European Ombudsman/Médiateur européen
1 avenue du Président Robert Schuman
CS 30403
F-67001 Strasbourg Cedex
France

COMPLAINT TO THE EUROPEAN OMBUDSMAN UNDER ARTICLE 228 TFEU: EU TRANSFERS OF SURVEILLANCE CAPABILITIES TO THIRD COUNTRIES

I. The complainants

Privacy International (PI) is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.[1] PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. This submission relates to PI's ongoing work on 'Challenging the Drivers of Surveillance'.[2]

Access Now defends and extends the digital rights of users at risk around the world.[3] By combining direct technical support, comprehensive policy engagement, global advocacy, legal interventions, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Border Violence Monitoring Network (BVMN) is a non-profit coalition of organizations working to document in the form of testimonies and consolidated into reports human rights violations at border, pushbacks, collective expulsions and state violence along the EU's external borders in the Western Balkans, Greece and Turkey since the network's formulation in 2016.[4] BVMN is registered under the framework of RigardU e.V. in Germany.

Homo Digitalis (HD) is a digital rights civil society organization based in Athens, Greece.[5] HD works for the protection of human rights and freedoms in the digital age, by organist raising awareness activities for the wider public, conducting research studies to inform policy decisions, and participating in legal actions before competent authorities an national and EU level.

International Federation for Human Rights (FIDH) is an international human rights NGO federating 192 organisations from 117 countries.[6] Since 1922, FIDH has been defending all civil, political, economic, social and cultural rights as set out in the Universal Declaration of Human Rights.

Sea-Watch e.V. is a civil non-profit organisation (NGO) which has conducted search and rescue operations in the Central Mediterranean Sea for over five years, currently with the *Sea-watch 3* and the *Sea-Watch 4*.[7] Sea-Watch also documents human rights violations

[1] Privacy International (PI), https://privacyinternational.org.
[2] PI, Challenging the Drivers of Surveillance, https://privacyinternational.org/challenging-drivers-surveillance.
[3] Access Now, https://www.accessnow.org.
[4] Border Violence Monitoring Network (BVMN), https://www.borderviolence.eu.
[5] Homo Digitalis (HD), https://www.homodigitalis.gr/en.
[6] International Federation for Human Rights (FIDH), https://www.fidh.org/en.
[7] Sea-Watch e.V., https://sea-watch.org/en.

and reports people in distress using civil reconnaissance airplanes, *Moonbird* and *Seabird,* operated together with the Swiss non-profit organisation *Humanitarian Pilots Initiative*.

II. Purpose of this Submission

The purpose of this complaint is to request the European Ombudsman to open an inquiry into whether the failure of the EU institutions and bodies listed below to carry out (prior) human rights risk and/or impact assessments when transferring surveillance capabilities to third countries constitutes maladministration.

The aforementioned organisations (hereinafter the **'Complainants'**) are gravely concerned about the activities carried out by the European Commission as well as the European Border and Coast Guard Agency (Frontex), the European Union Agency for Law Enforcement Training (CEPOL) and the European External Action Service (EEAS), which relate to the transfer of surveillance capabilities, involving capacity building or trainings of third country authorities in surveillance techniques, the transfer of surveillance equipment to third countries, as well as any other support.

EU institutions are under an obligation to conduct human rights risk and impact assessments prior to engaging in any form of surveillance transfer. Prior risk and impact assessments are needed to ensure that any surveillance transfer will not result to serious violations of the right to privacy or that it will not facilitate other human rights abuses. However, our extensive research into EU surveillance transfers suggests that in most of these cases no (prior) human rights risk and impact assessments seem to have been carried out prior to the engagement of the aforementioned bodies with authorities of third countries.

We believe that such practices raise significant concerns about the institutions' compliance with their obligations under EU law and could amount to instances of maladministration.[8] They may not only result in impeding transparency and public scrutiny, but they may also seriously undermine the rights and freedoms of both EU and non-EU citizens, including human rights defenders and journalists. Such transfers will very often involve extremely intrusive forms of surveillance that, without the proper (prior) assessments, could be left prone to abuse by regimes that fail to respect human rights.

PI also asserts that despite its constant efforts to have access to more information around the compliance of the aforementioned institutions with their EU law obligations, by filing, among others, a series of access to documents requests under EU Regulation 1049/2001,[9] it is still unclear whether and how human rights considerations, including but not limited to considerations with regard to individuals' privacy and data protection rights, are taken into consideration by the aforementioned bodies.

The Complainants are therefore urging the European Ombudsman to open an inquiry into the concerns detailed in this submission and to investigate the matter, including by obtaining further documents by the relevant institutions and bodies. Specifically, we are,

[8] According to the European Ombudsman, *"[m]aladministration occurs if an institution or body fails to act in accordance with the law or the principles of good administration, or violates human rights. Maladministration can include administrative irregularities, unfairness, discrimination or the abuse of power, for example in the managing of EU funds, procurement or recruitment policies. It also includes the failure to reply, or the refusal or unnecessary delay in granting access to information in the public interest*", https://www.ombudsman.europa.eu/en/how-can-the-ombudsman-help.

[9] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

first, asking the Ombudsman to confirm that the bodies complained against are under an obligation to carry out human rights risk and impact assessments prior to engaging in any form of transfer of surveillance capabilities to authorities of third countries. Second, should the European Ombudsman find that the aforementioned bodies have failed to carry out said assessments, we ask her to find that such failure constitutes maladministration, and we invite her to issue recommendations to effectively address the matter that could potentially have implications for millions of people located both within and outside the EU.

This complaint is structured in four parts. The first part provides an overview of the key institutional frameworks that we have identified as enabling EU transfers surveillance capabilities to authorities of third countries. The second details the previous engagement and exchanges PI had with the European Commission and other EU institutions as part of its access to documents requests and other avenues. The third part describes the legal framework, under which we understand that EU institutions are obliged to carry out human rights risk and impact assessments before engaging with authorities of third countries in the context of transfers of surveillance capabilities. Finally, our complaint highlights the grave human rights concerns arising in the context of surveillance transfers and provides further evidence of lack of (prior) human rights risk and impact assessments.

III. Involvement of EU bodies in the transfer of surveillance capabilities to third countries

EU bodies and EU member states have pursued counterterrorism and migration policies at odds with fundamental values. As a result, for example, the EU has passed legislation regarding the collection and use of Passenger Name Record (PNR) data,[10] has funded the development of advanced surveillance technology,[11] and is seeking interoperability between EU large-scale information systems, which the European Data Protection Supervisor has stressed "*could become a dangerous tool against fundamental rights.*"[12]

Below we have identified some of the key institutional frameworks through which the EU funds the development and installation of advance surveillance technologies, as well as transfers surveillance capabilities to authorities of third countries.

a) EU Trust Fund for Stability and Addressing Root Causes of Irregular Migration and Displaced Persons in Africa

The EU Trust Fund for Stability and Addressing Root Causes of Irregular Migration and Displaced Persons in Africa (EUTF for Africa) was set up in the wake of the 2015 'migration crisis' in Europe and is largely made up of money earmarked for development aid (80% of its budget comes from development and humanitarian aid funds).[13] EUTF for Africa commits billions of euros to tackle and "manage" migration from African countries.[14]

---

[10] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119.

