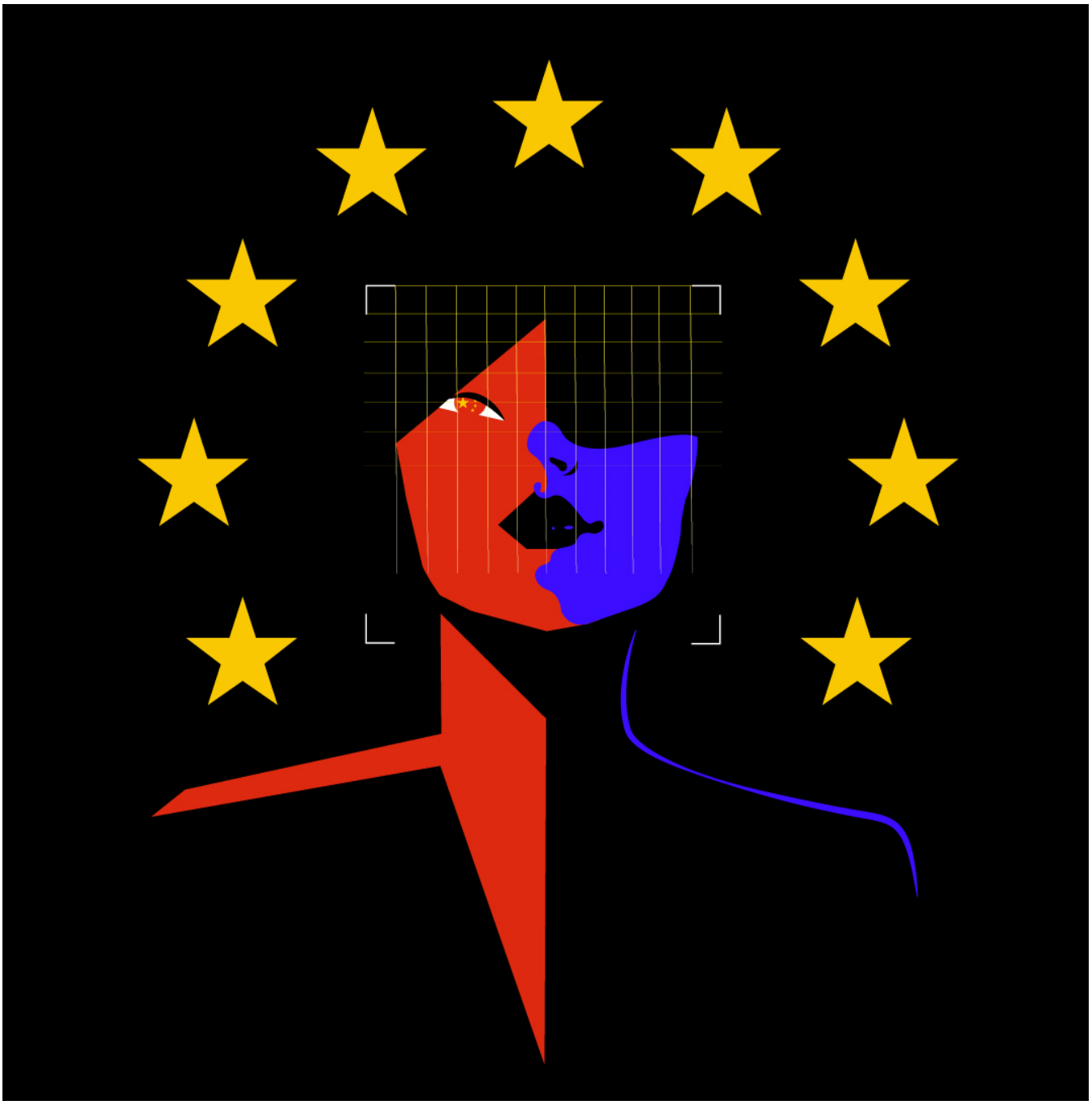

OUT OF CONTROL:

FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in 2020
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: EUR 01/2556/2020
Original language: English

amnesty.org

Cover photo: *A person with the colors of the EU and Chinese flags, standing behind facial recognition software.*
© Toscanabanana

AMNESTY INTERNATIONAL

CONTENTS

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

AMNESTY INTERNATIONAL

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

GLOSSARY

WORD	DESCRIPTION
BIOMETRIC SURVEILLANCE TECHNOLOGIES	Biometric technologies (or biometrics) use human characteristics for selection, identification, verification, and authentication processes. For example, biometrics make it possible to identify an individual in a public space, detect an individual's characteristics, such as wearing a headscarf or a beard, track their movements, and/or deny or approve their access to locations or services. Biometric data includes physiological and behavioural characteristics, ranging from face, gait, vein pattern, voice and DNA profiles. Biometric surveillance technologies also include ethnicity and emotion recognition software.
CONTROL LIST	The control list is the list of items that require export authorisation under the European export regulation framework and thus are 'controlled'. The list is included in Annexes to the EU Dual Use Regulation. Traditionally, the control list is formed by adding items that were put on the international control lists by the decisions under international non-proliferation regimes and export control arrangements. In the recast version of the export controls, the EU discusses the introduction of an EU control list, which controls items independently from decisions made at international forums.
DIGITAL SURVEILLANCE TECHNOLOGIES	Digital surveillance technologies are technologies, including hardware, software and services which are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies.
DUAL USE REGULATION	Dual Use Regulation refers to EU Regulation (EC) No. 428/2009 that governs the EU's export regulation regime for surveillance technology. This legislation includes a common set of export licensing criteria, a list of controlled items, mechanisms to prevent exports of non-listed items, and types of export authorisations.
EMERGENCY BRAKE PROCEDURE	Emergency brake procedure (or 'catch-all') is a mechanism under the European export regulation framework. This mechanism allows licensing authorities to control exports of items that are not (yet) listed on the control list but are nevertheless noncompliant with the export regulation framework.
FACIAL RECOGNITION TECHNOLOGY	Facial recognition technology is an umbrella term that is used to describe a suite of applications that perform a specific task using a human face to verify or identify an individual. FACIAL RECOGNITION SYSTEM is one of numerous biometric technologies being deployed by states and commercial entities across a wide range of use-cases.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

HUMAN RIGHTS DUE DILIGENCE	All companies have the responsibility to respect all human rights wherever they operate, including throughout their operations and supply chain. Human rights due diligence is a corporate, proactive and on-going process to identify, prevent, mitigate and account for the impacts of their operations on human rights. This process is established to fulfil the responsibility to respect human rights.
INDISCRIMINATE MASS SURVEILLANCE	Mass surveillance is the practice of monitoring an entire population, or a significant subset of it. Indiscriminate mass surveillance is conducted in the absence of adequate legal safeguards, without a reasonable suspicion, and without the consent of the individual under surveillance or a possibility to 'opt out'.
NON-LISTED DIGITAL SURVEILLANCE ITEMS	Non-listed digital surveillance items fall within the scope of the export regulation framework, but do not require authorisation for export as they are not listed on the control list. These items can be regulated through ad-hoc mechanisms that prevent exports of non-listed items (e.g. the 'emergency brake' procedure).
PREDICTIVE POLICING	Predictive policing refers to algorithmic models that use data to predict the likelihood that types of crime will happen at a certain location or will be committed by a certain individual, group or type of person or group. Some predictive policing tools use data collected by mass surveillance.
PROFILING	Profiling refers to the process of constructing and applying profiles about individuals generated by digital data analysis based on volunteered data, observed patterns in traits or characteristics (e.g. ethnicity) and inferred data. Profiling can lead to discrimination if individuals are being treated differently based on their profile.
TARGETED SURVEILLANCE	Targeted surveillance is the practice of selecting, monitoring and tracking selected individuals or particular groups within the population. Targeted surveillance may be deployed to target criminal suspects but may also be used unlawfully to target human rights defenders, journalists, political dissidents or individuals belonging to a religious minority or specific ethnicity.

ABBREVIATIONS

EU	European Union
FRT	Facial Recognition Technology
ICCPR	International Covenant on Civil and Political Rights
OHCHR	Office of the United Nations High Commissioner for Human Rights
UN	United Nations
UNGP	United Nations Guiding Principles on Businesses and Human Rights
UDHR	United Nations Universal Declaration on Human Rights
WA	Wassenaar Arrangement
XPCC	Xinjiang Production and Construction Corps, also known as *Bingtuan*

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

EXECUTIVE SUMMARY

This report gives evidence of the gaps in the current European Union (EU) export regulation framework for digital surveillance technologies and provides the EU institutions and its member states with actionable recommendations to improve the protections of human rights in the upcoming Recast Dual Use Regulation. Amnesty International investigated the exports of digital surveillance technologies from Europe to China, a country that (mis)uses its criminal law system to restrict human rights. China is also rapidly installing surveillance networks that are used for indiscriminate mass surveillance and use facial and ethnicity recognition software to discriminate against the Uyghur population.

Amnesty International's investigation revealed that three EU-based companies – Morpho (now Idemia) from France, Axis Communications from Sweden, and Noldus Information Technology from the Netherlands- exported digital surveillance tools to China. These technologies included facial and emotion recognition software, and are now used by Chinese public security bureaus, criminal law enforcement agencies, and/or government-related research institutes, including in the region of Xinjiang. None of the companies fulfilled their human rights due diligence responsibilities for these transactions, as prescribed by international human rights law. The exports pose significant risks to human rights. Amongst other risks, some of the technologies can eliminate the possibility for individuals to remain anonymous in public spaces, which interferes with the rights to privacy, non-discrimination, freedom of opinion and expression, and may impact the rights to assembly and association. Yet, the export of most digital surveillance technologies, including facial recognition, remains unregulated by the EU.

The current EU exports regulation (i.e. Dual Use Regulation) fails to address the rapidly changing surveillance dynamics and fails to mitigate emerging risks that are posed by new forms of digital surveillance technologies. For example, facial recognition technologies are not on the control list of the EU export regulation framework. These technologies can be exported freely to every buyer around the globe, including Chinese public security bureaus. The export regulation framework also does not obligate the exporting companies to conduct human rights due diligence, which is unacceptable considering the human rights risk associated with digital surveillance technologies.

The EU exports regulation framework needs fixing, and it needs it fast. At the time of publishing this report, the European legislature is in the legislative procedure to amend the exports regulation framework (i.e. Recast Dual Use Regulation). This is the window of opportunity that must be seized to establish a robust framework that respects, protects and promotes human rights. Amnesty International published this report to illustrate the gaps and to present six concrete proposals for change in the EU exports regulation framework.

Chapter 1, 'The Landscape of digital surveillance exports', defines digital surveillance technology as technologies, including hardware, software and services that are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies. Examples include surveillance network cameras, biometric technology, predictive policing tools, as well as malware, spyware, and other forms of interception technology. Governments around the world, including in China, are increasingly tapping into the resources of the private sector to acquire more advanced technologies, including biometric technologies to use for surveillance. Currently, Europe is the region with the second-highest revenue on the global biometrics market, and the second-largest provider of such technologies to governments

worldwide. These exports should be regulated, but currently they are not. The legislative changes that are proposed to bring the EU exports regulation framework in-line with human rights are being watered down by the governments of the Member States.

Chapter 2, 'The risks of digital surveillance technologies', explains why digital surveillance technologies pose a risk to human rights. The use of digital surveillance technology that enables the monitoring, tracking, classification, and identification of individuals is always in interference with the right to privacy. The use also poses a significant risk to the right to non-discrimination, freedom of opinion, expression and information, and the right to peaceful assembly and association when the technology facilitates profiling and targeting. Interferences with human rights, must be justifiable - conducted with a legitimate aim, necessary, and proportionate. Amnesty International considers that there cannot exist a reasonable justification to conduct mass surveillance, for mass surveillance can never be proportionate. Where the legal system provides insufficient safeguards to protect against human rights abuse, there is a risk that digital surveillance technologies may be misused.

Chapter 3, 'China: indiscriminate mass surveillance with discriminatory outcomes', discusses the use of surveillance technologies in China. The Chinese government uses large-scale surveillance networks that are rolled out nation-wide to keep its citizens under pervasive observation and control. Digital surveillance technologies, such as facial and ethnicity recognition systems are used to discriminate against and oppress the Uyghur population. The Skynet project (**天网工程**) and the Sharp Eyes project (**雪亮工程**) are two examples of indiscriminate mass surveillance initiatives in China that are increasingly implementing biometric technology. Chinese laws are facilitating unlawfullunlawful surveillance practices and contain a striking absence of human rights safeguards. National security measures and criminal law are (mis)used in China to restrict human rights.

