing to provide information on Italian electronic surveillance technology company, Area SpA, in particular in relation to the reports of its export of surveillance technology to Egypt. We are concerned about the potential use of this technology in violation of Italy’s commitment to human rights, and requests urgent clarification and assurances from the Ministero dello Sviluppo Economico (Mise).

Area SpA

Last month, Privacy International published a report based on hundreds of original documents, describing evidence of the Syrian government’s ambitious surveillance projects aimed at monitoring the national communications infrastructure. The report highlighted how companies around the world were willing and able to supply surveillance equipment, despite evidence at the time that the Syrian government was engaged in wide-scale and serious human rights abuses.¹

As you may be aware, one of the companies mentioned in our report, Area SpA, was involved in a mass surveillance project in Syria, prior to the imposition by the Italian government of a “catch-all” export licensing requirement to the Syrian Telecommunications Establishment in September 2012.

Last month, Italian and international media reported that the offices of Area SpA had been raided by Italian law enforcement, for unspecified reasons.²

¹ <https://privacyinternational.org/node/1009>

² <http://motherboard.vice.com/read/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria>

Another media report, published in June 2016, states that Area SpA had been granted an export license by the Mise to export controlled Internet Protocol (IP) surveillance equipment to the Technical Research Department (TRD) in Egypt.³

Internet Protocol (IP) network communications surveillance systems

IP network communications surveillance equipment was introduced into the Wassenaar Arrangement Dual Use list in 2013 (Category 5A001j). It was incorporated across EU member states, including into Italy's national export control list, with the update of the list of controlled items in Regulation (EC) No 428/2009 in December 2014.

The control, proposed initially by France, came after evidence emerged in 2011 that a French company had provided the Libyan government of Colonel Muammar Gaddafi with such a system, which according to a former official of the Libyan External Security Organisation, allowed the government to listen “in on the entire country,” find “targets within the country’s massive flow,” and identify “individual suspects using key words”.⁴

Category 5A001j is aimed at controlling general traffic analysis systems, such as through deep packet inspection items, which can classify and collect information flowing through a network. The Internet Protocol is one of the core standards upon which today’s communications infrastructure is built, enabling online searches, emails, and Voice over IP calls among other services. The interception of these communications lies at the heart of many mass surveillance systems. Such systems can collect, store, and analyse information about large numbers of people, often without any regard to whether they are legally suspected of wrongdoing. In countries with weak rule of law and under the control of an authoritarian government, these systems are wielded to violate the right to privacy, and pose a serious threat to other human rights. They can be used to identify, target, and locate individuals, thereby facilitating torture and other cruel, inhuman and degrading treatment or punishment, arbitrary detention, extrajudicial killing, and other major violations of fundamental human rights.

Recent European Court of Human Rights judgments in the cases of Szabo and Vissy v. Hungary⁵ and Zakharov v. Russia⁶ have ruled against untargeted, mass intelligence collection systems. In Zakharov, the Court distilled the body of its case law to summarise the requirements of an interception authorisation, which “must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered.”

Export to Egypt

The export of an IP network communications surveillance system to Egypt poses a clear risk to human rights. Recent months have seen an increased clampdown on legitimate dissent, freedom of expression and overall the capacity of human rights defenders to operate in the country. Various UN human rights independent expert bodies, including the UN Special Rapporteurs on freedom of expression, freedom of peaceful assembly and association, and human rights defenders and the UN High Commissioner for Human Rights have expressed serious concern regarding the deterioration of human right in the country.⁷

On 13 July 2016, Amnesty International (“AI”) published a report entitled: ‘Egypt: ‘Officially, You Do Not Exist – Disappeared and Tortured in the Name of Counter-Terrorism’.⁸ The Report documents recent developments, including:

“the emergence of a new pattern of human rights violations against political activists and protesters, including students and children, hundreds of whom have been arbitrarily arrested and detained and subjected to enforced

³<http://www.lastampa.it/2016/06/28/italia/litalia-esporter-software-di-sorveglianza-in-egitto-11iR9uYFcPpkP9PebyHdwM/pagina.html>

⁴ <https://www.fidh.org/en/region/north-africa-middle-east/libya/16959-the-amesys-case-the-victims-anxious-to-see-tangible-progress>