[11] Statewatch, The European security-industrial complex, 24 May 2021 (latest update), https://www.statewatch.org/observatories/the-european-security-industrial-complex.

[12] EDPS, Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 2018/C 233/07, https://edps.europa.eu/sites/default/files/publication/18-04-16_opinion_interoperability_executive_summary_en.pdf.

[13] PI, The Future of the EU Trust Fund for Africa: Policy Briefing, September 2019, https://privacyinternational.org/sites/default/files/2019-09/EUTF%20Policy%20Briefing.pdf.

[14] European Commission, EU Emergency trust Fund for Africa, https://ec.europa.eu/trustfundforafrica/index_en.

The EUTF for Africa was established to support the implementation of the 2015 Joint Valetta Action Plan,[15] which lists as priorities the reinforcement of "[s]tate capacity to ensure security and fight against terrorist threats", the prevention of irregular migration through capacity building and provision of relevant equipment to law enforcement and border management authorities, the improvement of intelligence gathering and sharing, the improvement of border management systems, and the provision of civil registry systems and biometric identification in order to facilitate the return and readmission of irregular migrants.[16]

As well as equipping and training security agencies in surveillance, the Fund is being used to bankroll the development of mass-scale biometric identity systems across the African continent and is awarding lucrative contracts to well-connected European security companies in the process.[17]

b) European Neighbourhood Instrument

The European Neighbourhood Instrument (ENI) has provided over €15 billion from 2014-2020 to non-EU countries to its east and south aiming to foster human rights and the rule of law, reduce poverty, and support economic development, among other priorities.[18]

c) Instrument contributing to Stability and Peace

With a budget of €2.3 billion for 2014 – 2020, the Instrument contributing to Stability and Peace (IcSP) funds projects aimed at conflict prevention, peacebuilding, crisis response and managing security threats.[19]

d) The Instrument for Pre-accession Assistance

The Instrument for Pre-accession Assistance (IPA) is the means by which the EU funds countries which are potential future members and provides them with technical assistance, amounting to some €11.7 billion for the period 2014-2020.[20]

e) European External Action Service

The European External Action Service (EEAS) is the EU's "diplomatic service", responsible for implementing its Common Foreign and Security Policy, which includes promoting environmental protections, providing assistance in crisis zone, and promoting democracy worldwide.[21] The EU is a key security player in the Sahel region, providing €147 million to

---

[15] European Commission, Joint Valletta Action Plan (JVAP), https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/joint-valletta-action-plan-jvap_en.

[16] Council of the European Union, Joint Valetta Action Plan – Updated Version, https://www.statewatch.org/media/1835/eu-council-migration-plan-jvap-updated-5722-21.pdf.

[17] PI, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds, 10 November 2020, https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

[18] EU Neighbours, The European Neighbourhood Instrument (ENI), https://www.euneighbours.eu/en/policy/european-neighbourhood-instrument-eni.

[19] EU External Action Service, Instrument contributing to Stability and Peace (IcSP), https://eeas.europa.eu/topics/instrument-contributing-stability-and-peace-icsp_en.

[20] European Commission, European Neighbourhood Policy and Enlargement Negotiations, https://ec.europa.eu/neighbourhood-enlargement/instruments/overview_en.

[21] EEAS, About the European External Action Service (EEAS), https://eeas.europa.eu/headquarters/headquarters-homepage/82/about-european-external-action-service-eeas_en.

establish the African led G5 Sahel Joint Force aiming to improve regional security and fight terrorist and criminal groups[22].

f) European Border and Coast Guard Agency (Frontex)

The European Border and Coast Guard Agency (Frontex) is responsible for border control of the EU Schengen area.[23] In 2016, its mandate and role was significantly increased and is now involved in joint operation in non-EU countries. Frontex has concluded working arrangements with the authorities of 18 countries.

IV. PI's correspondence with EU institutions and bodies, and access to documents requests to EU institutions

a) Communication with the European Commission

On 23 September 2019, PI wrote to the European Commission to share its concerns and request further clarifications with regard to the activities of the EUTF for Africa (Annex 1).

On 28 October 2019, the European Commission replied to PI by email, stating that *"[t]hrough the EU Trust Fund for Africa, we assist our partners in Mali, Senegal, Cabo Verde, Guinea and Ivory Coast in the rollout of a secure civil registry system and biometric database for identity and travel documents*". While the Commission's response conceded that they provide "*capacity building to ensure that partner countries enforce a proper legal framework*" and that they also "*provide trainings for national authorities and support awareness raising campaigns on the use of biometric data*", they noted that there "***is no obligation or need for the Commission to carry out a data protection impact assessment for EU Trust Fund Projects***" (emphasis added). The response makes no reference to the need of any other risk and impact assessment to be carried out in the context of the activities of the EUTF for Africa (Annex 1.1).

On 29 April 2020, PI followed up to the European Commission's response with a letter, requesting "*more information on the Fund's current policies and practices*" (Annex 1.1). The letter outlined PI's alarms and asked the Commission, among others, to:

- Provide more details on what "*measures to protect human rights, notably by providing capacity building to ensure that partner countries enforce a proper legal framework*" will be undertaken;
- Provide more information on what risk assessments or due diligence was undertaken to ensure the biometric databases being supported are lawful.

On 5 June 2020, the European Commission responded to PI via email (see full response in Annex 1.2). Their response provides further information on the nature and extent of the activities and projects within the EUTF for Africa:

> **Under question 1**, you request to "*provide more details on what measures to protect human rights, notably by providing capacity building to ensure that partner countries enforce a proper legal framework, will be undertaken".*
>
> The EUTF programmes supporting the modernisation of the civil registry systems and e-identification include a preliminary diagnosis of the national legal framework (including data protection legislation), as well as components of capacity building

[22] EEAS, The European Union's Partnership with the G5 Sahel Countries, https://eeas.europa.eu/sites/default/files/factsheet_eu_g5_sahel_july-2019.pdf
[23] Frontex, Our mission, https://frontex.europa.eu/about-frontex/vision-mission-values/.

for the government staff working with civil registration (on the entire applicable legal framework, not only data protection).

EUTF programmes working on civil registration do not provide equipment for identification, nor training to operate equipment for identification. Most of the EUTF programmes provide capacity building for reform of the civil registration system, including the use of computers and databases for registering population.

Under question 4, you request to provide more information *"on what risk assessments or due diligence was undertaken to ensure the biometric databases being supported are lawful"*.