Chapter 4, 'EU-based companies' digital surveillance exports to China', of this report shows that EU-based companies sold digital surveillance technology to the Chinese government, government-related institutions in the field of criminal enforcement and in some cases to end-users in Xinjiang. These are the French company Morpho (now Idemia) that provided facial recognition to the Shanghai Public Security Bureau, the Swedish company 'Axis Communications' that delivered surveillance cameras for the Skynet and Sharp Eyes projects, and the Dutch company 'Noldus Information Technology' that sold emotion recognition and behaviour analysis tools to various Chinese bodies, including the Chinese Ministry of Public Security. These exports pose a significant risk to human rights and should not have happened. Amnesty International's investigation reveals that none of the companies fulfilled their human rights due diligence responsibilities under international human rights law for the investigated transactions.

Chapter 5, 'How to include human rights safeguards in EU export regulation', we conclude based on the finding from Chapter 4 that the current European export regulation framework is failing to protect human rights. The following key recommendations to the EU legislature are detailed in that chapter:

1) **Define the scope of the Recast Dual Use Regulation in a technology-neutral manner in order to ensure that present and future digital surveillance technologies can be brought under it**. The following criteria should determine the definition of cyber-surveillance technologies. The technologies may consist of hardware, software and related services; could be used in connection with the violations of human rights or the commission of violations of human rights law or international humanitarian law; and are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies.

2) **Establish expeditious procedures to put new forms of digital surveillance items on the control list** that can be initiated by member states, a group of member states or the institutions of the European Union, without depending on surveillance companies for flagging the human rights risks. These procedures must allow for human rights risks to be addressed swiftly and efficiently as soon as a Member State or the EU institutions become aware of the risk.

3) **Include the obligation for licensing authorities that decide on an authorisation of exports of digital surveillance technologies to take into account the occurrence of domestic and international violations of human rights law,** fundamental freedoms and international humanitarian law in the country of final destination and/or by the end-user and/or if the legal framework in the destination country fails to provide

adequate safeguards against human rights abuses. An authorisation must be denied when a significant risk is identified that the exported item might be used in connection with human rights violations.

4) **Introduce obligations for companies to identify, prevent, mitigate and account for how they address the actual and potential impacts on human rights** associated with their operations, services and products, as well as the supply chain. The obligation to conduct human rights due diligence must apply equally to all exporting companies, regardless of their size, location or structure. Victims of human rights harm should have access to judicial remedy, followed by adequate sanctions. When a company has identified significant risks to human rights and was unable to mitigate those risks, companies must be obligated to refrain from export and notify the licensing authorities, regardless of whether the item in question is on the export control list or not.

5) **Establish an emergency brake procedure for anticipated exports of non-listed items that pose a significant risk to human rights**.

6) **Include the obligation for licensing authorities in the EU to publicly and regularly disclose the information on authorisation decisions**, including information on export volume and the nature, value and destination of the intended export of listed digital surveillance items for which an authorisation has been requested, and on authorisation processes of non-listed digital surveillance technologies under the emergency brake procedure.

The report closes with the conclusions and recommendations to the European legislature, EU member states and digital surveillance companies. Amnesty international included received reactions to the main findings of this report from the companies in the analysis. With this report, Amnesty International hopes to observe a positive outcome of the EU-level negotiations related to the modernization of the export controls. The European Union must take action to regulate the export of surveillance products from EU-based companies to third countries. It is time that the export regulation framework reflects the values and commitments of the European Union, specifically those of the promotion and protection of human rights worldwide. At the same time, Amnesty International urges companies to fulfil their human rights obligations prescribed by international standards, implement adequate mechanisms to mitigate risks of their products, services, and operations to rights and freedoms of people wherever in the world, and to refrain from engagement with actors in countries with poor human rights safeguards.

METHODOLOGY

Amnesty International used the following methodology for the investigation of this report.

First, Amnesty International conducted a legal review of the current EU export regulation framework and assessed its gaps in the protection of human rights. Next, Amnesty International assessed together with the members of the CAUSE coalition, including Human Rights Watch, Privacy International, Reporters without Borders and Access Now, what human rights safeguards will have to be added to the current framework. Amnesty International used this mapping as the base of the recommendations that are elaborated on in Chapter 5.

Secondly, Amnesty International made an extensive political analysis of the ongoing negotiations of the revision of the EU export regulation framework (the Recast Dual Use Regulation) and identified the key countries that oppose and the key ones that support the call for more human rights protection in the export regulation framework.

Thirdly, Amnesty International analysed industry reports, media articles, websites of digital surveillance companies and conferences to map the field of the emerging digital surveillance technology industry in the European Union. Next, Amnesty shortlisted EU companies based on previous media reporting, their own press releases or the nature of the technology that they produce, and their links with the key countries from the political analysis.

The focus on China has been picked, due to the Chinese advancements in implementing digital surveillance technology in society. The research for the human rights situation in China, is based on previous Amnesty research, media reporting and reporting by other human rights organisations.

Lastly, Amnesty International had access to databases that record data on public procurement procedures and tenders in China. Those databases were interrogated based on the company names and product names that were shortlisted. The results of this investigations were drawn up in preliminary findings that have been communicated with the companies through investigation letters. All companies provided Amnesty International with details on the transactions upon request at this or a later stage of the investigation. Based on all collected material, including the responses of the companies. Amnesty International assessed the risks of the business activities that were discovered in the public procurement databases. The findings relating to the business activities and the risks were shared with the companies and they were invited to respond to them. Where necessary these responses have been included in the results presented in Chapter 4. Amnesty International also engaged in a conversation with one of the named companies.

The investigation for this report was done between October 2019 and September 2020.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

1. THE LANDSCAPE OF DIGITAL SURVEILLANCE EXPORTS

1.1 THE DIGITAL SURVEILLANCE MARKET

Technological developments – such as artificial intelligence, big data, and biometrics – move digital surveillance into physical public spaces. Digital surveillance technologies are technologies, including hardware, software and services which are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies. Emerging digital surveillance technologies, such as facial recognition technology,[1] eliminate the possibility for individuals to remain anonymous in public spaces. These technologies facilitate the possibility for governments to identify and track individuals in public spaces, or single them out based on their physiological and/or behavioural characteristics, such as wearing a headscarf or being of a certain ethnicity. Biometric tools are amongst the most prominent digital surveillance technologies that fuel this trend. With the help of surveillance cameras, someone's unique face, vein or gait patterns can be recognised from a distance by biometric surveillance technologies. The use of these technologies in public spaces interferes with the right to privacy and can lead to automated discrimination.[2] China's mass surveillance programmes are at the forefront of these developments. Chinese Public Security Bureaus coordinate the collection of biometric data like 360-degree body and facial imagery from people. This happens, for example, in the Xinjiang Uyghur Autonomous Region (Xinjiang) where the Uyghur population and other ethnic groups are the target of a discriminatory comprehensive surveillance programme. Throughout China, networks of surveillance cameras pointed at public spaces are hooked up to video analysis systems, and technologies like facial recognition and ethnicity recognition are being used to conduct ubiquitous mass surveillance.

Governments around the world, including in China, are increasingly tapping into the resources of the private sector to acquire more advanced technologies to use for digital mass and/or targeted surveillance.[3] Despite that, there are hardly any controls on the export of digital surveillance technologies from companies based in the European Union (EU) to customers that are likely to use these technologies in connection with violations of international human

[1] Digital surveillance technologies, including hardware, software and services, are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyze data, including biometric surveillance technologies.
[2] 'Biometrics', https://privacyinternational.org/learning-topics/biometrics.
[3] Amnesty International, Digital Surveillance Threats for 2020, 15 January 2020, https://www.amnesty.org/en/latest/news/2020/01/digital-surveillance-threats-for-2020/; and Likhita Banerji, A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work, Amnesty International, 16 August 2019, https://www.amnesty.org/en/latest/research/2019/08/a-dangerous-alliance-governments-collaborate-with-surveillance-companies-to-shrink-the-space-for-human-rights-work/

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

rights law. Only a few types of digital surveillance items are subjected to export control, and human rights considerations play a dangerously small role in the authorisation processes. This is unacceptable under international human rights and EU law – even more so since the EU has committed itself to the promotion and protection of human rights worldwide[4] and the proposal for the new EU Action Plan for Human Rights and Democracy prioritizes the harnessing of opportunities and addressing of challenges that arise from new technologies.[5]

European companies that produce spyware and wiretapping tools, in law often referred to as intrusion and interception products, occupy a significant position on the global surveillance technologies market. The United Kingdom, France, and Germany are amongst the top five countries with the highest number of registered surveillance companies. These three countries together host approximately than 35% of the world's surveillance companies.[6] The significance and implications of Europe's position on the global surveillance market became evident during the Arab Spring. In 2011, countries in the Middle East and North Africa were engulfed in an unprecedented outburst of popular protests and demand for reform.[7] Some countries cracked down on protests with the use of digital surveillance technologies that were developed and exported by companies based in the EU.[8] Reports show that European companies have exported intrusion and interception technologies to Egypt, Libya, Syria, Ethiopia, Saudi Arabia, and other countries with poor human rights reputations.[9] In response, the EU and its member states put intrusion and interception technologies on the control list of the EU export regulation framework in 2014. However, since then the framework and the accompanying control list have failed to anticipate the growing EU biometric surveillance industry that is about to further arm governments with emerging surveillance tools around the world. European companies compete to be at the forefront of the biometric technologies market. Currently, Europe is the region with the second-highest revenue on the global biometrics market, and the second-largest provider of such technologies to governments worldwide.[10] This fast-developing industry is forecasted to experience at least five-fold growth up to EUR 54 billion by 2025 worldwide.[11]

1.2 LEGISLATIVE PROCESS OF EU EXPORT REGULATION

The European Commission stresses that "the gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights."[12] Despite this acknowledgment, biometric surveillance technologies are not on the control list of the EU export regulation framework, which in itself lacks important human rights safeguards. This has to change. Luckily, this change is within arm's reach. The EU export regulation framework is codified in the Dual Use

[4] The commitment of the EU to human rights is enshrined in the Treaty on European Union in the Preamble and Article 2: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities." The Treaty further stipulates in Article 3 (5) that the EU should uphold and promote the protection of human rights "in its relations with the wide world". Available at https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

[5] European Commission, Joint Communication to the European Parliament and the Council: EU Action Plan on Human Rights and Democracy 2020-2024, March 25, 2020, p. 4. https://ec.europa.eu/transparency/regdoc/rep/10101/2020/EN/JOIN-2020-5-F1-EN-MAIN-PART-1.PDF.

[6] The study identified 528 surveillance companies worldwide, of which 122 are headquartered in the United States, 104 in the United Kingdom, 45 in France, 41 in Germany, and 27 in Israel. Privacy International, The Global Surveillance Industry, July 2016, p. 18, www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

[7] Amnesty International, The 'Arab Spring': Five Years On, www.amnesty.org/en/latest/campaigns/2016/01/arab-spring-five-years-on/.

[8] Amnesty International, Ending the Targeted Digital Surveillance of Those Who Defend Our Rights: A Summary of the Impact of the Digital Surveillance Industry on Human Rights Defenders, 2019), pp. 12–14, www.amnesty.org/download/Documents/ACT3013852019ENGLISH.PDF; Ben Wagner, Exporting Censorship and Surveillance Technology, Humanist Institute for Co-Operation with Developing Countries (Hivos), January 2012; Privacy International, Open Season: Building Syria's Surveillance State, December 2016, privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf; Privacy International, The Global Surveillance Industry.

[9] Grayson Morris and Moore Erica, Security for Sale - The Price We Pay to Protect Europeans, The Correspondent, 4 September 2017, thecorrespondent.com/10221/security-for-sale-the-price-we-pay-to-protect-europeans/497732037-a3c8cc9e

[10] Grand View Research, Biometrics Technology Market Analysis Report By End-Use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), and Segment Forecasts, 2018 - 2025, September 2018.

[11] The baseline for the estimate is from year 2017. Originally indicated value for 2025 in USD: 59.31 billion. Grand View Research, Biometrics Technology Market Analysis Report.

[12] European Commission, White Paper on Artificial Intelligence - A European Approach to Excellence and Trust, 19 February 2020, pp. 21–22, ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Regulation, which is under revision at the time of writing this report.[13] The European export regulation framework consists of: a set of general rules that are applicable to all exports; a set of rules for selecting the types of items to be on the control list; the rules that should be applied to exports of controlled items; and the control list, which enumerates the items subject to export controls. At the start of the recasting process, the European Parliament and the European Commission recognised that human rights form an integral and fundamental part of the EU principles and that there is an obligation for the EU to uphold these values in the exports regulation framework.[14] They recognised the need to expand the control list to include emerging digital surveillance technologies and incorporate adequate human rights safeguards into the framework. However, the efforts of the European Parliament and the European Commission are being held back by the EU member states that are represented in the Council of the European Union. The Council of the EU is trying to water down the proposed and amended legal obligations on exporting companies and the licensing authorities to safeguard human rights.[15] While the opposing views were formed by the majority of the member states, Germany, Netherlands, Malta and Greece were among the few to support the efforts of the European Parliament and the Commission.[16] With the publication of this investigation, Amnesty International hopes to convince all member states and the EU legislators of the need for a strong and flexible export regulation framework. This report will illustrate why and how human rights must be secured in the EU export regulation framework.