⁵<http://hudoc.echr.coe.int/eng?i=001-160020>

⁶<http://hudoc.echr.coe.int/eng-press?i=001-159324>

⁷ See in particular, Egypt: Worsening crackdown on protest, a further setback to human rights – UN experts, 9 May 2016, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=19933&LangID=E> and Egypt NGO bill threatens to “devastate” civil society, UN expert warns, 23 November 2016, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=20920&LangID=E>

⁸<https://www.amnesty.org/en/latest/news/2016/07/egypt-hundreds-disappeared-and-tortured-amid-wave-of-brutal-repression/>

disappearance by state agents...Local NGOs allege that an average of three to four people are abducted and arbitrarily subjected to enforced disappearance each day.” (p. 7)

The Report describes the complicity of various Egyptian state actors in the enforced disappearances. For example, former detainees and their relatives and lawyers accuse state prosecutors of:

“authoriz[ing] further detention without charge for up to seven days during which the authorities can deny the detainee any contact with their family and lawyer. This facilitates enforced disappearances and directly contravenes Egypt’s Constitution, which gives everyone deprived of their liberty the right to immediate contact with their family and a lawyer.” (p. 9)

The Report further describes that enforced disappearances are committed by the Egyptian authorities in the context of other grave human rights abuses. It states that enforced disappearances:

“facilitate torture and other serious violations against detainees. In Egypt, they are used to enable the Egyptian N[ational] S[ecurity] A[gency] (“NSA”) to torture detainees with impunity and extract ‘confessions’ and other information that can be used to convict them or others under the Penal Code, Counter-Terrorism Law or on other criminal charges, such as participating in anti-government protests. Enforced disappearances and torture are also used to intimidate government critics and opponents and to deter dissent. They form part of a state system of repression that allows NSA officers and other security officials to commit serious human rights violations with impunity and includes a criminal judicial system that readily accepts and relies on torture-tainted ‘confessions’ to convict defendants in trials that fail to respect the right to due process and often result in long prison terms or death sentences.” (p. 10)

The Report explains that the Egyptian NSA is responsible for maintaining the internal stability of the Egyptian State, through the collection of information (p. 18). AI has documented that the NSA routinely searches, monitors and enters houses of the victims of enforced disappearances without a judicial order and contrary to Articles 54 and 58 of the Egyptian Constitution (p. 23).

The Report concludes by calling on the international community to “impose a binding cessation on exports of equipment of the type that has been used, and is likely to be used, by the Egyptian security forces to commit or facilitate serious violations of human rights. The Report notes that the scope of the cessation should include at a minimum all...surveillance technologies” (para. 11.2.2, p. 68).

In addition, PI's research paper: ‘The President’s Men? Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure’ draws the link between the purchase of surveillance technologies by the Egyptian government's Technical Research Department (the "TRD") with a pattern of political repression and curtailment of press freedoms.⁹ The TRD is most likely a branch of the Egyptian government's General Intelligence Service, and an integral part of Egypt's intelligence infrastructure. The TRD has reportedly purchased a range of surveillance technologies, including for a communications monitoring centre, interception management system, and highly intrusive spyware (p. 10).

Surveillance technology appears to have been purchased by the TRD from EU companies. For example, in or before 2011, Nokia Siemens Networks (“NSN”) sold an interception management system and a monitoring centre for fixed and mobile networks to the TRD, providing the Egyptian government with the capability to surveil its population on a mass scale by intercepting phone communications of any line routed through the new system (p. 13).

These items may have been used by the Egyptian government, via the TRD, to commit serious violations of human rights, including acts of internal repression. Other authoritarian regimes exhibit this pattern. In Iran, the Wall Street Journal alleged that the same type of monitoring centre sold by NSN to the TRD was used during protests in 2009 to facilitate a crackdown on opposition activists.¹⁰ In Bahrain, Bloomberg reported that a similar item was used to facilitate the arrest of political activists opposed to the government, who were subsequently tortured, while being read transcripts of their text messages and phone conversations.¹¹ This scenario parallels

⁹https://privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf

¹⁰http://www.wsj.com/articles/SB124562668777335653#mod=rss_whats_news_us

¹¹<http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomesroutine-with-help-from-nokia-siemens-networking>

reports from an Egyptian activist, who claimed that transcripts of personal emails and online chats were slipped under her door shortly before she was questioned by the Egyptian NSA.¹²

As PI's report concludes, Egypt is a party to the International Covenant on Civil and Political Rights (ICCPR), which explicitly protects the right to privacy. The use of surveillance technology to indiscriminately surveil Egyptian residents, including protesters and journalists, would clearly contravene Egypt's obligations under the ICCPR.