Each programme is based on an assessment of the existing national legislation and the existing databases. Projects supported by the EU assess whether there are any gaps in the legislation, including on data protection and privacy. Additionally, project support the Government in drafting legislation which provides legal basis for biometric databases.

b) Access to documents requests

Between August and November 2019, PI submitted a series of access to documents requests, under Regulation (EC) No 1049/2001, to several EU bodies regarding the transfer of surveillance capabilities to non-EU countries.[24] The requests seek documents providing information on the transfer of personal data, surveillance technology, training, financing, and legislation to third countries, and were submitted to:

- European Border and Coast Guard Agency (Frontex)
- European Union Agency for Law Enforcement Cooperation (Europol)
- The European Union Agency for Law Enforcement Training (CEPOL)
- The European External Action Service (EEAS)
- The Directorate-General for Economic and Financial Affairs (DG ECFIN)
- The Directorate-General for Budget (DG BUDG)
- The Directorate-General for Migration and Home Affairs (DG HOME)
- The Directorate-General for International Cooperation and Development (DG DEVCO) (now Directorate-General for International Partnerships (INTPA))
- The Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR)
- The Data Protection Officer at the European Commission (EC DPO)
- The European Data Protection Supervisor (EDPS)

Among others, PI requested documents relating to:

- how the agencies ensured that any transfer of surveillance capabilities would adhere to EU human rights law and principles, including a request for any risk and/or due diligence assessments, evaluations or audits were conducted, and specific information about the type and content of these risk and/or due diligence assessments, evaluations or audits;
- transfers of personal data to third countries in the context of migration or law enforcement, including documents showing whether Data Protection Impact Assessments were conducted in the context of transfer agreements and/or for

[24] PI, Challenging the Drivers of Surveillance: EU Access to Documents Requests, 18 September 2019, https://privacyinternational.org/report/3225/challenging-drivers-surveillance-eu-access-documents-requests.

each transfer, in accordance with Regulation 2018/172or any other previous instrument. PI also requested copies of all relevant documents containing an assessment or evaluation of the impact of the envisaged transfer on the protection of personal data, as well as the documents containing information about the risks posed by the further processing by the authority or authorities of third countries and how these were mitigated.

Additionally, in January 2020, PI submitted an access to documents request to the EU Trust Fund for Stability and Addressing Root Causes of Irregular Migration and Displaced Persons in Africa (Annex 2) requesting any documents related to the following projects:

- "Sector reform contract / Support for civil status reform in Côte d'Ivoire" (« Contrat de réforme sectorielle / Appui à la réforme de l'état civil en Côte d'Ivoire ») (Référence: T05-EUTF-SAH-CI-01)
- "Support program for strengthening the civil status information system and creating a national biometric identity file – Senegal" (« Programme d' appui au renforcement du système d'information de l'état civil et à la création d'un fichier national d'identité biométrique - Sénégal») (Référence: IATI ID XI-IATI-EC_DEVCO_T05-EUTF-SAH-SN-07)

Notwithstanding the clarifications provided in the sections below, all of the EU agencies and bodies that responded to PI's access to documents requests confirmed that they appear to not hold or to have refused to disclose documents pertaining to any sort of (prior) human rights risk or impact assessments carried out in the context of transfer of surveillance capabilities by the European Union to third-country authorities.

With regard to DG NEAR, PI originally submitted an application for access to documents on 2 August 2019, asking for documents pertaining to the system for legal interception of communications located in the State Investigation and Protection Agency (SIPA) in Bosnia-Herzegovina, to which DG NEAR replied on 20 September 2019 (Annex 3). With regard to the existence of (prior) human rights risk and impact risk assessments, including any privacy or data protection impact assessments, the response notes:

> [T]he Commission does not hold any documents that contain information on due diligence checks, risk assessments, or privacy / data protection impact assessments conducted in relation to the establishment of the system described in your query. The contract in question only concerns the purchase of the equipment. The responsibility for the implementation of the project lies with the competent authorities in Bosnia and Herzegovina thus, the legal requirements with regard to the functioning of the system, including data protection, should be in line with the applicable legal framework in Bosnia and Herzegovina (Annex 3).

On 16 November 2020, PI submitted a new application for access to documents to DG NEAR requesting copies of:

> Documents pertaining to any kind of impact assessments (human rights impact assessments, including privacy or data protection impact assessments, due diligence assessments, audit reports or any other risk assessment) that were produced in the context of transfer of surveillance capabilities by the European Union to third countries (Annex 3.1).

On 21 December 2020, DG NEAR responded to PI's access to documents request confirming that "*that the Directorate General for Neighbourhood and Enlargement*

Negotiations does not hold any documents that would correspond to the description given in your application" (Annex 3.2). The response further notes:

> Although we have not identified documents that correspond to your request, please be assured that the Commission's cooperation with third countries follows a human-rights based approach. The projects funded by the EU aim to ensure that the rule of law and human rights are respected in the activities related to these projects, and as far as possible in beneficiary countries' own regulations and procedures.

No further information was provided by DG NEAR about how the human rights compliance of the European Commission's cooperation with third countries is ensured.

With regard to the EEAS, the latter initially responded to PI's request on 13 December 2019, confirming that no documents were held by the Agency (Annex 4.1). However, following a confirmatory application by PI, EEAS responded on 9 March 2020, identifying 63 documents held by in relation to the access to documents request (Annex 4.2). Only 5 of these documents were provided to PI in full, all of them dealing with Operational Guidelines. The rest of the documents were either partially disclosed or their disclosure was refused on grounds relating to the exceptions contained in Regulation (EC) No 1049/2001. No (prior) human rights risk and impact assessments, including any privacy or data protection impact assessments, appear to have been disclosed in response to PI's access to documents request or conducted as part of the aforementioned transfer of surveillance capabilities.

Following a series of exchanges between PI and DG DEVCO, PI limited its original request to documents relating to the following two projects: West Africa Police Information System Programme (WAPIS 3) (Decision Number: 38921); Assistance technique pour la mise en oeuvre du Programme de coopération pour la sécurité intérieure entre le Sénégal et l'Union européenne (SECSEN-UE) (Decision Number: 38567) (Annex 5). On 2 February 2021, DG DEVCO responded to PI's request with regard to the WAPIS 3 project only (Annex 5.1). In its response, DG DEVCO identified a total of 28 documents, only 4 of which were provided to PI in full. The rest were either partially disclosed or their disclosure was denied on various grounds.

Some of the documents provided by DG DEVCO make references to data protection or privacy risks with regard to the WAPIS action, namely the Description of the Action (Annex 5.2/Document 2.2), the Best Practice Guide on Personal Data Protection (Annex 5.3/Document 7), the Executive Summary WAPIS Progress Report (Annex 5.4/Document 3.6). Specifically, page 15 of the Executive Summary WAPIS Progress Report (Annex 5.4/Document 3.6) highlights the existence of various data protection concerns with regard to WAPIS:

> Firstly, the implementation of WAPIS at a national level requires appropriate national data protection legislation. Not all countries have put in place the required data protection legislation. Furthermore, while some WAPIS beneficiary countries do have data protection legislation, the content of this legislation may not necessarily be uniform across all countries and may also not specifically address issues unique to data processing through WAPIS. From country missions which have been conducted, it appears that the enactment of data protection legislation falls within the mandate of ministries of technology or of communication and technology. Law enforcement authorities participating in WAPIS in countries with no data protection legislation do not appear to have leverage with those state authorities whose mandate it is to adopt data protection legislation.

Nevertheless, it appears that no human rights risk and impact assessments, including any privacy or data protection impact assessments, were disclosed in response to PI's access to documents request or conducted as part of the aforementioned transfer of surveillance capabilities.

Finally, with respect to the documents disclosed by the EUTF for Africa detailing the development of the €28 million biometric identity system in Senegal,[25] a data protection study (Annex 2.1/Document 7.7) was conducted to allegedly guarantee the effectiveness of the central register of civil status (Annex 2.2/Document 3.3, page 7) and to ensure that that it complies with international data protection standards (Annex 2.2/Document 3.3, page 7).