[13] Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items (Council of the European Union, 5 May 2009), eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009R0428&from=GA.

[14] Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast) (European Commission, 28 September 2016), eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF; Amendments Adopted by the European Parliament on 17 January 2018 on the Proposal for a Regulation Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast) (European Parliament, 17 January 2018), www.europarl.europa.eu/doceo/document/TA-8-2018-0006_EN.html.

[15] In a joint letter to the Council, member states (e.g. Finland, Sweden, Italy, Ireland, and Poland) opposed due diligence obligations, considered transparency of licensing decisions to be "at own initiative or at a request", and blocked the discussion in the Council in regards an EU control list. Working Paper on the EU Export Control – Paper for Discussion For Adoption Of An Improved EU Export Control Regulation 428/2009 and For Cyber-Surveillance Controls Promoting Human Rights and International Humanitarian Law Globally (The Council of the European Union, 15 May 2018), www.euractiv.com/wp-content/uploads/sites/2/2018/06/nine-countries-paper-on-dual-use.pdf.

[16] Germany, initially together with France, presented several letters promoting the inclusion of e.g. the control list. The Netherlands, Malta and Greece were amongst the only member states to support the inclusion of the 'catch-all' provision. Daniel Moßbrucker, Surveillance exports: Federal Government puts industry before human rights, Netzpolitik.org, 29 October 2018, netzpolitik.org/2018/ueberwachungsexporte-bundesregierung-stellt-industrie-vor-menschenrechte/; Working Paper on the EU Export Control – Recast of Regulation 428/2009 (The Council of the European Union, 29 January 2018), www.euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf.

2. THE RISKS OF DIGITAL SURVEILLANCE TECHNOLOGIES

2.1 HUMAN RIGHTS AND DIGITAL SURVEILLANCE TECHNOLOGIES

At its core, surveillance – and by extension the use of digital surveillance technologies – interferes with the right to privacy.[17] This right is enshrined in Art. 12 of the United Nations Declaration on Human Rights (UDHR) and Art. 17 of the International Covenant on Civil and Political Rights (ICCPR). The majority of states are bound by these provisions, as they have ratified or signed the ICCPR and must thus at the very least refrain from acts that defeat the object and purpose of that treaty.[18] The scope of the right to privacy has always evolved in response to societal change, particularly to new technological developments. The United Nations High Commissioner for Human Rights explains that "[p]rivacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[19] This private sphere is not limited to private secluded spaces, such as a home, but extends to public spaces and information that is publicly available about individuals.[20] According to the United Nations High Commissioner for Human Rights: "[t]he right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby observing individuals."[21] In the digital environment, information that exists or can be derived about a person's life and the (automated) decisions based on that information, is of particular importance to the right to privacy.[22] The United Nations High Commissioner for Human Rights has also recognised that "even the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy,

[17] United Nations, International Covenant on Civil and Political Rights (ICCPR), December 16, 1966, art 17 and Universal Declaration of Human Rights (UDHR), 10 December 1948, art 12; UN Human Rights Council, United Nations Commissioner for Human Rights, The Right to Privacy in the Digital Age (A/HRC/27/37), 30 June 2014, para. 12 and 13.
[18] Vienna Convention on the Law of Treaties (1969), Article 18: "A State is obliged to refrain from acts which would defeat the object and purpose of a treaty when: (a) it has signed the treaty or has exchanged instruments constituting the treaty subject to ratification, acceptance or approval, until it shall have made its intention clear not to become a party to the treaty; or (b) it has expressed its consent to be bound by the treaty, pending the entry into force of the treaty and provided that such entry into force is not unduly delayed."
[19] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 5.
[20] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 6.
[21] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 6.
[22] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 5.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

as through those steps an individual loses some control over information that could put his or her privacy at risk."[23] When biometric surveillance tools are used, biometric data is being processed. This type of data is especially sensitive. The impact of the processing can be particularly grave when it is misused.[24]

Digital surveillance technologies are technologies, including hardware, software and services which are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies This group of technologies is diverse and includes for example spyware, communication interception systems, facial recognition systems and IP surveillance cameras. Amongst other uses, digital surveillance technologies make it possible to monitor, track, classify and identify individuals in public spaces. The right to privacy, as laid down in Art. 12 UDHR and Art. 17 of the ICCPR, comes into play when these technologies are used. Biometric digital surveillance technologies process biometric data; their use therefore falls under the ambit of Art. 12 UDHR and Art. 17 of the ICCPR.

Various digital surveillance tools include automated processes of decision-making that target a person based on volunteered data, observed patterns or characteristics (e.g. ethnicity), and inferred data (e.g. predictions based on behavioural analysis). This is the case with predictive policing tools, which make use of profiling and biometrics surveillance technologies. Using characteristics like ethnicity in the design of related algorithmic systems can easily lead to systematic discrimination. Differences in treatment are inconsistent with the right to equality and non-discrimination contained in Art. 26 of the ICCPR when the difference has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms on the basis of nationality, ethnicity or any other grounds in such a way that the treatment undermines rights.[25] Digital surveillance tools that make use of ethnicity recognition technology pose a significant risk of contributing to automated unlawful discrimination.[26]

The use of digital surveillance technologies can also lead to interference with the freedom of opinion, expression and information, and the right to peaceful assembly and association.[27] The threats to human rights from the uncontrolled export and use of digital surveillance technologies are becoming clearer every day: protesters in Russia, human rights defenders in Morocco and Pakistan, and journalists in Uzbekistan were intimidated and humiliated; they were forcibly disappeared and were physically detained after having been identified using video cameras, spyware, malware and other hacking attacks.[28] In other cases, digital surveillance has contributed to torture and extrajudicial killings.[29]

[23] UN, The Right to Privacy in the Digital Age (A/HRC/27/37), para. 20 and The Right to Privacy in the Digital Age (A/HRC/39/29), para. 7; See also Weber and Saravia v. Germany, No. 54934/00 (European Court of Human Rights, 29 June 2006), para. 78; Malone v United Kingdom, No. 8691/79 (European Court of Human Rights, 2 August 1984), para. 64.
[24] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 14; see also: Privacy International, Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism, June 2019, www.privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf
[25] UN, The Right to Privacy in the Digital Age (A/HRC/27/37), para. 36; UDHR, art. 7; and ICCPR, art. 26.
[26] See also UN, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Surveillance and Human Rights (A/HRC/41/35), 28 May 2019, para. 12.
[27] UN, The Right to Privacy in the Digital Age (A/HRC/27/37), para. 14.
[28] Amnesty International, Russia: Intrusive Facial Recognition Technology Must Not Be Used to Crackdown on Protests, 31 January 2020, www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/; Amnesty International, Moroccan Human Rights Defenders Targeted Using Malicious NSO Israeli Spyware, 10 October 2019, www.amnesty.org/en/latest/news/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/; Amnesty International, Uzbekistan: New Campaign of Phishing and Spyware Attacks Targeting Human Rights Defenders, 12 March 2020, www.amnesty.org/en/latest/news/2020/03/uzbekistan-new-campaign-of-phishing-and-spyware-attacks-targeting-human-rights-defenders/; and Human Rights Under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan, 2018, www.amnesty.org/download/Documents/ASA3383662018ENGLISH.PDF
[29] Banerji, A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work.

2.2 JUSTIFIABLE LIMITATIONS ON HUMAN RIGHTS

Any interference with the rights to privacy and freedom of expression must serve a legitimate aim and meet the standards of necessity, legality, and proportionality. National security is one of the legitimate aims which is frequently applied to the use of digital surveillance tools that lead to invasive curtailment of the enjoyment of human rights. The UN Special Rapporteur on the Freedom of Opinion and Expression explained that the concept of national security in relation to surveillance is "vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists, or activists."[30] National security as a legitimate aim does not coincide with the interests of the regime in power.[31] For it to be justifiable, the use of digital surveillance measures must be the least intrusive measure to achieve the legitimate aim. Surveillance can only be conducted in a manner that is both proportionate to that aim and non-discriminatory.[32]

The law that authorises surveillance must be sufficiently clear to provide an adequate indication of the conditions and circumstances under which the authorities are empowered to resort to the use of specific digital surveillance tools. Any restriction may not be unduly vague or overly broad such that it could confer unfettered discretion on officials.[33] Effective safeguards against abuse must also be set forth. Similar to intrusion and interception surveillance technology, other digital surveillance technologies are accompanied by extreme risks of abuse.[34] The UN Special Rapporteur on the Freedom of Opinion and Expression identified these types of tools as key surveillance technologies and practices and underlined the "comprehensive intrusiveness of these technologies".[35]

This means that its use should be authorised by a competent, independent, and impartial judicial body, with appropriate limits set for the duration, manner, place, and scope of the surveillance.[36] Safeguards may include strict data retention periods on the data that is collected and analysed with digital surveillance technologies, strict control of access to the data, and requirements for permanent deletion or destruction of the data after the retention period has passed.[37] In addition, these technologies and their use should also be subjected to detailed record-

keeping requirements.[38] Surveillance requests should only be permitted in accordance with regular, documented legal processes and the issuance of warrants for such use.[39] Individuals that have been under surveillance should be notified of the decision to authorise their surveillance as soon as such a notification would not seriously jeopardise the purpose of the surveillance.[40] The government should provide adequate safeguards to protect data against risks violating its integrity, confidentiality, availability and resilience.[41]

Surveillance that is conducted in the absence of adequate legal safeguards, without a reasonable suspicion, or without the consent of the individuals under surveillance or a possibility to 'opt out', amounts to indiscriminate mass surveillance.[42] Amnesty International considers that all indiscriminate mass surveillance fails to meet the test of necessity and proportionality and therefore violates international human rights law. The use of large-scale video

[30] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue (A/HRC/23/40), 17 April 2013, para. 60.
[31] UN, Promotion and Protection of the Right to Freedom of Opinion and Expression. Note by the Secretary-General (A/71/373), 6 September 2016, para. 18.
[32] UN. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. Surveillance and Human Rights (A/HRC/41/35), 28 May 2019, para. 25.
[33] UN Human Rights Committee, General Comment No. 34 on Article 19: Freedoms of Opinion and Expression (CCPR/C/GC/34), 12 September 2011, para. 25.
[34] See: UN, Resolution Adopted by the General Assembly (A/RES/73/179), 21 January 2019); and UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, 1 May 2017, para. 36.
[35] UN, Surveillance and Human Rights (A/HRC/41/35), para. 12.
[36] UN, Surveillance and Human Rights (A/HRC/41/35), para. 50(c).
[37] UN, Working Draft Legal Instrument on Government-Led Surveillance and Privacy. Including the Explanatory Memorandum. Ver 7.0, 28 February 2018, www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf art. 4(1)(l).
[38] UN, Surveillance and Human Rights (A/HRC/41/35), para. 50(d).
[39] UN, Surveillance and Human Rights (A/HRC/41/35), para. 50(d).
[40] Concluding Observations on the Sixth Periodic Report of Italy, para. 37.
[41] Working Draft Legal Instrument on Government-Led Surveillance and Privacy. Including the Explanatory Memorandum, art. 11(1).
[42] Plixavra Vogiatzoglou, Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity, European Journal of Law and Technology vol. 10, no. 1, 2019, ejlt.org/article/view/669/901.

surveillance networks that analyse the footage using facial recognition software amounts to indiscriminate mass surveillance.

Amnesty International calls for a ban of facial recognition technology

Facial recognition technology is an umbrella term that is used to describe biometric technologies that perform a specific task using a human face to verify or identify an individual. In the view of Amnesty International, facial recognition technology in all its forms violates the right to privacy of individuals and hampers the right to peaceful assembly, non-discrimination, and expression. It is a form of mass surveillance that poses a unique risk to human rights. Amnesty International calls for a ban on the use, development, production, sale, and *export* of all facial recognition technology systems by both state agencies and private sector actors - regardless of whether it is used *live* on video streams or used on previous recorded footage, such as photo's, videos or database comparison.

3. CHINA: INDISCRIMINATE MASS SURVEILLANCE WITH DISCRIMINATORY OUTCOMES

> **"…the [Chinese] authorities are also using a vast, secret system of advanced facial recognition technology to track and control the Uighurs, a largely Muslim minority. It is the first known example of a government intentionally using artificial intelligence for racial profiling…"**
>
> Paul Mozur, The New York Times, 14 April 2019

Chinese state mass surveillance efforts have been established and steadily modernised since the inauguration of the People's Republic of China in 1949.[43] Today, Chinese law enforcement agencies have integrated a wide range of advanced digital surveillance technologies, including biometric surveillance, to keep citizens under pervasive observation and control.[44] In this chapter, we observe the Chinese state of surveillance specifically in the Xinjiang region and more broadly throughout the country, we describe how Chinese laws are facilitating surveillance

[43] Katherine Atha et al., China's Smart Cities Development, SOS International LLC, January 2020, pp. 44–47, www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf.
[44] Human Rights Watch, China: Police 'Big Data' Systems Violate Privacy, Target Dissent, 19 November 2017, www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent; Kenneth Roth and Maya Wang, Data Leviathan: China's Burgeoning Surveillance State, The New York Review of Books, www.nybooks.com/daily/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state/; Willy Wo-Lap Lam, Beijing Harnesses Big Data & AI to Perfect the Police State, The Jamestown Foundation, July 21, 2017, jamestown.org/program/beijing-harnesses-big-data-ai-to-perfect-the-police-state/.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

practices and contain a striking absence of human rights safeguards, and underline how criminal law is (mis)used in China to restrict human rights.