On 21 August 2013, the Council of the EU, in its 'Council Conclusions on Egypt' stated:

*"Member States also agreed to suspend export licenses to Egypt of any equipment which might be used for internal repression and to reassess export licences of equipment covered by Common Position 2008/944/CFSP and review their security assistance with Egypt."*¹³

The Council of the EU reiterated these conclusions in February 2014.¹⁴

On 10 March 2016, the EU Parliament passed a resolution, calling for "the suspension of any form of security cooperation with Egyptian authorities" considering the recent backdrop of human rights violations, including torture, deaths in custody and enforced disappearances across the country.¹⁵

Further, as you will be aware, an investigation into the torture and murder of Italian student Giulio Regeni is still under way in Egypt, where police recently admitted to spying on Regeni prior to his murder.¹⁶

Request for Information & Assurances

Given the information available on the use of IP network communications surveillance systems for human rights abuses and the deteriorating human rights protection in Egypt, we would appreciate an urgent response to the questions below:

- a. Whether, as reported in La Stampa on 28 June 2016 and elsewhere, Area SpA obtained a license to export IP surveillance equipment to the TRD in Egypt. If so:
 - 1) Is the end use, as stated in the export license, (or might the end use be) for military, security, intelligence, or law enforcement purposes?
 - 2) Whether Mise accepts as accurate (or at least credible) reports by the EU Parliament and NGOs of serious human rights violations in Egypt; including torture and other cruel, inhuman and degrading treatment or punishment; summary or arbitrary executions; enforced disappearances; arbitrary detentions; and other major violations of IHRL (directed against political dissidents, trade unionists, human rights activists and others).
 - 3) What information was obtained and considered prior to the granting of the licence to export Equipment to Egypt regarding:
 - 3.i. the end users and if they might have been involved in internal repression and/or serious violations of IHRL or IHL;
 - 3.ii. the commitment of the governments of Egypt (and their respective end users) to respect human rights and the rule of law;
 - 3.iii. the findings of any independent monitoring and/or investigations of alleged repression or serious violations of IHRL or IHL and whether it has implemented any findings.
 - 4) Whether Mise is satisfied that Egypt has in place (and effectively enforces) domestic legislation to prevent violations of IHL and IHRL, arrangements to prosecute, discipline

¹²<http://www.madamasr.com/sections/politics/sexual-assault-and-state-history-violence>

¹³http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151710.pdf

¹⁴http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/140971.pdf

¹⁵<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT+MOTION+B8-2016-0338+0+DOC+XML+V0%2F%2FEN&language=EN>

¹⁶<https://www.varsity.co.uk/news/10650>

and/or punish any state entities or officials who commit IHL or IHRL violations, or domestic legislation which ensures adequate protection for human rights, including the rights to privacy and freedom of expression. Please confirm whether any of these issues were considered in granting licences for the Equipment to any of the destination countries.

- 5) Whether any end user guarantees were sought for any of the grants of export licences of equipment and, if so, the details on what conditions were made.
- 6) On what basis Mise concluded that any grant of a licence to export IP surveillance equipment to the Egyptian TRD, was/is compatible with Italy's human rights obligations?
- 7) On what basis Mise concluded that any grant of a licence to export IP surveillance equipment to the Egyptian TRD was/is compatible with the 'Council Conclusions on Egypt' agreed on 21 August 2013, wherein "*Member States also agreed to suspend export licenses to Egypt of any equipment which might be used for internal repression*".
- 8) Whether, owing to the respective developing human rights situations in Egypt, Mise has considered revoking or suspending the export licences to Egypt.
- 9) Given the human rights concerns highlighted above, whether Mise will now suspend the licences to Egypt.

We thank you for your attention in this matter and look forward to a prompt response.

Yours sincerely,

Edin Omanovic
Privacy International
edin@privacyinternational.org

Antonella Napolitano
Coalizione Italiana Libertà e Diritti civili
antonella@cild.eu

Fabio Pietrosanti
Hermes Center for Transparency and Human Rights
fabio.pietrosanti@logioshermes.org