However, the document disclosed contains several suggestions that diverge from international data protection standards. Beyond the data protection study, the only other study that pertains to an impact assessment is a separate informatic and security study which confines itself to some general information of possible technical options for securing the information (Annex 2.3/Document 7.6). No (prior) human rights risk and impact assessments appear to have been conducted, which would have enabled the identification and management of data protection and privacy risks arising from the project.

V. Relevant Legal Framework

Article 228(1) of the Treaty of the Functioning of the European Union (TFEU) empowers the EU Ombudsman to receive, examine and report on complaints "*from any citizen of the Union or any natural or legal person residing or having its registered office in a Member State concerning instances of maladministration in the activities of the Union institutions, bodies, offices or agencies concerning instances of maladministration in the activities of the Union institutions, bodies, offices or agencies*".

With the approval of the European Parliament, the European Ombudsman has defined 'maladministration' in a way that requires respect for human rights, for the rule of law and for principles of good administration.[26] According to the European Ombudsman:

> [m]aladministration occurs if an institution or body fails to act in accordance with the law or the principles of good administration, or violates human rights. Maladministration can include administrative irregularities, unfairness, discrimination or the abuse of power, for example in the managing of EU funds, procurement or recruitment policies. It also includes the failure to reply, or the refusal or unnecessary delay in granting access to information in the public interest[27]

In accordance with its founding principles, including the principles of liberty, democracy, respect for human rights and freedoms and the rule of law, the European Union's external relations are underpinned by a constant commitment to human rights and freedoms and

[25] EUTF for Africa, Programme d'appui au renforcement du système d'information de l'état civil et à la création d'un fichier national d'identité biométrique, https://ec.europa.eu/trustfundforafrica/region/sahel-lake-chad/senegal/programme-dappui-au-renforcement-du-systeme-dinformation-de-letat_en.
[26] European Ombudsman, 2006 Annual Report, page 10, https://www.ombudsman.europa.eu/en/publication/en/3415.
[27] European Ombudsman, How can the Ombudsman help?, https://www.ombudsman.europa.eu/en/how-can-the-ombudsman-help.

the rule of law.[28] Article 2 of the Treaty on European Union (TEU) underlines that the EU's founding values are "*human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*". Article 3 of the Treaty on European Union (TEU) requires the European Union in "*its relations with the wider world*" to contribute to "*the protection of human rights*", while Article 21 of the TEU lists "*democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity*" among the principles inspiring the European Union's external action. Similarly, Article 205 of the Treaty on the Functioning of the European Union (TFEU) determines that the EU's international actions are to be guided by the principles laid down in Article 21 of the TEU.

Article 21(3) of the TEU clarifies that the EU has a duty to respect the listed principles, including human rights, in the development and implementation not only of all areas of the Union's external action, but also of the external aspects of its other policies. Human rights, therefore, form part of those common principles and objectives that should cement policy coherence among different areas of the EU's external action.[29]

With the adoption of the Treaty of Lisbon on 1 December 2009, the Charter of Fundamental Rights of the European Union (CFREU) came into direct effect, as provided for by Article 6(1) TEU, thereby becoming a binding source of primary law.[30] Most of the rights recognised by the Charter are granted to "*everyone*" regardless of nationality or status. Among the rights and freedoms guaranteed by the CFREU are human dignity (Article 1), the right to life (Article 2), respect for private and family life (Article 7), protection of personal data (Article 8), freedom of expression and information (Article 11), the right to asylum (Article 18), the prohibition of collective expulsion (Article 19), the right to good administration (Article 41) and the right of access to documents (Article 42).

Article 51 para 1 of the CFREU states that "*the provisions of this Charter are addressed to the institutions, bodies, offices and agencies of the Union*". It adds that *"[t]hey shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers.*"

In its judgment in *Ledra*, the Court of Justice of the European Union (CJEU) confirmed that Article 51 CFR applies to the EU institutions always and at all times as it is addressed to them also "when they act outside the EU legal framework".[31] In its reviews of the compatibility of the European Commission's actions with the CFREU, the CJEU has increasingly focused on procedural aspects, assigning particular weight, among others, to whether EU institutions have exercised due diligence in assessing the potential fundamental rights impacts of their choices.[32]

Furthermore, the second EU Action Plan on Human Rights and Democracy, published by the Council of the European Union in 2015 and seeking to cover the period between 2015 and 2019, underlines:

> The EU will promote human rights in all areas of its external action without exception. In particular, it will integrate the promotion of human rights into trade,

[28] European Parliament, Human Rights, https://www.europarl.europa.eu/factsheets/en/sheet/165/human-rights.
[29] Chiara Macchi, With trade comes responsibility: the external reach of the EU's fundamental rights obligations, Transnational Legal Theory (Vol. 11:4, 2020) pages 409-435.
[30] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
[31] Case C-8/15 P, *Ledra Advertising v. Commission and ECB*, 20 September 2016, para 67.
[32] See Olivier De Schutter, The implementation of the Charter by the institutions of the European Union in Steve Peers et al (eds), The EU Charter of Fundamental Rights: A Commentary (Hart Publishing, 2014), pages 1644-1645.

> investment, technology and telecommunications, Internet, energy, environmental, corporate social responsibility and development policy as well as into Common Security and Defence Policy and the external dimensions of employment and social policy and the area of freedom, security and justice, including counter-terrorism policy. In the area of development cooperation, a human rights based approach will be used to ensure that the EU strengthens its efforts to assist partner countries in implementing their international human rights obligations.[33]

The European Ombudsman has repeatedly held that the European Commission's refusal to conduct a human rights impact assessment in the context of trade agreement negotiations constitutes maladministration. For example, in her draft recommendation adopted on 26 March 2015, the EU Ombudsperson found that "*the Commission's failure to carry out a specific human rights impact assessment, in relation to Vietnam, constitutes maladministration.*"[34] The issue in this case was whether the European Commission should carry out a human rights impact assessment in the context of its negotiations to conclude a free trade agreement with Vietnam:

> 10. In her analysis leading to her recommendation, the Ombudsman pointed out that good administration means, in the first place, observance of and respect for fundamental rights. In fact, where fundamental rights are not respected, **there cannot be good administration**. Accordingly, EU institutions and bodies must always consider the compliance of their actions with fundamental rights and the possible impact of their actions on fundamental rights. This applies also with respect to administrative activities in the context of international treaty negotiations.
>
> 11. The Ombudsman noted that the principles set out in Article 21(1) TEU and Article 21(2) TEU apply also in the area of the common commercial policy. Although the Ombudsman agreed with the Commission that there appears to be no express and specific legally binding requirement to carry out a human rights impact assessment concerning the relevant free trade agreement, she took the view that it would be in conformity with the spirit of the legal provisions mentioned above to carry out a human rights impact assessment. Since the 2009 sustainability impact assessment concerning ASEAN covers only certain aspects of the impact on social rights, it is not a proper substitute for a human rights impact assessment.
>
> 25. As rightly argued by the complainants, the human rights impact assessment is not a collection of data or a response to public opposition, but rather an analytical tool for demonstrating that all necessary factors and circumstances have been taken into account in framing a policy. The human rights impact assessment tool identifies the sources of risks and the human rights impacts on the affected stakeholders at each stage of the implementation of the agreement concerned. Its role is preventive in the first place because when negative impacts are identified, either the negotiated provisions need to be modified or mitigating measures have to be decided upon before the agreement is entered into. This analytical tool

[33] Council of the European Union, EU Action Plan on Human Rights and Democracy (2015), page 10, https://www.consilium.europa.eu/media/30003/web_en__actionplanhumanrights.pdf.
[34] European Ombudsman, Draft recommendation of the European Ombudsman in the inquiry into complaint 1409/2014/JN against the European Commission (26 March 2015), https://www.ombudsman.europa.eu/en/recommendation/en/59398.