3.1 XINJIANG AND THE UYGHUR POPULATION: CANARIES IN THE COAL MINE OF DIGITAL SURVEILLANCE

The use of digital surveillance technologies has been extensively documented in Xinjiang. This region in north-western China appears to be a 'living lab' for digital surveillance technologies.[45] In Xinjiang, Uyghurs and other ethnic groups are the chief target of a comprehensive population monitoring programme.[46] Biometric data on Xinjiang residents, including DNA samples, iris scans and facial imagery, is being collected and processed.[47] Biometric surveillance technologies like facial recognition and emotion recognition are being deployed to conduct ubiquitous surveillance.[48] The authorities have envisioned these surveillance systems as a series of "filters," picking out people with certain behaviour or characteristics that they believe indicate a threat.[49] These systems have furthermore enabled authorities to implement fine-grained control, subjecting people to differentiated restrictions depending on their perceived levels of "danger".[50]

It is estimated that up to one million Uyghurs and members of other ethnic groups have been held captive arbitrarily in so-called "re-education camps" in Xinjiang for reasons including public or private displays of religious and cultural affiliation.[51] The Uyghur people are also targeted by surveillance initiatives outside of Xinjiang. A recent report documents 12 government projects across China, including various video surveillance initiatives, which specifically require Uyghur analytics.[52] It allows state authorities to recognise the ethnicity of the Uyghurs and extensively monitor their lives throughout the country.[53] In 2019, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression warned against the discriminatory use of profiling techniques specifically targeting the Uyghur population in China.[54]

[45] Cate Cadell, From Laboratory in Far West, China's Surveillance State Spreads Quietly, Reuters, 14 August 2018, www.reuters.com/article/us-china-monitoring-insight-idUSKBN1KZ0R3; Zak Doffman, Why We Should Fear China's Emerging High-Tech Surveillance State, Forbes, 28 October 2018, www.forbes.com/sites/zakdoffman/2018/10/28/why-we-should-fear-chinas-emerging-high-tech-surveillance-state/#7f6032a94c36.
[46] Chris Buckley and Paul Mozur, How China Uses High-Tech Surveillance to Subdue Minorities, The New York Times, 22 May 2019, www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html; James Leibold, Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement, Journal of Contemporary China vol. 29, no. 121, 2 January 2020, pp. 46–60.
[47] Human Rights Watch, Eradicating Ideological Viruses: China's Campaign of Repression Against Xinjiang's Muslims, 9 September 2018, www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.
[48] Darren Byler, China's Hi-Tech War on Its Muslim Minority, The Guardian, 11 April 2019, www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition; Sue-Lin Wong and Qianer Liu, Emotion Recognition Is China's New Surveillance Craze, Financial Times, 1 November 2019, www.ft.com/content/68155560-fbd1-11e9-a354-36acbbb0d9b6.
[49] Human Rights Watch, Eradicating Ideological Viruses - China's Campaign of Repression Against Xinjiang's Muslims, 2018, www.hrw.org/sites/default/files/report_pdf/china0918_web2.pdf.
[50] Human Rights Watch, Eradicating Ideological Viruses - China's Campaign of Repression Against Xinjiang's Muslims, 2018, www.hrw.org/sites/default/files/report_pdf/china0918_web2.pdf.
[51] Amnesty International, China: "Where Are They?" Time For Answers About Mass Detentions In The Xinjiang Uighur Autonomous Region, 14 September 2018, p. 15, https://www.amnesty.org/download/Documents/ASA1791132018ENGLISH.PDF.
[52] The report unearthed draft central government guidelines requiring such analytics. Charles Rollet, China Government Spreads Uyghur Analytics Across China, IPVM, https://ipvm.com/reports/ethnicity-analytics.
[53] Paul Mozur, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, The New York Times, 14 April 2019, www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[54] UN, Surveillance and Human Rights (A/HRC/41/35), para. 12.

3.2 NATION-WIDE MASS SURVEILLANCE NETWORKS WITH BIOMETRIC SURVEILLANCE FEATURES

Mass surveillance efforts are not limited to the Xinjiang region or to the Uyghur people. Advanced digital surveillance technologies have become a central feature of Chinese state control efforts in all parts of the country.[55] With the assistance of private entities, Chinese officials have prioritized the use of surveillance technologies to keep people under non-stop observation, from megacities to tiny villages, thus facilitating greater government control.[56] 'Skynet' and 'Sharp Eyes' are two of the most prominent mass surveillance projects developed by the Chinese state. Launched by the central government, these initiatives are then rolled out by local governments, with Public Security Bureaus being some of the main actors in developing the Chinese state surveillance apparatus.[57] Both projects illustrate that gradual integration of biometrics is being encouraged by the Chinese central government.

The **Skynet project** (*tianwang gongcheng* **天网工程**) was, according to Chinese state media, launched by the central government in 2005.[58] The project involves the installation of cameras and video control centres for city management, crime and disaster prevention.[59] In 2017, Skynet reportedly had over 20 million cameras in use.[60] One year later, the Chinese state newspaper *Global Times* indicated that facial recognition constituted an essential part of Skynet and reported its application in 16 Chinese cities and provinces.[61]

The **Sharp Eyes project** (*xueliang gongcheng* **雪亮工程**) integrates public and private cameras into one large police network.[62] Since 2015, the Sharp Eyes project has connected existing public security camera networks that scan large public areas[63] with privately owned cameras, such as those installed at the entrances of residences and other buildings.[64] By 2020, the roll-out of the networked public security video surveillance is expected to be completed with "full coverage, network sharing, real-time availability, and full control".[65] The project purportedly has a rural focus, but in practice it extends beyond the countryside and is nation-wide in scope. According to the policies that underpin the project, local authorities that build the system are encouraged to integrate digital surveillance

[55] Qiang Xiao, The Road to Digital Unfreedom: President Xi's Surveillance State, Journal of Democracy vol. 30, no. 1, 2019; Josh Chin and Liza Lin, China's All-Seeing Surveillance State Is Reading Its Citizens' Faces, The Wall Street Journal, 26 June 2017, www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020.
[56] Amnesty International, Human Rights in Asia-Pacific: Review of 2019, 2020, p. 17, www.amnesty.org/download/Documents/ASA0113542020ENGLISH.PDF.
[57] The 2015 normative document inaugurating the Sharp Eyes project (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, sina.com, 13 May 2015, finance.sina.com.cn/roll/20150513/175522172766.shtml.
[58] Skynet was jointly launched by the Ministry of Public Security and the Ministry of Industry and Information Technology, known in 2005 as the Ministry of Information Industry. Zhang Zihan, Beijing's Guardian Angels?, Global Times, 10 October 2012, www.globaltimes.cn/content/737491.shtml.
[59] Zhang Zihan, Beijing's Guardian Angels?, Global Times, 10 October 2012, www.globaltimes.cn/content/737491.shtml.
[60] "天网"网什么, People's Weekly, 2017, paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm.
[61] Zhao Yusha, 'Sky Net' Tech Fast Enough to Scan Chinese Population in One Second: Report, Global Times, 25 March 2018, www.globaltimes.cn/content/1095176.shtml.
[62] Josh Rudolph, Sharper Eyes: Surveilling the Surveillers (Part 1), China Digital Times, 9 September 2019, chinadigitaltimes.net/2019/09/sharper-eyes-surveilling-the-surveillers-part-1/ referring to Simon Denyer, In China, Facial Recognition Is Sharp End of Big Data Drive for Total Surveillance, The Washington Post, 7 January 2018, www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.
[63] Sharp Eyes is thus often portrayed as an extension and upgrade of programs such as Skynet. Charles Rollet, China Public Video Surveillance Guide: From Skynet to Sharp Eyes, IPVM, ipvm.com/reports/sharpeyes. See also: Liu Xuanzun, Ubiquitous surveillance cameras in a Beijing district reduce crimes by nearly 40%, Global Times, 1 August, 2018, www.globaltimes.cn/content/1113386.shtml.
[64] Sharp Eyes was launched in 2015, following the promulgation of the normative document entitled 'Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance' by the Ministry of Public Security, the National Development and Reform Commission, and seven other ministries and commissions. Rudolph, Sharper Eyes: Surveilling the Surveillers (Part 1); The 2015 normative document inaugurating the Sharp Eyes project (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网.
[65] The 2015 normative document inaugurating the Sharp Eyes project, (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, para 3.

technologies, such as 'portrait comparison' (*renxiang bidui* 人像比对).[66] Hundreds of Sharp Eyes projects have been identified across China.[67]

3.3 SURVEILLANCE AND 'NATIONAL SECURITY'

According to internationally recognised human rights standards (discussed above in Chapter 2), any interference with the rights to privacy and the freedom of expression must serve a legitimate aim and meet the standards of necessity, legality, and proportionality. Both the Chinese legal framework and Chinese surveillance practices indicate that Chinese state surveillance does not meet these conditions.

In the Chinese context, it is important to distinguish the concepts of privacy from government actors and privacy from corporate actors. Whereas the rights to privacy and data protection for individuals / consumers in their relations with the private sector have increasingly received regulatory attention, China's current legal system does not afford significant privacy protection against government intrusion.[68] China's current regulatory framework does little to protect citizens' privacy against state surveillance. A recent comparative study on data privacy laws and government surveillance ranks China at the bottom on a list of 47 countries.[69]

Aspects of the right to privacy are mentioned in various Chinese legislative and normative documents, including the Constitution[70] and the Cyber Security Law.[71] These Chinese laws and normative documents invariably allow the state to interfere with the right to privacy in order to safeguard issues such as "national security".[72] In addition, Chinese laws contain numerous clauses instructing private entities to provide support and assistance to government agencies for national and public security purposes[73] This creates leeway for the Chinese authorities to request, use and integrate technology and personal data that is in the hands of private entities for surveillance purposes.

As indicated by the United Nations Special Rapporteur on Freedom of Expression, the concept of national security in relation to surveillance is vulnerable to manipulation by the State.[74] This is exactly what happens in China. Terms such as "national security" are cited prominently as main aims of state surveillance projects like Sharp Eyes. When

---

[66] The Chinese term used in the legislation (renxiang bidui 人像比对), translated here as 'portrait comparison', refers to the realisation of computerised automatic comparison and recognition of pictures or video containing full-body features. (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联, para 13; 唯庄,公安人像比对应用的建设与探索, ITS114.com, 5 July 2018, www.its114.com/html/itswiki/technology/2018_07_95253.html, p. 114.

[67] Josh Rudolph, Sharper Eyes: Shandong to Xinjiang (Part 3), China Digital Times, 13 September 2019, https://chinadigitaltimes.net/2019/09/sharper-eyes-shandong-to-xinjiang-part-3/

[68] Emmanuel Pernot-Leplay, China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?, Journal of Law & International Affairs vol. 49, 2020, https://elibrary.law.psu.edu/jlia/vol8/iss1/6, p. 107; Li, Tiffany, Jill Bronfman, and Zhou Zhou, Saving Face: Unfolding the Screen of Chinese Privacy Law, Journal of Law, Information, and Science, 2017, https://ssrn.com/abstract=2826087, p.14.

[69] Bischoff, Paul. Data Privacy Laws & Government Surveillance by Country. Comparitech, October 15, 2019. www.comparitech.com/blog/vpn-privacy/surveillance-states/.

[70] Most notably, article 40 of the Chinese Constitution mentions the freedom and privacy of correspondence of Chinese citizens. Available at: npcobserver.files.wordpress.com/2018/12/PRC-Constitution-2018.pdf

[71] The Cyber Security Law is currently the most comprehensive legislation regarding data protection in China. In a 2015 submission to the NPC Standing Committee's Legislative Affairs Commission on the draft Cyber Security Law, Amnesty International highlighted various privacy and other human rights concerns about the law: Amnesty International, China: Submission to the NPC Standing Committee's Legislative Affairs Commission on the Draft 'Cyber Security Law', 2015. The Cyber Security Law contains various clauses regarding the gathering and protection of personal information by network products, services and operators (see also articles 22, 40), available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Other documents of interest include the (non-binding) normative document National Standard of Information Security Technology – Personal Information Security Specification, available at: https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf; and the General Provisions of the Civil Law (art. 110), available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm. China furthermore adopted a Civil Code on 28 May 2020, which contains privacy legislation, available at: https://zh.wikisource.org/wiki/中华人民共和国民法典 . The Code will enter into force on 1 January 2021.