> cannot be replaced by trade or non-trade policy measures, meetings with stakeholders, internal summaries or reports of such meetings.[35]

Most recently, in March 2021, the European Ombudsman found that the European Commission's failure to complete a sustainability impact assessment (SIA) essential to evaluating the social and environmental impact of the negotiated trade deal between the EU and Mercosur – the South American trade bloc comprised of Argentina, Brazil, Paraguay and Uruguay – constituted maladministration.[36] In her decision, the Ombudsman noted that "*while it was impossible to foresee the dynamics of the negotiations, the SIA in this case has taken much longer to finalise than anticipated. Specifically, the Commission should have ensured that the SIA was finalised before the conclusion of the EU-Mercosur trade negotiations*".[37] She also underlined that:

> 39. While Article 21 TEU does not set out an explicit and legally binding requirement to conclude an SIA before the end of trade negotiations, SIAs are one of the Commission's most important tools to ensure that the principles set out in Article 21 TEU are respected in trade agreements.[38]

Our understanding is that EU institutions are under an obligation to conduct human rights risk and impact assessments, including privacy and data protection impact assessments, prior to engaging in any form of surveillance transfer. Such assessments must consider impact and risks on the whole spectrum of human rights. Without prior assessments it is not possible to ensure that any surveillance transfer will not cause serious violations of or interferences with privacy or other fundamental rights.[39] They may not only result in impeding transparency and public scrutiny but may also seriously undermine the rights and freedoms of both EU and non-EU citizens, including human rights defenders and journalists.

While the transfer of surveillance capabilities to third countries will very often involve extremely intrusive forms of surveillance that without the proper (prior) assessments could be left prone to abuse by regimes that fail to respect human rights, our findings based on the documents disclosed to us and relevant desk-research suggest that, in most of these cases. No human rights risk and impact assessments seem to have been carried out prior to the engagement of the aforementioned bodies with authorities of third countries.

VI. The need for (prior) human rights risk and impact assessments, including privacy and data protection impact assessments, in EU transfers of surveillance capabilities to third countries

As it will be outlined below, the disclosures obtained by PI suggest that authorities of third countries are trained in controversial surveillance techniques, equipped with intrusive surveillance tools or, generally, supported in carrying out surveillance by the EU without any

[35] European Ombudsman, Decision in case 1409/2014/MHZ on the European Commission's failure to carry out a prior human rights impact assessment of the EU-Vietnam free trade agreement (26 February 2016), https://www.ombudsman.europa.eu/en/decision/en/64308.
[36] European Ombudsman, Decision in case 1026/2020/MAS concerning the failure by the European Commission to finalise an updated 'sustainability impact assessment' before concluding the EU-Mercosur trade negotiations (17 March 2021), https://www.ombudsman.europa.eu/en/decision/en/139418#_ftnref16.
[37] Ibid.
[38] Ibid.
[39] On biometric data, see Dr. Krisztina Huszti-Orbán and Prof. Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' – Report prepared under the aegis of the Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2020), https://www.law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists.

(prior) human rights risk and impact assessments, including any privacy or data protection impact assessments, by the relevant agencies or bodies.

1. Trainings on controversial surveillance techniques and tools

To support EU policies in neighbouring countries, the European Union Agency for Law Enforcement Training (CEPOL) facilitates experts and law enforcement officials from EU member state authorities to train counterparts from agencies across the Balkans, Northern Africa, and the Middle East. Documents obtained by PI suggest that CEPOL is facilitating training in surveillance techniques prone for abuse, which lack safeguards in EU countries themselves, including courses in advanced open-source intelligence gathering techniques, the use of indiscriminate surveillance equipment, techniques for cracking mobile devices, and methods for investigating charities.[40]

While people in many of these countries face serious security threats as well as under-resourced public services, they are also confronted with unaccountable security agencies that engage in the unlawful surveillance of civilians enabled by inadequate legal frameworks and human rights protections. In the absence of effective human rights, including privacy and security safeguards and in contexts where security agencies arbitrarily target activists, journalists and others, surveillance techniques and tools pose a serious threat to people's rights and their work.

Specifically, the documents obtained following PI's access to documents requests indicate that CEPOL is facilitating training in open-source intelligence gathering to several third-country authorities.[41] For example, a training session organised by CEPOL in April 2019 to 20 members of Algeria's National Gendarmerie, a rural police force, provides an insight into the regime (Annex 6). Participants are advised to use "sock puppets" for open-source research - anonymous and fake profiles used to gather intelligence that are harder to trace. To avoid detection, the officers are directed to purchase different sim cards for different accounts, use picture editing tools, and to remember to post frequently and outside of work hours. Participants are also recommended online platforms to make it easier to manage numerous fake accounts at the same time (Annex 6, pages 43-45).

At the same time as CEPOL was advising participants how to thwart these restrictions, in Algeria's capital in April 2019, while a huge protest movement, known as the Revolution of Smiles, was taking place, culminating in the resignation of President Abdelaziz Bouteflika after 20 years in power. What followed was a wave of online disinformation and censorship, driven by networks of pro-regime fake accounts posting propaganda and reporting high-profile democracy activists.[42]

While there is no indication that any of these troll networks were organised by anyone who attended the training, the promotion by the EU of techniques used to silence pro-democracy voices in a key neighbour must nevertheless ring alarm bells. None of the documents received by CEPOL suggest that they also provided adequate training to ensure the use of these surveillance capabilities in a human rights-compliant manner.

---

[40] PI, Revealed: The EU Training Regime Teaching Neighbours How to Spy (10 November 2020), https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy.

[41] PI, Challenging the Drivers of Surveillance: EU Access to Documents Requests CEPOL Disclosures, https://privacyinternational.org/legal-case-files/4286/challenging-drivers-surveillance-eu-access-documents-requests-cepol.

[42] Layli Forudi, In Algeria, 'electronic flies' threaten a protest movement (Coda Story, 10 December 2019), https://www.codastory.com/disinformation/algeria-election-protest.

In a module on how to "*go further*" on Facebook provided to 20 agents of Morocco's Directorate General for National Security (DGNS), accompanied by the advice that Facebook has been "*helping stalkers since 2004*", the participants are advised to never use their personal profile, but to use fake profiles which are described as precious assets which need to be maintained like an "*orchid*" (Annex 8, pages 36-41). Participants are advised to use open-source websites designed to access information from Facebook, including Stalkscan, WhoPostedWhat, PeopleFindThor, and Facebook Matrix, as well as social network analysis tools used to visualise relationships (Annex 8, pages 42ff).

A session provided in Montenegro also seems to promote the use of TrueCaller (Annex 7, page 112), an application that ostensibly allows users to identify phone numbers so they can filter out calls, even if it is from a number they have never encountered before, but which can also be utilised to identify people who have been uploaded to the TrueCaller database.[43]

As well as open-source tools, the training in Algeria describes the use of specialised surveillance tools available to law enforcement agencies. A session titled "*CDR and IPDR analysis and possible attacks against the mobile user*" describes the use of Call Detail Records (CDR) and Internet Protocol Detail Records (IPDR) in investigations (Annex 6, page 2). CDRs and IPDRs are metadata obtained from telecommunications networks and operators which describes general details of a call, such as who called who, and general details of internet traffic, such as the source and destination IP address.

A slide described "*Special Software Using SS7 and its Possibilities: Geomapping, Practical Solutions Descriptions*" (Annex 6, page 112) could likely refer to tracking the location of devices using the SS7 protocol, a suite which allows telecommunications' operators to talk to one another, for example to aid roaming.[44] By exploiting the protocol, law enforcement agencies are able to identify a device's location: a whistle-blower recently revealed that operators in Saudi Arabia were using such SS7 look-ups to track the locations of individuals in the US.[45]

Another slide titled "*IMSI Catchers and Radio Transmitters*" (Annex 6, page 104), also provided to participants in a training session in Montenegro (Annex 7, pages 79ff), refers to IMSI Catchers. The latter are indiscriminate tools used to identify mobile devices in a certain area,[46] for example, during a protest.[47] PI has sought to increase transparency around the use of such devices by law enforcement agencies in the UK, which maintain that they could "neither confirm nor deny" whether or not they use them.[48]

Other slides include "*Special Technical Solutions from Scientific Projects in the Area of Predictive and Descriptive Analytics*" (Annex 6, page 113), as well as "*Issues Around Forensic Examinations of SIMs/Handsets & Communication*" (Annex 6, page 101), as well as modules

[43] PI, "Betrayed by an app she had never heard of" - How TrueCaller is endangering journalists (28 May 2019), https://privacyinternational.org/node/2997.
[44] Tobias Engel, Locating Mobile Phones using Signalling System #7, https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.
[45] Stephanie Kirchgaessner, Revealed: Saudis suspected of phone spying campaign in US (The Guardian, 29 March 2020), https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us.
[46] PI, IMSI Catchers (6 August 2018), https://privacyinternational.org/explainer/2222/imsi-catchers.
[47] PI, IMSI catchers: facilitating indiscriminate surveillance of protesters (19 June 2020), https://privacyinternational.org/news-analysis/3948/imsi-catchers-facilitating-indiscriminate-surveillance-protesters
[48] PI, Information Tribunal Decisions re IMSI Catchers: A loss for transparency and why we will continue the fight through other means (12 June 2020), https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will.

on investigating cryptocurrency exchanges (Annex 6, pages 61ff), and the 'darknet' - websites accessible to users of Tor, the anonymous browser (Annex 6, pages 120ff).

A training session delivered in Morocco on collecting counter-terrorism information from the internet also provides an insight into how the trainings seem to promote electronic surveillance techniques. Presentations provided by EU member states officials include modules on investigating mobile phones, involving for example a technical breakdown of the architecture of telecommunications networks, how different internet and telephone hardware function, and types of unique identifiers which appear on devices and sim cards (Annex 8, pages 49-121).

A training session provided by the Policia Nacional, the national police force of Spain, to police, security, and intelligence authorities in Bosnia and Herzegovina (federal as well as those based in Republika Srpska) on financial investigations similarly outlines potential avenues for tracking IP addresses, emails, and conducting wiretapping (Annex 9, pages 52-79). A slide towards the end of the session also promotes the use of malware or computer trojans software (Annex 9, page 71) used to hack into devices to extract data and take control of functions such as the camera and microphone,[49] and sold on the open market by companies, such as NSO Group.[50]

Reports have highlighted how such technology has regularly been used to target human rights defenders, journalists, political opposition and others.[51] Most recently, Amnesty International and Forbidden Stories, in collaboration with media around the world, exposed how such technology has been used to target hundreds of devices belonging to activists, journalists, as well as European leaders, including Emmanuel Macron.[52] Without sufficient legal safeguards, the use of such technology presents a grave risk to fundamental rights given its invasiveness.[53]

In Morocco, participants were taught how to extract data from mobile phones in a module on "*telecommunication training*", including "*precautions to take when seizing a telephone*" and the exploitation of telephone data using Xry/Ufed, two high-profile brand names for mobile phone extraction software produced by MSAB[54] and Israeli-based Cellebrite[55] (Annex 8, pages 155-161). Such software is used by law enforcement agencies who have seized devices to extract and visualise data contained within them. A technical analysis by PI showed that, in addition to extracting photos, messages, and web histories, such tools can also extract content that the phone collects without any user action (and sometimes without user knowledge) such as GPS data and data contained within images, as well as data the user has deleted.[56]

Another training session goes a step further, promising access to not just what is contained within the phone, but also to what is accessible from it. A module promoting the use of cloud extraction details how forensic software is also able to extract data that is

[49] PI, Government Hacking, https://privacyinternational.org/learn/government-hacking.
[50] PI, Operating from the Shadows: Inside NSO Group's Corporate Structure (1 June 2021), https://privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure.
[51] See, for example, Citizen Lab, Targeted Threats Archive, https://citizenlab.ca/tag/targeted-threats/.
[52] Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/.
[53] European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.
[54] MSAB, XRY – Extract, https://www.msab.com/products/xry.
[55] Cellebrite, UFED, https://www.cellebrite.com/en/ufed.
[56] PI, A technical look at Phone Extraction (14 October 2019), https://privacyinternational.org/long-read/3256/technical-look-phone-extraction.

contained in the cloud (Annex 8, pages 162-168), a term used to describe user data which is stored on third-party servers, typically used by device and application manufacturers to back up data.[57] As cloud storage is increasingly used for social media, internet-connected devices and apps, such cloud extraction is capable of accessing large amounts of personal data, including from apps such as Dropbox, Slack, iCloud, Instagram, Twitter, Facebook, Uber and Hotmail, as well as messages that are end-to-end encrypted such as WhatsApp, if cloud back-up is enabled.[58] Once an authority obtains a user's credentials, not only can they obtain their cloud-based data, they can also track them using their cloud-based accounts. For example, Cellebrite claims its Cloud Analyzer can track online behaviour, analyse posts, likes, events and connections to better understand a suspect or victim's interests, relationships, opinions and daily activities.[59]

Training on financial investigations given in Tunisia provide a concerning insight into how CEPOL raises awareness about the risk of charities raising funds for terrorism, and how in doing so it risks promoting suspicion and regulatory actions designed to undermine the freedom of civil society. Specifically, three modules on financial investigations were provided to participants from the Directorate General of Training, the Directorate General of Technical Services, the Directorate General of Special Services, the Financial Brigade, the Tunisian Customs and the National Unit for the Investigation of Terrorist Crimes in 2018 and 2019 (Annex 10). Topics covered include techniques for investigating informal banking systems such as hawala banks (a transfer system popular across North Africa, the Middle East, and the Indian subcontinent), analysing accounting records, and understanding the use of businesses by financiers of terrorism (Annex 10).