[72] Apart from safeguarding national security, the safeguarding of related issues such as public security, social public order and the public interest is often also mentioned as a legitimate aim to restrict human rights. See, for example, Article 40 of the Constitution; Article 58 of the Cybersecurity Law; Articles 5.4, 7.11 and 8.5 of the National Standard of Information Security Technology – Personal Information Security Specification; Article 1036(3) of the new Civil Code.

[73] Chinese National People's Congress, National Intelligence Law of the People's Republic (Adopted at the 28th Meeting of the Standing Committee of the 12th National People's Congress on 27 June 2017), 27 June 2017, art 7 & 14, cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf. See also: art. 28 of the Cybersecurity Law.

[74] UN, Report of the Special Rapporteur (A/HRC/23/40), para. 58.

conducting operations within the aims of national security, the Chinese state does not safeguard the right to privacy. These aims are undefined and overly broad, thus exposing them to manipulation by the state. Amnesty International has previously documented how the concept of national security forms the core of a legal infrastructure that progressively limits the exercise of freedom of expression, association, religion or belief, and other rights in China.[75] (see also Section 3.4.)

Chinese mass surveillance projects also fail to meet internationally recognised standards of necessity and proportionality.[76] The 2015 normative document inaugurating the Sharp Eyes project, entitled "Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance", can serve as a specific illustration.[77] It centrally features national security and social stability as justifications for the improvement of video surveillance and contains little mention of necessity or safeguards to ensure that surveillance is only used in line with the necessity principle.[78] The project is intended to establish "full coverage, network sharing, real-time availability, and full control",[79] and the 2015 normative document presents only general considerations of proportionality. The aim of "full coverage", for example, is broadly specified by indicating that "key public areas" and "important parts of key industries and fields" need to have 100% video surveillance coverage.[80] Concerning privacy, it merely contains exhortations to accelerate regulatory work on personal privacy protection,[81] which, as indicated above, is currently still inadequate and gives blanket authorisation to the State to interfere with the right to privacy for vaguely defined aims such as safeguarding national security.

Furthermore, there is a conspicuous absence of safeguards against abuse that should accompany the use of digital surveillance technologies (see Section 2.2.). The 2015 normative document indicates that state surveillance projects such as Sharp Eyes are not dependent on the authorisation of judicial bodies or the prior issuance of warrants, and they do not contain appropriate limitations on the duration, manner, place or scope of the surveillance. Instead of regulating strict access control to data gathered, the normative document emphasises the networking and sharing of data across different platforms and government departments.[82] While the Sharp Eyes project's inaugurating document mentions that regulatory work on personal privacy protection should be accelerated, today it is still apparent that privacy measures concern the processing of personal information by private parties and generally do not apply to state organs that process data in the interest of 'national security', 'public interest' or other vaguely defined constructs.[83]

---

[75] Amnesty International, China: Human Rights Violations in the Name of 'National Security', 1 March 2018, https://www.amnesty.org/en/documents/asa17/8373/2018/en/.

[76] Bischoff, Paul. Data Privacy Laws & Government Surveillance by Country. Comparitech, October 15, 2019. www.comparitech.com/blog/vpn-privacy/surveillance-states/.

[77] The 2015 normative document inauguring the Sharp Eyes project (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网.

[78] The only vague reference to this, is contained in paragraph 2, where the document mentions that "[all regions and departments should] promote the networking of public safety video surveillance systems and integrate various types of video image resources in accordance with the actual needs of maintaining national security and social public safety". (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, para 2.

[79] (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, para 3.

[80] (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, para 3.

[81] (trans. Several Opinions on Increasing Efforts to Establish and Network Public Security Video Surveillance) 关于加强公共安全视频监控建设联网, para 10.

[82] Various reports show that many of the state servers retaining wide-ranging personal data are unprotected and easy for anyone access. See e.g. Mozur, Paul, and Aaron Krolik. A Surveillance Net Blankets China's Cities, Giving Police Vast Powers, The New York Times, 17 December 2019. www.nytimes.com/2019/12/17/technology/china-surveillance.html.

[83] This harks back the above-described nature of the Chinese system, where privacy protection mainly concerns protection from private parties and not from government actors. Government actors are invariably allowed to interfere with privacy-related rights on the basis of vaguely defined concepts. The newly enacted Chinese Civil Code, which will enter into force on 1 January 2021, largely confirms this reality. It contains specific rules on (the processing of) personal information in arts. 1032 to 1039. While it notes in general terms that 'no organization or individual may infringe on the privacy rights of others' (art. 1032), and refers in general terms to the duties of 'information processors' (arts. 1037, 1038), its article 1039 seems to imply that state organs are only bound to protect confidentiality. It is the only article specifically referring to state organs in the Civil Code chapter on privacy and protection of personal information. Reiterating some but not all of the confidentiality provisions provided for all information processors in previous articles, article 1039 reads: "State organs, statutory bodies that undertake administrative functions, and their staff shall keep the privacy and personal information of natural persons learned in the course of performing their duties confidential, and shall not disclose or illegally provide it to others." In addition, article 1036(3) provides that in the processing of personal information, no civil liability shall be borne by any kind of perpetrator for acts "reasonably carried out in order to protect the public interest", thus leaving all private and public parties off the hook when it concerns matters of 'public interest'.

In the absence of adequate legal safeguards, Chinese surveillance practices and projects such as Skynet and Sharp Eyes are conducted without a reasonable suspicion, a possibility to 'opt out' or even the awareness of targeted individuals, amounting to indiscriminate mass surveillance. National security and related concepts are used to legitimise ubiquitous surveillance and control of large segments of the population, without adequate recourse. The fact that there is no legal or other adequate protection against the use and abuse of digital surveillance technologies for mass surveillance by the Chinese state is backed by numerous reports that show, amongst other things, how Chinese citizens who object to surveillance are intimidated or are told to fall in line because the expansion of surveillance infrastructure serves objectives of 'public security'.[84]

Within the Chinese surveillance domain, you see that data is collected through indiscriminate mass surveillance and is further processed to single out and track individuals belonging to ethnic minorities without a reasonable suspicion.[85] The use of facial and ethnicity recognition software facilitates automated and systematic discrimination. Ethnic minorities such as the Uyghur population are singled out by digital surveillance tools and treated differently throughout the country based on their ethnicity.[86] This violates the right to equality and non-discrimination and affects the rights to freedom of expression, association, religion or belief, and cultural life. Moreover, the use of surveillance in relation to arbitrary detentions raises concerns with the right to liberty.

China signed the ICCPR in 1998 and must, therefore, refrain from acts that defeat the object and purpose of the ICCPR.[87] The Chinese practices of targeted and mass surveillance interfere, however, with the right to privacy as protected by the ICCPR. Additionally, Chinese surveillance practices interfere with international human rights standards as laid out by the United Nations High Commissioner for Human Rights. Individuals are being monitored and identified; data about their private life is collected and analysed. This can easily lead to unsolicited interventions in their private life and abuse of other human rights.[88]

3.4 THE (MIS)USE OF CRIMINAL LAW TO RESTRICT HUMAN RIGHTS

The concept of 'national security' forms the core of a legal infrastructure that progressively limits the exercise of freedom of expression, association, religion or belief, and other rights in China.[89] The previous section highlighted the problematic use of national security and related concepts to legitimize ubiquitous surveillance and pervasive control of the Chinese population. This section focuses on the central space of these concepts within the Chinese criminal system and indicates how they are (mis)used to restrict a variety of human rights.

China has failed to bring its criminal law system in line with international laws and standards.[90] [91] Under international law and standards, laws criminalizing acts that endanger national security or public order must not, under any circumstances, be used to deter or punish individuals for the legitimate exercise of their human rights, including the freedom of expression, association, and peaceful assembly.[92] However, Chinese authorities have in practice frequently used precisely such crimes to punish individuals for exercising these rights. Instances include,

[84] Mozur, Paul, and Aaron Krolik. A Surveillance Net Blankets China's Cities, Giving Police Vast Powers, The New York Times, 17 December 2019. www.nytimes.com/2019/12/17/technology/china-surveillance.html; Li, Jane, Shanghai Apartment Buildings Are Secretly Installing Facial-Recognition Devices, Quartz, 18 October 2019, qz.com/1729799/shanghai-apartment-buildings-secretly-install-facial-recognition/.
[85] Human Rights Watch, China: Police 'Big Data' Systems Violate Privacy, Target Dissent. https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent.
[86] UN, Surveillance and Human Rights (A/HRC/41/35), para. 12.
[87] China has not yet ratified the ICCPR. For more information, see: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en#4.
[88] UN, The Right to Privacy in the Digital Age (A/HRC/39/29), para. 5.
[89] Amnesty International, China: Human Rights Violations in the Name of 'National Security', 1 March 2018, p. 5. https://www.amnesty.org/en/documents/asa17/8373/2018/en/.
[90] Amnesty International, Briefing on China's 2013 Criminal Procedure Law: In Line with International Standards?, 2013, https://www.amnesty.org/download/Documents/12000/asa170212013en.pdf.
[91] Amnesty International, Submission to the NPC Standing Committee's Legislative Affairs Commission on the Criminal Law Amendments (9) (Second Draft), 2015, https://www.amnesty.org/download/Documents/ASA1722052015ENGLISH.pdf
[92] Amnesty International, Submission to the NPC Standing Committee's Legislative Affairs Commission on the Criminal Law Amendments (9) (Second Draft), 2015, https://www.amnesty.org/download/Documents/ASA1722052015ENGLISH.pdf, p. 7 a.f. referring to, among others, the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1995).

among many others, using charges of 'separatism' to suppress freedom of expression;[93] and using charges of 'inciting subversion of state power' to target human rights lawyers[94] and suppress freedom of expression.[95]

The (mis)use of 'national security' and related concepts to quash the legitimate exercise of human rights including freedom of expression has been a hallmark of the Chinese criminal system for decades,[96] and remains so up till this day. A particular case in point is the use of vague and overly broad charges related to 'terrorism' and 'extremism'. In December 2001, China amended the criminal law with the purpose of making more explicit the measures it already contained to punish 'terrorist' crimes, yet left the concept largely open to interpretation.[97] This did not change in further legislation including the Anti-Terrorism Law (passed in 2015), which "has virtually no safeguards to prevent those who peacefully practice their religion or simply criticize government policies from being persecuted on vague and overbroad charges related to 'terrorism' or 'extremism'".[98]

In sum, Chinese laws exploit concepts such as 'national security' and 'terrorism' to provide broad discretionary powers to authorities to conduct mass and targeted surveillance and restrict the exercise of freedom of speech, religion, and assembly. The rise of digital surveillance technology, and more specifically of biometrics, has been an important development within this Chinese reality.

USE OF BIOMETRIC TECHNOLOGY IN CRIMINAL LAW ENFORCEMENT

Facial recognition technology and other biometric technologies are being used by states around the world as a tool of surveillance to identify and monitor people. Law enforcement agencies may have privileged access to a wealth of people's sensitive personal data; they also have authority to detain, pursue criminal charges and use force. Biometric technologies have the capacity to hugely influence decision-making in law enforcement. Additionally, these technologies pose a danger of implementing biased algorithmic decisions, disproportionately affecting certain groups in society. Deference to biometric systems in law enforcement is, therefore, highly problematic.

[93] Amnesty International, Five facts about Ilham Tohti, award-winning activist jailed in China, 20 October 2016, https://www.amnesty.org/en/latest/campaigns/2016/10/five-facts-about-ilham-tohti-uighur-activist-jailed-in-china/
[94] Amnesty International, Third Anniversary of the lawyers crackdown in China: Where are the human rights lawyers?, 9 July 2018, https://www.amnesty.org/en/latest/campaigns/2018/07/china-human-rights-lawyers-crackdown-third-anniversary/.
[95] Amnesty International, China: Free human rights activist jailed after unfair trial, 9 February 2010, https://www.amnesty.org/en/press-releases/2010/02/china-free-human-rights-activist-jailed-after-unfair-trial-20100209/
[96] As documented for example in a 1995 Amnesty report, which lists the use of vague "state secrets" charges to curtail the legitimate exercise of people's right to freedom of expression. Amnesty International, Women in China: Imprisoned and abused for dissent, 27 June 1995, https://www.amnesty.org/download/Documents/172000/asa170291995en.pdf
[97] Amnesty International, People's Republic of China: China's Anti-Terrorism Legislation and Repression in the Xinjiang Uighur Autonomous Region, March 2002, https://www.amnesty.org/download/Documents/116000/asa170102002en.pdf
[98] Amnesty International, China: Submission to the United Nations Committee on the Elimination of Racial Discrimination 96th Session, 6-30 August 2018, July 2018, https://www.amnesty.org/download/Documents/ASA1787422018ENGLISH.pdf, p.3.

4. EU-BASED COMPANIES' DIGITAL SURVEILLANCE EXPORTS TO CHINA

China's problematic state surveillance efforts have been nurtured and sustained by the EU industry of digital surveillance technology. Amnesty International chose to focus on a limited set of cases involving transactions with Chinese government(-related) entities, as these clearly point to high risks for human rights. This does not mean however that transactions with Chinese private companies are without human rights risks.