Finally, another training programme, led by the Italian government but financed by the EU Trust Fund for Africa, involves the training and equipping of Libyan authorities in ways that raise human rights concerns around, for instance, the misuse of data and possible privacy infringements of third country populations in a vulnerable position. A 2018 document details the training, provided by FRONTEX to Libya's General Administration for Coastal Security (GACS) (Annex 11). The document indicates that FRONTEX taught participants how to secure "*evidence for prosecution and intelligence purposes*", including from electronic devices, how to acquire fingerprints, including from "*children and people with vulnerabilities*", as well as "*basic self-defence techniques that can be used during the apprehension of suspects on board, including the use of force and its limitations*" (Annex 11, pages 2-4).

A risk assessment undertaken for the training does not identify any possibility that the training could facilitate human rights abuses or undermine the local reputation of the EU (Annex 11.1), despite evidence of Libyan authorities shotting at or beating migrants on board vessels or threatening NGOs,[60] and reports detailing how people are then locked in

[57] PI, Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps (7 January 2020), https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data.
[58] Ibid.
[59] Ibid.
[60] Sea-Watch, So-called Libyan Coast Guard firing shots at migrant boat in distress (5 July 2021), https://sea-watch.org/en/libyan_coast_guard_shots_fired; Benjamin Bathke, When helping hurts – Libya's controversial coast guard, Europe's go-to partner to stem migration (InfoMigrants, 24 July 2019), https://www.infomigrants.net/en/post/18196/when-helping-hurts-libya-s-controversial-coast-guard-europe-s-go-to-partner-to-stem-migration.

crammed detention camps rampant with diseases and subjected to serious human rights abuses,[61] including rape and torture.[62]

2. Equipping third country authorities with surveillance and tracking equipment, whose suggested use derives from international, European and national data privacy standards

In Niger, €11.5 million was allocated from the EU Trust Fund for Africa for the provision of surveillance drones, surveillance cameras, surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher.[63] The allocation of funds for the transfer of this equipment comes in the context of a recent crackdown on activists in Niger and a surveillance legal framework which lacks essential and well-established safeguards and is in direct defiance of international legal standards.[64]

In Bosnia and Herzegovina, a wiretapping system sold by Swedish tech giant Ericsson was provided to the State Investigation and Protection Agency (SIPA) (Annex 3), which has a Memorandum of Understanding with other law enforcement agencies in the country allowing them to use the system, including the Border Police.[65]

Biometric registration equipment and databases are provided to authorities for border and migration control: for example, fingerprinting devices were provided to authorities in Bosnia and Herzegovina sold by electronics company NEC (Annex 11.2), while mass-scale biometric databases are provided to numerous countries, including Senegal and Côte d'Ivoire.[66]

To its east, on the Ukraine-Belarus border, an EU project for an "*automated intelligent video-control system*" financed cameras and license plate scanning software in order to alert authorities to information about an approaching vehicle and its passengers (Annex 3.3). Similarly, license plate scanning equipment for use by authorities along the Ukrainian-Moldovan border connected to a centralised monitoring centre was provided as part of 2018 project (Annex 3.4).

Various projects financed and managed by a mix of aid and other agencies work to provide equipment for border forces and border control purposes across Northern Africa and the Middle East. A 2018 aid project worth €11 million, for example, was provided to Lebanon to support "*the establishment and operationalisation of central operations*

---

[61] Sally Hayden, Calls for inquiry after migrants captured by Libyan coast guard shot dead (The Irish Times, 29 July 2020), https://www.irishtimes.com/news/world/europe/calls-for-inquiry-after-migrants-captured-by-libyan-coast-guard-shot-dead-1.4317019.

[62] Amnesty International, Libya 2020, https://www.amnesty.org/en/countries/middle-east-and-north-africa/libya/report-libya.

[63] EUTF for Africa, Document d'Action: Fonds fiduciaire d'urgence de l'union européenne en faveur de la stabilité et de la lutte contre les causes profondes de la migration irrégulière et du phénomène despersonnes déplacées en Afrique (T05-EUTF-SAH-NE-05), https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf. With regard to the concerns raised by IMSI catchers specifically, see also section V.1. above.

[64] PI, The Nigerien bill giving broad powers to intercept communications (2 June 2020), https://privacyinternational.org/news-analysis/3854/nigerien-bill-giving-broad-powers-intercept-communications.

[65] European Commission, IPA 2014-2020, Bosnia and Herzegovina: EU support to home affairs to combat illegal acts, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/ipa_2017_040524.03_eu_support_to_home_affairs_to_combat_illegal_acts.pdf.

[66] PI, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds (10 November 2020), https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.

rooms and coordination entities", including the armed forces' border control unit (Annex 3.5).

In Libya, more than €42 million was allocated from the Trust Fund for Africa for a border control project in 2019, which included the provision of patrol boats, SUV vehicles workstations, radio-satellite communication devices, and other equipment to authorities in Libya as well as the Directorate for Combatting Illegal Migration (Annex 3.6).

Another 2018 aid project worth €11 million was provided to Jordan to equip border crossing points with "*operational equipment, IT tools [and] software*" and to provide equipment to officers for "*specialised investigation techniques*" (Annex 3.7). The agreement states that the equipment, which can presumably range from communication devices to highly intrusive surveillance equipment, is to be "*defined at inception phase*" – meaning funds were approved before the equipment was identified (Annex 3.8).

Finally, the documents disclosed by the EUTF for Africa to PI detail the development of a €28 million biometric identity system in Senegal and raise various concerns, which also pertain to the lack of appropriate human rights risk and impact assessments. The documents received by PI suggest that no human rights risk and impact assessments or studies were even considered let alone conducted.

In addition, the documents suggest conducting a massive census operation to collect all kinds of data from the population, including biometric data. They further suggest merging in the new system data collected from other databases, including the current national ID system and the passport system. However, the documents do not specify exactly what biometric data they intend to collect. A partial answer might be found in one of the documents that were identified in response to PI's request, but which the EUTF for Africa refused to disclose (Annex 2.4).

On the contrary, the data protection study that was conducted for the project contains several suggestions that diverge from international data protection standards (Annex 2.1/Document 7.7). Among others, there is no consideration in the study that biometric data is sensitive data and as such require additional and enhanced protections. The current national data protection law does not provide for enhanced protections for biometric data. The use of biometric data is uniquely problematic given that it represents a part of a person's body, and as in the case of fingerprints and iris scans, raises concerns of sensitivity and control of one's own body. In addition, the study asks for the procedures and formalities regarding the obligations of those responsible for processing personal data to be simplified (Annex 2.1/Document 7.7). While, the current national legal framework contains only one reference to biometric data, requiring that any processing of biometric data and other data is subject to authorisation by the national data protection authority,[67] the study requests to lower this standard. Finally, the study asks for the definition of processing of data to exclude the erasure of personal data, contrary to Senegal's national law,[68] as well as international and European standards on data protection.[69] It is not clear

[67] See Law No 2008-12 of 25 January 2008 Concerning Personal Data Protection and Decree No 2008-721 of 30 June 2008 Concerning Law Enforcement, Relating to Application of the Data Protection Law, https://www.cdp.sn/content/journal-officiel-d%c3%a9cret-n%c2%b0-2008-721-du-30-juin-2008-portant-application-de-la-loi-n%c2%b0-2008-12, Article 20.
[68] Article 4, ibid.
[69] For example, both the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) (Convention 108+), which has been ratified by all EU member states, as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) include erasure or destruction of personal data in their definition of processing in articles 2(b) and 4(2), respectively.

why such an exception, which could potentially have detrimental effects for the exercise of individuals' data protection rights, is sought.