Amnesty International found evidence implicating three different companies – Morpho (now Idemia), Axis Communications, and Noldus Information Technology - based in three different EU member states - France, Sweden, and the Netherlands - that exported digital surveillance technology to China. The recipients of these technologies were Chinese Public Security Bureaus and other entities that contribute to the Chinese surveillance domain, including law enforcement agencies and research institutions. These three cases represent smaller companies that sell digital surveillance technology ranging from network cameras to facial recognition and behavioural analytics software.

Exports described in this chapter have occurred despite the ongoing indiscriminate mass surveillance practices in China, incompliant with international human rights laws and standards. The exports of exposed digital surveillance technologies are currently not covered by the export regulation frameworks of neither the EU nor the EU member states. However, this does not release the exporting companies from their responsibilities under international human rights standards - that is the obligation to protect and mitigate the impacts of their products to human rights.

All businesses have the responsibility to respect human rights, as set out in the UN Guiding Principles on Business and Human Rights (UNGPs).[99] As part of fulfilling this responsibility, companies must, amongst other activities, carry out human rights' due diligence on an ongoing basis in order to address the actual and potential human rights impacts of their products, services, operations and of business partners in the supply chain.[100] This process requires companies to identify human rights risks related to their operations, take effective action to prevent and mitigate against them, and be transparent about their efforts in this regard. In the context of exports, the process should at its core establish a verifiable review of laws, regulations and practices in the country of destination and of credible reports as to whether the end-user "engages in the use or misuse of surveillance capabilities to conduct

[99] UN, Guiding Principles on Business and Human Rights (UNGP), 2011, pp. 14–15, www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[100] See the OECD Due Diligence Guidance for Responsible Business Conduct, 2018, mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

human rights abuses", and then take appropriate action – including restricting sales of surveillance technologies in contexts that pose a high risk to human rights.[101]

Amnesty International chose to investigate the exports from Europe to China due to the ongoing nation-wide surveillance practices, specifically Skynet and Sharp Eyes projects, and resulting human rights violations (see chapter 3). The involvement in Chinese surveillance projects of EU-based companies selling surveillance technologies at the outset indicates a high risk to human rights. Amnesty International chose to focus on a limited set of cases and did not pursue all leads. Our findings are presented in the sections below.

4.1 FRENCH FACIAL RECOGNITION SYSTEMS SOLD TO THE SHANGHAI PUBLIC SECURITY BUREAU

Idemia is a French multinational company specialising in security and identity solutions, including facial recognition systems and other biometric identification services.[102] Idemia is the result of the merger of Oberthur Technologies (OT) and Safran Identity & Security (Morpho) on 31 May 2017.[103] Variations on the names of the merging parent companies are still used for subsidiaries of Idemia. For example, Idemia holds 100% of the shareholder rights in a Shanghai-based subsidiary named Morpho Security System (Shanghai) Co. Ltd.

A 2015 public procurement document[104] (of which a copy is in the possession of Amnesty International) reveals that Morpho (now Idemia) supplied automatic facial recognition equipment directly to the Shanghai Public Security Bureau. The procurement document concerns a winning bid result announcement. Idemia confirmed this business activity when confronted with the findings of this report.[105] When asked by Amnesty International about this transaction, Idemia explained that the product is a *post*-event facial recognition system, meaning a system that identifies faces that appear on recorded footage instead of a *live* identification feed. Idemia explains that the software is "aimed at helping the police investigators for criminal case analysis after the offence took place (i.e. burglary, criminal offences etc.)."[106]

The above mentioned sale poses a particularly significant risk to human rights. It concerns a product with an inherent violation of human rights (facial recognition technology); it concerns a sale for an end-use with significant human rights risks. Amnesty International urges companies not to sell facial recognition technology to law enforcement authorities, post-event or live. On top of this, the end-user is based in a country with lacking human rights safeguards (China); and it concerns a sale to an end-user with a significant risk of adverse impact on human rights (Shanghai Public Security Bureau). Public Security Bureaus are prominent actors within Chinese law enforcement[107] and occupy a prominent role in the development and deployment of the Chinese state surveillance apparatus (see Section 3.2).

In communication with Amnesty International, Idemia did not provide evidence that the company had undertaken human rights due diligence to assess the risks associated with the export of its facial recognition system.[108] In this respect, Morpho (now Idemia) failed to fulfil its obligation under UNGP to identify human rights risks related to their operations, take effective action to prevent and mitigate them.

---

[101] York, Jillian C. and Cohn, Cindy, 'Know Your Customer' Standards for Sales of Surveillance Equipment, Electronic Frontier Foundation, 24 October 2011, www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment.
[102] 'Our Journey,' Idemia, accessed 28 May 2020, https://www.idemia.com/our-journey.
[103] After the merger, the company was initially named OT-Morpho, and then renamed Idemia on 28 September 2017. "OT–Morpho Becomes IDEMIA, the Global Leader in Trusted Identities," IDEMIA, accessed 28 May 2020, https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.
[104] The document is entitled "(trans. Automatic Facial Recognition System Equipment Winning Bid Result) 人脸自动识别系统装备中标结果" and is dated 24/03/2015. It lists the Shanghai Public Security Bureau as the tender owner and purchasing party, and Morpho Security System (Shanghai) Co. Ltd. as the successful bidder.
[105] Response of Idemia to a letter of Amnesty International. Dated 19 June 2020.
[106] Response of Idemia to a letter of Amnesty International. Dated 19 June 2020.
[107] Scoggins, Suzanne E. "Policing Modern China." China Law and Society Review 3.2 (2018): 79-117.
[108] Response of Idemia to a letter of Amnesty International. Dated 19 June 2020.

Notably, after the merger of Oberthur Technologies and Safran Identity & Security (Morpho) in 2017, that is two years after the mentioned transaction, Idemia enforced a policy of not selling identification systems to Chinese authorities. Idemia explains that this policy reflects "our concerns as to *inter alia* the protection of our technology and the use that Chinese authorities could make of our systems."[109] In its response, Idemia refers to its 2019 Corporate Social Responsibility Report to illustrate its current commitment to promoting and embedding corporate social responsibility throughout its sphere of influence.[110] The evidence provided by the company shows that in the last four years, the company has identified human rights risks associated with exports of surveillance technology to China and is conducting transparent reporting of its processes. Amnesty International applauds this change in policy. Amnesty International encourages companies, including Idemia, to continue transparently reporting on their human rights due diligence procedures and activities.

4.2 SWEDISH SURVEILLANCE CAMERAS IN CHINESE INDISCRIMINATE MASS SURVEILLANCE NETWORKS

Axis Communications is a company headquartered in Lund, Sweden.[111] It develops and markets network cameras, with a focus on applications in security surveillance and remote monitoring.[112] Axis Communications lists two sales companies in China:[113] one in Shanghai,[114] of which the European parent company owns 100% of the shares,[115] and one in Beijing,[116] which is a subsidiary of the Shanghai office. Axis Communications is repeatedly listed as a 'recommended brand' or a 'compatible third-party brand' in Chinese state surveillance procurement calls and inquiries dating from 2012 to 2019 of which Amnesty International holds copies.[117] As set out below, multiple sources point out that Axis Communications' products are actively being used in Chinese indiscriminate mass surveillance projects, including Skynet and Sharp Eyes projects.

The first transaction refers to the supply of Axis Communications' technology to the Skynet Upgrading and Reconstruction Project in Guilin, a city in the south of China.[118] This transaction is described by the company under customer stories on its website.[119] The company reveals that it provided cameras to the Guilin Municipal Public Security Bureau to expand the "Social Management Video Surveillance System Construction Programme 2012".[120] The 2013 customer story indicates that the network of 8 000 previously installed cameras was to be expanded to 30 000 cameras within one year. The cameras in the network have a 360-degree angle and a range of 300 to 400

[109] Response of Idemia to a letter of Amnesty International. Dated 19 June 2020.
[110] Idemia Corporate Responsibility Report January – December 2019, https://www.idemia.com/sites/corporate/files/2020-05/idemia-csr-report-202005.pdf.
[111] Axis Communications is part of Canon Inc. Axis Communications has its own identity and operates from Sweden.
[112] Axis Communications is considered a pioneer in network video surveillance and has been credited with bringing IP cameras into traditional analogue security. Security News Desk, IP Security Camera and Network Video Surveillance Visionary, 29 September 2016, securitynewsdesk.com/ip-security-camera-and-network-video-surveillance-visionary/.
[113] 'Contact Us', Axis Communications, accessed 28 May 2020, https://www.axis.com/en-us/contact-us?/corporate/contact.htm?countryId=cn.
[114] The official name of the Shanghai branch is Shanghai Axis Communications Equipment Trading Co., Ltd. (上海安讯士网络通讯设备贸易有限公司).
[115] The shareholder is the European parent company Axis Communications (安讯士网络通讯有限公司).
[116] The official name of the Beijing branch is Beijing Axis Communications (安讯士北京分公司).
[117] These include, among others, the following documents: "(trans. Tender Announcement for the Construction of a Video Surveillance System) 视频监控系统建设招标公告", dated 14/08/2012, administered by the bidding agent Hefei Bidding Center for the project "Hefei Construction of a Video Surveillance System" (indicated to be a part of the Skynet Project), listing Axis as a recommended brand; "(trans. Xiaji Town Social Order Technology System Integration Project Tender Announcement) 夏集镇社会治安技术系统集成项目招标公告", dated 22/09/2016, administered by the bidding agent Jiangsu Huicheng Investment Consulting Management Co., Ltd. for the People's Government of Xiaji Town, Baoying County (tender owner), listing Axis as a recommended brand; "(trans. Shimen County Xinguan Town Sharp Eyes Project Material Procurement - Online Bidding (Transaction) Announcement) 石门县新关镇雪亮工程物资采购-网上竞价（成交）公告", dated 22/03/2019, listing the People's Government of Xinguan Town, Shimen County as the purchaser and Hunan Qunsi Information Technology Co., Ltd. as the successful bidder, listing Axis as a compatible third brand.
[118] The project is the expansion of the Guilin Police Bureau's "Social Management Video Surveillance System Construction Programme 2012". "High-Definition, Intelligent 'Sky Net' Enhances City's Quality of Life. Axis Helps to Build HDTV Video Surveillance System in Guilin, Guangxi, China." (Axis Communications, 2013).
[119] 'Customer Stories', Axis Communications, accessed 28 May 2020, https://www.axis.com/customer-story/2901.
[120] Models of supplied cameras: Q1602 and Q1604.

metres, making it possible to track targets from all directions. The company further explains that cameras improved the surveillance capacities of the Skynet project by providing better video footage.[121]

Public procurement documents[122] of which Amnesty International has copies show that Axis Communications' involvement in the Skynet projects in Guilin goes beyond this one transaction. The second case reported by Amnesty International relates to Axis Communications' technology listed in 2015 and 2018 tender awards for equipment for Skynet projects of the Lingchuan County Public Security Bureau (under the administration of the Guilin city). [123] The tenders were won by a local Chinese entity,[124] and involved a subsequent purchase of Axis Communications' equipment, including cameras, [125] through that local company.

The third transaction reveals that Axis Communications' cameras have also been purchased by the Shanghai Public Security Bureau, much like the facial recognition system sold by Morpho (now Idemia). A document from 2018[126] lists a tender issued by the Huangpu Branch of the Shanghai Public Security Bureau, won by a local company[127] that acted as a reseller/redistributor and involving the purchase of Axis Communications' cameras for the use in the Sharp Eyes project. Axis Communications confirmed to Amnesty International that in the period from 2018 to 2020 the company has been part of the city surveillance projects in Shanghai.[128]

The fourth transaction refers to Axis Communications' surveillance cameras[129] sold to the Jingjiang Public Security Bureau for the '3.20' anti-crime campaign.[130] The 3.20 anti-crime campaign is a mass surveillance project which expanded an already extensive surveillance camera network and connected the footage to data obtained through criminal investigations, traffic management, and patrolling processes.[131] The system is focused on public spaces and roads and facilitates the "capturing of human images, recording of vehicle numbers, logging of phone information, detection of regulation violations, obtaining of crime evidences, and tracking of trajectories".[132] This data is then shared and analysed in ways that incorporate behaviour analysis.[133] This mass surveillance project is an example of ways in which cameras and biometrics are deployed in public spaces and incorporated into the enforcement of broadly defined 'criminal offences' (see Section 3.4).

As shown in the aforementioned transactions of Axis Communications, surveillance cameras were among the exported products. Amnesty International notes that the export of surveillance cameras does not inherently pose a significant risk to human rights.[134] There may be legitimate cases in which such tools are implemented without inflicting harm. However, where surveillance cameras are used by law enforcement agencies in relation with mass

---

[121] High-Definition, Intelligent 'Sky Net' Enhances City's Quality of Life. Axis Helps to Build HDTV Video Surveillance System in Guilin, Guangxi, China.