Apart from the aforementioned data protection study, the sole document that bears some resemblance to an impact assessment is a separate study which confines itself to some general information of possible technical options for securing the information (Annex 2.3/Doc. 7.6). However, it fails to consider the fact that the technology underlying identity systems is often fallible and inaccurate, leading to authentication failures which can have profoundly negative consequences for individuals, and particularly affect the most vulnerable populations,[70] and which would have been a factor examined by an appropriate human rights assessment.

3. Sharing of personal data with EU bodies

As well as providing equipment for establishing biometric identity systems, training officials in their use, and influencing laws in beneficiary countries, the documents disclosed to PI in response to its access to documents requests suggest that such initiatives might also be used to assist in deportations from Europe and to share data with EU authorities. The project justification for the establishment of a biometric identification system in Côte d'Ivoire, for example, makes it clear that one of the reasons of developing it is to facilitate the identification of people in Europe who are of Ivorian nationality and to organize their return more easily.[71] Similarly, the documents relating to the biometric identification system in Senegal repeatedly underline the need to ensure that any biometric collection will take into account the data of the Senegalese living abroad.[72]

In Niger, although EU authorities do not have direct access to databases, the Nigerien legislation which criminalises human trafficking and was developed with EU assistance,[73] stipulates that if a foreign state authority (such as one in the EU) requests the verification of the authenticity or validity of travel or identity documents believed to have been issued in Niger, the Nigerien authorities are obliged to provide relevant information to them.[74]

Finally, a 2019 project financed by the Instrument for Pre-Accession II aims to provide countries in the western Balkans with a "*registration system interoperable at the [western Balkans] regional level*", in the aim of achieving "*future interoperability with EU information systems on border and migration management*" such as the Eurodac database, a pan-European fingerprint database for asylum seekers (Annex 11.2).

As the above illustrate, by equipping and training third country authorities and developing mass-scale biometric databases in third countries, the EU is providing authorities with digital tools of surveillance, which have already been used and will likely continue to be used authorities of these countries to circumvent individuals'

[70] PI, Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations (29 March 2021), https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible.
[71] European Commission, Document d'action du Fonds Fiduciaire de l'UE, T05-EUTF-SAH-CI-01, https://rsr.akvo.org/media/db/project/7540/document/T05-EUTF-SAH-CI-01.pdf.
[72] PI, Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds (10 November 2020), https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric.
[73] Oriol Puig, Europe's invisible new border (Euractiv, 5 July 2019), https://www.euractiv.com/section/africa/news/europes-invisible-new-border.
[74] Article 36, République du Niger, Loi N° 2015-36 du 26 mai 2015 relative au traffic illicite de migrants, https://sherloc.unodc.org/cld/uploads/res/document/ner/2015/loi_relative_au_trafic_illicite_de_migrants_html/Loi_N2015-36_relative_au_trafic_illicite_de_migrants.pdf.

freedoms and violate their privacy and data protection rights as well as other fundamental rights. While we believe that EU bodies and agencies are under an explicit obligation to promote and safeguards human rights and the rule of law in all their dealings with third countries, the responses received by the EU institutions show a lack of any (prior) human rights risk and impact assessments, including any privacy and data protection impact assessments, in order to mitigate the risks described in the section above. It is therefore crucial that the European Ombudsman investigates the circumstances under which such assistance is provided to third countries by the EU and whether robust and necessary safeguards, including any (prior) assessments mentioned above, are in place to ensure the compliance of EU institutions with their human rights obligations, and whether such safeguards are applied in practice.

VII. Applications/Remedy

For the reasons set out above, the Complainants submit that the European Commission, EEAS, FRONTEX, and CEPOL have been and continue to be transferring surveillance capabilities to third countries, including trainings in the use of ambiguous and intrusive surveillance technologies, transfer of surveillance equipment as well as any other support, in absence of the required (prior) human rights risk and impact assessments, including any privacy and data protection impact assessments. As outlined above, such practices raise grave concerns with regard to the compliance of EU bodies and institutions with their obligation to respect human rights and promote the rule of law in all their external relations and can also seriously undermine the rights and freedoms of vulnerable populations within and outside the European Union. We therefore request that the aforementioned EU bodies as well as any other EU institution involved in the transfer of surveillance capabilities to third countries carry out all (prior) human rights risk and impact assessment required in the context of transfer of surveillance capabilities to third countries.

Specifically, we ask the European Ombudsman to examine the present complaint and open an inquiry into whether the lack of (prior) human rights risk and impact assessments, including any privacy and data protection impact assessments, by the aforementioned bodies in the context of the transfer of surveillance capabilities to third countries constitutes maladministration under EU law.

Privacy International (PI)

Access Now

Border Violence Monitoring Network (BVMN)

Homo Digitalis (HD)

International Federation for Human Rights (FIDH)

Sea-Watch e.V.

19 October 2021

Table of annexes

Annex 1: Correspondence with EC 2019

Annex 1.1: PI Letter to EC 2020

Annex 1.2: EC Response 2020

Annex 2: PI Access to Documents Request (EUTF for Africa)

Annex 2.1: Document 7.7

Annex 2.2: Document 3.3

Annex 2.3: Document 7.6

Annex 2.4: EUTFA Response 2020

Annex 3: DG NEAR Request and Response 2019

Annex 3.1: Correspondence and Request to DG NEAR 2020

Annex 3.2: DG NEAR Response 2020

Annex 3.3: DG NEAR AD Belarus-Ukraine 2016

Annex 3.4: DG NEAR Moldova-Ukraine 2018

Annex 3.5: DG NEAR AD AAP Lebanon 2018

Annex 3.6: DG NEAR AD EUTF Libya

Annex 3.7: DG NEAR AD ENI BM Jordan

Annex 3.8: DG NEAR AD 2016 Security Package

Annex 4.1: EEAS Initial Response

Annex 4.2: EEAS Response to Confirmatory Application

Annex 4.3: EEAS (2017)189 Operational Guidelines on Legislative Drafting

Annex 5: Correspondence with DEVCO

Annex 5.1: DEVCO Response

Annex 5.2: Document 2.2 (Description of the Action)

Annex 5.3: Document 7 (Best Practice Guide on Personal Data Protection)

Annex 5.4: Document 3.6 (Executive Summary WAPIS Progress Report)

Annex 6: CEPOL Algeria

Annex 7: CEPOL Montenegro

Annex 8: CEPOL Morocco

Annex 9: CEPOL Bosnia and Herzegovina

Annex 10: CEPOL Tunisia

Annex 11: FRONTEX Training Programme Libya

Annex 11.1: FRONTEX ToR Libya

Annex 11.2: FRONTEX Bosnia and Herzegovina

Annex 11.3: FRONTEX Western Balkans