[122] It concerns the following 2 documents: "(trans. Guangxi Jianxin Construction Project Management Co., Ltd. regarding the Lingchuan County High-definition Skynet System, High-definition Bayonet System Equipment Procurement [GXJXZCLC2015-18 (Double)] Winning Bid Announcement) 广西建信建设项目管理有限公司关于灵川县高清天网系统、高清卡口系统设备采购【GXJXZCLC2015-18(重)】中标公告", dated 21/08/2015, listing the Lingchuan County Public Security Bureau as the tender owner, and Guangxi Kaiyale Network Technology Co., Ltd. as the successful bidder; "(trans. Guangxi Jianye Zhongtian Engineering Consulting Co., Ltd. regarding the "Skynet Phase III" and Bali Street "Skynet Phase III" video surveillance large-screen procurement [Project Number: JYZTGL2018-G1-220 (double)] Winning Bid Announcement) 广西建业中天工程咨询有限公司关于"天网三期" 及八里街"天网三期"视屏侦控大屏采购【项目编号：JYZTGL2018-G1-220(重)】中标公告", dated 18/10/2018, listing the Lingchuan County Public Security Bureau as the tender owner and purchasing party, and Guangxi Kaiyale Network Technology Co., Ltd. as the successful bidder.

[123] Amnesty International found transactions in 2015 and 2018 in Lingchuan County. See footnote above. These business instances were not confirmed by Axis Communications, who indicates that it only provided products for a city surveillance project in Lingui County in 2015 – Amnesty International does not possess public procurement documents relating to the Lingui business activities.

[124] In both tenders, this was Guangxi Kaiyale Network Technology Co., Ltd. (广西凯雅乐网络科技有限公司)

[125] Models of Q6045-E MKII and Q1635 of Axis Communications in 2015; model Q6045-E MKII of Axis Communications in 2018.

[126] "(trans. Winning Bid Announcement: Shanghai Public Security Bureau Huangpu Branch Winning Bid Announcement on the Construction and Application of the Public Security Video Networking of the First Phase of the 2018 Sharp Eyes Project) 中标公告：上海市公安局黄浦分局 2018 年雪亮工程一期公共安全视频联网建设及应用的中标公告", dated 31/10/2018, listing the Huangpu Branch of the Shanghai Public Security Bureau as the tender owner and purchasing party, and Strong Digital Technology Co. Ltd. as the successful bidder.

[127] The Chinese firm Strong Digital Technology Co. Ltd. (思创数码科技股份有限公司)

[128] Response of Axis to a letter of Amnesty International. Dated 13 May 2020. In the letter, the company also revealed to be part of a city surveillance project in Wuhan. Amnesty International did not further investigate this.

[129] Models P1343 and Q1604 of Axis Communications.

[130] A Safer Jingjiang City Helped by Axis Communications, Axis Communications, accessed 28 May 2020, www.axis.com/customer-story/2790.

[131] A Safer Jingjiang City Helped by Axis Communications, Axis Communications.

[132] A Safer Jingjiang City Helped by Axis Communications, Axis Communications.

[133] A Safer Jingjiang City Helped by Axis Communications, Axis Communications.

[134] Case of Peck v. the United Kingdom (application no. 44647/98), European Court of Human Rights, 28 January 2003, para 59.

surveillance projects or in countries incompliant with international human rights law - there is an actual risk that the right to privacy is violated without justification under international human rights (see Section 2.2).

Axis Communications traded with Chinese Public Security Bureaus on multiple occasions. Its sales had a direct impact on the surveillance projects Skynet, Sharp Eyes, and the '3.20' anti-crime campaign. These projects amount to mass surveillance because of their widespread and indiscriminate application and a lack of adequate human rights safeguards in the Chinese legal system. In a system without safeguards, data collected through surveillance cameras is analysed without there being a reasonable suspicion against passers-by, or individuals having an option to consent or 'opt out' from the surveillance. Exports of surveillance equipment, like the cameras, to Chinese Public Security Bureaus for indiscriminate mass surveillance as an end-use pose a significant risk to human rights.

In response to the findings in this report, Axis Communications explains that at the time of the business operations they had no information their products would be used for large-scale surveillance. Amnesty International confronted Axis Communications with the fact that the company must at some point have known about the end-use and end-users, since on the company's website Axis Communications advertises its products with costumer stories involving Chinese Public Security Bureaus as end-users and Chinese mass surveillance projects as end-use. Axis Communications replied: "It's correct that some of the projects you refer to were described as a "customer stories" on our website. When Axis took part in those projects, we had no information from our customers indicating that our products would be used for purposes that could risk violating human rights."[135] Axis Communications screens the end-users of large-scale orders when the end-user is known to Axis Communications to ensure that their products are used in accordance with Axis' intentions.[136] End-users can differ from customers when a company uses re-sellers for the distribution of their products, which is the case for some of the business operations of Axis Communications. The company screens its customers and Axis Communications has "close dialogue with customers to detect any risk of [their] products being used in a non-intended way."[137] Since 2018 the company deploys an "automatic screening process of Axis partners as well as of end-users that are known to Axis (which is the case in most larger projects)."[138]

Amnesty International would like to make three clarifications in regard to the response from Axis Communications to the investigation results. Firstly, the company brings forward examples of legal compliance to illustrate how the company fulfils its human rights due diligence responsibilities. Axis Communications refers to compliance with exports control and UN sanctions and restrictions in relation to the end-user.[139] However, legal compliance is different from human rights due diligence that requires companies to address the actual and potential human rights impacts of their products, services, operations, and of business partners in the supply chain. Legal compliance cannot substitute for a *human rights impact assessment*. Secondly, when it comes to the screening of costumers and end-users, we learn that Axis Communications heavily relies on the information that they receive from their customers.[140] The company was unable to demonstrate what other methods the company used to investigate the impact of their business operations and the potential human rights impact of business partners in the supply chain.[141] Thirdly, Axis Communications mentions that it "clearly communicates" with buyers and resellers the need to use products "in accordance with [Axis'] intentions".[142] Communicating intentions and engaging in dialogue with end-users and/or resellers are inadequate measures to prevent and mitigate the potential human rights impacts in a context where there is a significant risk to human rights. What is more, the size and structure of business operations does not excuse businesses from their human rights responsibilities[143] Therefore,

[135] Response of Axis to a letter of Amnesty International. Dated 13 May 2020.
[136] Response of Axis to a letter of Amnesty International. Dated 23 June 2020.
[137] Response of Axis to a letter of Amnesty International. Dated 23 June 2020.
[138] Response of Axis to a letter of Amnesty International. Dated 23 June 2020.
[139] Response of Axis to a letter of Amnesty International. Dated 23 June 2020; and Response of Axis to a letter of Amnesty International. Dated 13 May 2020.
[140] Response of Axis to a letter of Amnesty International. Dated 23 June 2020.
[141] Supply chain responsibility is recognized by Axis Communications for other aspects of their business operations relating to conflict minerals. See https://www.axis.com/files/conformity/Conflict_Minerals_Policy_2019.pdf.
[142] Response of Axis to a letter of Amnesty International. Dated 13 May 2020.
[143] See: UNGP; and OECD Guidance on Human Rights Due Diligence, Annex Q6: "The size or resource capacity of an enterprise does not change its responsibility to conduct due diligence commensurate with the risk."

Amnesty International concludes that Axis Communications did not provide sufficient evidence to prove the fulfilment of its due diligence responsibilities under the UNGPs for the above-mentioned business activities.[144]

4.3 DUTCH EMOTION RECOGNITION AND BEHAVIOUR ANALYSIS TOOLS USED FOR CHINESE PUBLIC SECURITY RESEARCH

Noldus Information Technology is a developer of software, hardware, and integrated systems for measurement and analysis of human and animal behaviour.[145] Its international headquarters are in the Netherlands (Noldus Information Technology BV). Its presence in the People's Republic of China consists of its Asian headquarters in Beijing – Noldus (Beijing) Information Technology Co. Ltd – and three regional sales offices. According to information dating from 2019, Noldus (Beijing) Information Technology Co. Ltd is a limited liability company controlled solely by Noldus Information Technology BV, which holds 100% of the shareholder rights.

An investigation by the Dutch Customs and Tax Office (Team Export Control) that was finalized in June 2020 concluded that Noldus Information Technology has neither developed nor exported any goods that are currently regulated under the EU and Dutch exports regulation framework.[146] The fact that the below-described transactions are not export-regulated is trouble-some and one of the reasons for Amnesty International to publish this report.[147] In Chapter 5 we explain what is needed for human rights protections for such transactions. The business activities mentioned below have all been confirmed by Noldus Information Technology.[148]

The first transaction relates to the sale of *FaceReader* - an automated system of facial expressions analysis such as anger, happiness, sadness, surprise and disgust.[149] *FaceReader* is designed to be used in research environments. It runs on a Windows operating system that is connected to a camera that records facial expressions of people in front of the camera.[150] Previous versions of the software included facial recognition for the purpose of identifying a returning research subject and the ethnicity, gender and age of a research subject to refine the emotion recognition.[151] As reported by the Dutch media outlet 'De Correspondent' and confirmed by the company in 2019, Noldus Information Technology has directly sold FaceReader to the Chinese Ministry of Public Security.[152] The political debate that followed focussed on the ethnicity and facial recognition aspects of the technology and underlined that there might be a risk for the technology to be used directly for mass surveillance and discrimination of the Uyghur population in China.[153] When asked by Amnesty International about this transaction, Noldus Information Technology demonstrated through extensive documentation that their products are not sold for the use in public spaces without prior informed consent from subjects. Amnesty International notes that the Noldus products that are described in this report are not suitable for mass surveillance because they are specifically designed to be used in a laboratory setting. Yet, the exports of the technology posed a risk to human rights.

---

[144] Amnesty International acknowledges Axis Communications' expressed intentions to commit to human rights in future business operations in the Response of Axis to a letter of Amnesty International. Dated 23 June 2020.
[145] About Noldus - Innovative Solutions, Noldus, accessed 28 May 2020, www.noldus.com/about-noldus.
[146] Annex 5 to Response of Noldus Information Technology June 22, Conclusions of investigation Noldus Information Technology B.V. by Belastingdienst/Douane Groningen Team POSS/vestiging Rotterdam.
[147] Amnesty International makes a clear distinction between export regulated and export controlled. Amnesty wants to see all digital surveillance technologies exports regulated, meaning that the exporting entity will have the obligation to conduct human rights due diligence, the obligation to notify the competent authority when a significant risk is detected and that the company will have the obligation to refrain from exporting when such a risk cannot be mitigated. For digital surveillance technology that is not on the control list, the licensing authority should be able to hit the emergency brake when an export poses a significant risk to human rights, but the exporter is determined to export either way. When all digital surveillance technologies are export regulated, the ones that pose high risks to human right should be export controlled: meaning that the technology cannot be exported without a license. This is explained in more detail in Chapter 5.
[148] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[149] Noldus Information Technology, Reference Manual: FaceReader Version 6.1, August 2015.
[150] Noldus Information Technology, Reference Manual: FaceReader Version 6.1, August 2015.
[151] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[152] Maurits Martijn, Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest, De Correspondent, 12 July 2019, decorrespondent.nl/10307/berucht-chinees-veiligheidsministerie-gebruikt-nederlandse-software-die-emoties-leest/317002092-cae75d58.
[153] See e.g. https://groenlinks.nl/nieuws/groenlinks-wil-verbod-op-export-surveillancesoftware-naar-china

When asked about the end-use of the above-mentioned transaction, Noldus explained that they provided the software to the Center of Material Evidence Identification and that they were informed that "these tools are used in research on deceptive behavior of high-ranked individuals who are suspect of corruption."[154]

The second transaction refers to a public procurement procedure in 2017 to supply equipment to the People's Public Security University of China, in which Noldus (Beijing) Information Technology Co. Ltd was successful.[155] This transaction was also reported by 'De Correspondent'. [156] The People's Public Security University is directly run under the Ministry of Public Security. The tender concerned a project entitled "Second Phase of the Construction Project of the People's Public Security University of China Behavioural Science Applied Investigation Laboratory". Noldus (Beijing) Information Technology Co. Ltd won the bid. The transaction included a sale of two products: *FaceReader* and *The Observer XT*. On its website, Noldus Information Technology describes *The Observer XT* as "the most complete software for behavioural research" which provides "complete insight in behaviour and physiology" while letting the users "take advantage of fully integrated equipment". [157] Upon request, Noldus Information Technology informed Amnesty International that the software is used in the Behaviour Science Lab of the Public Security University to train investigators.[158] It is unclear what the investigators are being trained in.

When looking into more detail at the transaction reported by 'De Correspondent', Amnesty International discovered other previously unreported transactions. The third transaction is a sale of *The Observer XT* to the Fujian Police Academy through an intermediary sales entity in 2018.[159] The sale was made for a research project entitled "Digital Prison Teaching Practice Base (Laboratory for Criminal Behaviour Analysis and Correction)".[160] Noldus Information Technology explained to Amnesty International that they were informed that the "software is used to improve the way future prison managers are being trained." [161] It is unclear what the prison managers are being trained in.

The fourth transaction investigated by Amnesty International was made in 2012, when *The Observer XT* was bought by the Shihezi University in Xinjiang. Noldus Information Technology specified to Amnesty International that the product was bought by the College of Education of Shihezi University for research into educational psychology.[162] The university is instituted under the administration of the Xinjiang Production and Construction Corps (XPCC, also known as *Bingtuan*).[163] XPCC is "a distinctive military agricultural settlement and production institution" in Xinjiang,[164] formally subordinated to the dual leadership of the central government of China and the Xinjiang Uyghur Autonomous Region.[165] It takes up political, governmental, military, and enterprise roles. It handles its own administrative and judicial affairs within areas under its reclamation, and controls various entities including state

---

[154] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[155] "(trans. Winning Bid Announcement of the Second Phase of the Construction Project of the People's Public Security University of China Behavioral Science Applied Investigation Laboratory) 中国人民公安大学行为科学侦查应用实验室二期建设项目中标公告", dated 26/07/2017, listing the People's Public Security University of China as the tender owner and purchasing party, and Noldus (Beijing) Information Technology Co. Ltd, Beijing Fistar Technology Co., Ltd. and Shanghai Fedu Technology Co., Ltd. as the successful bidders
[156] Maurits Martijn, Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest, De Correspondent, 12 July 2019, decorrespondent.nl/10307/berucht-chinees-veiligheidsministerie-gebruikt-nederlandse-software-die-emoties-leest/317002092-cae75d58.
[157] Behavioral Coding - Event Logging Software | The Observer XT, Noldus, accessed 28 May 2020, www.noldus.com/observer-xt.
[158] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[159] Fujian Science Equipment Import & Export Co., Ltd. (福建省科学器材进出口有限公司).
[160] "(trans. Purchase Results Announcement of Digital Prison Teaching Practice Base (Laboratory for Criminal Behavior Analysis and Correction)) 数字化监狱教学实践基地(罪犯行为分析与矫正实验室)采购结果公告", dated 10/08/2018, listing the Fujian Police Academy as the tender owner and purchasing party, and Fujian Science Equipment Import & Export Co., Ltd. as the successful bidder.
[161] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[162] A 2012 tender document indicates an intent of Shihezi University to purchase The Observer XT: "(trans. Psychology Laboratory Equipment Tender Notice) 心理学实验室设备招标公告", dated 18/09/2012, listing products including The Observer XT 10.5, indicating that it is the Bingtuan Uniform Procurement Center that conducts the public tendering for the Shihezi University Psychology Laboratory Equipment Purchase Project. In a response of Noldus to a letter of Amnesty International, dated 22 June 2020, Noldus indicates that The Observer XT was bought in 2012 by the Shihezi University College of Education for research into educational psychology.
[163] Shihezi University was founded in April 1996 under the integration of institutional colleges by the Ministry of Education and the Xinjiang Production and Construction Corps. See: 'About Us', Shihezi Univeristy, accessed 15 August 2020, https://www.shiheziuniversity.com/about-us/. Scholars have characterized the university as being "owned" by the Xinjiang Production and Construction Corps. See, for example, Bao, Yajun, 'The Xinjiang Production and Construction Corps: An Insider's Perspective', BSG Working Paper Series, January 2018, https://www.bsg.ox.ac.uk/sites/default/files/2018-05/BSG-WP-2018-023.pdf, p.11.
[164] Zhu, Yuchao and Dongyan Blachford, '"Old Bottle, New Wine"? Xinjiang Bingtuan and China's ethnic frontier governance', Journal of Contemporary China 25/97, 2016, https://www.researchgate.net/publication/283187498_'Old_Bottle_New_Wine'_Xinjiang_Bingtuan_and_China's_ethnic_frontier_governance p.1.
[165] 'White Paper: The History and Development of the Xinjiang Production and Construction Corps', Sina English, accessed 15 August 2020, http://english.sina.com/china/2014/1004/742790.html.

farms, enterprises, and educational institutions.[166] XPCC was established in 1954 and is officially referred to as a "highly organized paramilitary force".[167] It fulfils a special role "in safeguarding the country's unification and Xinjiang's social stability and in cracking down on violent terrorist crimes".[168] It has been a Han majority institution from its beginning,[169] and has been instrumental in facilitating long-term Han migration into Xinjiang.[170]

The latest transaction to an entity in Xinjiang stems from late 2018, when Noldus Information Technology participated in a procurement procedure of the Xinjiang Normal University, which led to the sale of *FaceReader* and *The Observer XT* to the university's College of Educational Science.[171] Noldus Information Technology explained to Amnesty International that the tools were bought for research in educational psychology.[172]

In its response to Amnesty International's findings, Noldus argues that their products should not be classified as surveillance technology since they are sold with the purpose of "observation and analysis of human behavior […] in scientific research or professional training, in studies that are subject to ethical approval and consent of all participants".[173] The products do, however, qualify as digital surveillance tools because the Noldus' emotion recognition and behavioural analysis systems are specifically designed to enable non-covert surveillance by digital systems with a view to monitor, extract, collect and/or analyse data from individuals (See Section 2.1). What is more, at the time of the aforementioned transactions, *FaceReader* also included facial, gender, age and ethnicity recognition. These systems constitute clear examples of biometric technologies (See Section 2.2 and 3.4).

The exports described in this report pose a significant risk to human rights due to the combination of factors: the end-use (i.e. contributing to the upholding of the criminal law system), the type of product (i.e. biometric technology), the country of destination (i.e. China), and the end-user (i.e. public security and law enforcement-related institutions).

First, the end-use of transaction one to three is focussed on improving the enforcement of criminal law by doing behavioural research on corruption and training investigators and prison managers. As pointed out in Section 3.4, China has failed to bring its criminal law system in line with international laws and standards, and criminal law is often (mis)used to restrict human rights. Providing tools to facilitate the operation of this criminal law system forms a significant risk to human rights.

Second, as mentioned above, Noldus' products include biometric technology, including emotion recognition technology and at the time of the transactions the FaceReader also included facial recognition, which in itself poses a risk to human rights (See Section 3.4). Facial recognition systems form such a high risk to human rights that Amnesty International and the UN Special Rapporteur on Freedom of Opinion and Expression call for ban on the export this type of technology for identification purposes (See Section 2.2).[174]

Third, Noldus' products were sold to China. China is a country that actively pursues comprehensive surveillance and control over its population (See Section 3.2). It also has a poor human rights record and a lack of human rights safeguards in its legal system (See Section 3.3 and 3.4). Selling digital surveillance technology to a country such as China contributes to the risk to human rights. Moreover, in two of the investigated transactions, products of Noldus Information Technology were sold to entities in Xinjiang, which is known to be a place of widespread discrimination and human rights violations. The latest transaction to Xinjiang was in late 2018 when the mainstream

[166] Zhu and Blachford, '"Old Bottle, New Wine"? Xinjiang Bingtuan and China's ethnic frontier governance', p.10.
[167] 'White Paper: The History and Development of the Xinjiang Production and Construction Corps'.
[168] 'White Paper: The History and Development of the Xinjiang Production and Construction Corps'.
[169] Zhu and Blachford, '"Old Bottle, New Wine"? Xinjiang Bingtuan and China's ethnic frontier governance', p.11.
[170] 'Many Han Chinese don't mind the gulag for their Uighur neighbours', The Economist, 9 January 2020, accessed 15 August 2020, https://www.economist.com/china/2020/01/09/many-han-chinese-dont-mind-the-gulag-for-their-uighur-neighbours; Ramzy, Austin and Chris Buckley, 'Absolutely No Mercy: Leaked Files Expose How China Organized Mass Detentions of Muslims', The New York Times, 16 November 2019, accessed 15 August 2020, www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html; and Olesen, Alexa, 'China's Vast, Strange, and Powerful Farming Militia Turns 60', The Foreign Policy, 8 October 2014, accessed 15 August 2020, https://foreignpolicy.com/2014/10/08/chinas-vast-strange-and-powerful-farming-militia-turns-60/.
[171] "trans. Public Announcement of the Xinjiang Normal University Mental Development and Learning Science Laboratory Equipment Purchase Project Results 新疆师范大学心智发展与学习科学实验室设备采购项目成交结果公示", dated 13/12/2018, listing Xinjiang Normal University as the tender owner and purchasing party, and Beijing Fistar Technology Co., Ltd. as the successful bidder with products including FaceReader 7.
[172] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[173] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[174] See https://news.un.org/en/story/2019/06/1041231.

media reported frequently on the human rights abuses in Xinjiang. [175] Selling the tools to customers in this region forms a significant risk to human rights.

Lastly, Noldus' products were sold to end-users that included public security and law enforcement-related institutions. In the first transaction, the sale of Noldus' products to the Chinese Ministry of Public Security forms a risk to human rights caused by the fact that the Ministry of Public Security is an important force behind the integration of biometric surveillance technologies in targeted and mass surveillance initiatives. The sale of behavioural analysis and emotion recognition software that included facial and ethnicity recognition features – as basic as these features might have been – to the Chinese Ministry of Public Security facilitates the familiarization with and study of these tools by the end-user. A similar risk is posed in the second and third transaction where the end-users are the government-related People's Public Security University and the Fujian Police Academy.

The end-user in the fourth transaction is the Shihezi University in Xinjiang, which is owned by the XPCC, a paramilitary entity with extensive tasks regarding the maintaining of social stability in Xinjiang. [176] The export of the Noldus products to this end-user forms a significant risk to human rights. In 2012, the year of the transaction, it was already known that the Chinese government routinely conflates Uyghur cultural and religious practice with terrorism.[177] In the years that followed the technological advancement of the suppression of minorities in Xinjiang became apparent. In the fifth transaction, Noldus Information Technology entered a public procurement procedure in late 2018 to sell their emotion recognition and behaviour analysis tools to the Xinjiang Normal University as end-user. The Xinjiang Normal University is not under the direct administration of the central government. However, in the present-day Chinese reality, universities are heavily controlled by the Chinese authorities, as are all public (and private) entities in China.[178] While our research did not investigate direct links between the university projects involving Noldus products and the expansion of state surveillance and control in Xinjiang, the evidence emerging from our research and the information provided to Amnesty International by the company speak to the space that Noldus Information Technology occupies within the Chinese research field relating to emotion and behavioural analysis – an area which is of particular interest to the Chinese authorities. [179]

At the time of the transactions, the company should have conducted due diligence in order to verify the end-use and end-users and the actual and potential risks to human rights. In correspondence with Amnesty International, Noldus provided no clear answer as to what due diligence measures it carried out, if any, to address these potential human rights impacts of the above described business operations.[180] For these exports, Noldus did not fulfil its human rights due diligence responsibilities under the UNGPs.

The facial recognition and ethnicity recognition features from the FaceReader were removed from the tools in July 2019 and since then Noldus Information Technology has prepared and enacted policies to prevent future risks to human rights associated with their business operations throughout the supply chain, including a policy for sales to defence and law enforcement agencies, which was shared by Noldus Information Technology with Amnesty International. [181] In the policy Noldus Information Technology states that it does not allow its product to be used for public surveillance or other human rights violations. This policy commitment is a first step in the responsibility to respect human rights. The company has been actively engaged with Amnesty International during the investigation.

---

[175] See for example: https://www.reuters.com/article/us-china-rights-xinjiang/big-data-predictions-spur-detentions-in-chinas-xinjiang-human-rights-watch-idUSKCN1GB0D9 and https://www.economist.com/briefing/2018/05/31/china-has-turned-xinjiang-into-a-police-state-like-no-other.
[176] Bao, 'The Xinjiang Production and Construction Corps: An Insider's Perspective', p. 11.
[177] Amnesty International, 'China must reveal whereabouts of Uighur children detained after deadly clash', 6 January 2012, www.amnesty.org/en/latest/news/2012/01/china-must-reveal-whereabouts-uighur-children-detained-after-deadly-clash.
[178] Gu, Mini, Rachel Michael, Claire Zheng, and Stefan Trines, Education in China, 17 December 2019, https://wenr.wes.org/2019/12/education-in-china-3; and Phillips, T., China universities must become communist party 'strongholds', Guardian, 12 September 2016, www.theguardian.com/world/2016/dec/09/china-universities-must-become-communist-party-strongholds-says-xi-jinping.
[179] Apart from the instances cited above, our research revealed that Noldus products, FaceReader and The Observer XT, are used by a variety of other Chinese universities. The research was based on public procurement documents including, among others: "(trans. Winning Bid Announcement of the Purchase Project of Scientific Research Instruments and Equipment for the Beijing Forestry University in 2019 (4)) 北京林业大学 2019 年科研仪器设备采购项目(四)中标公告", dated 17/06/2019, listing the Beijing Forestry University as the tender owner and purchasing party, and Beijing Zhongtian Ruihe Technology Co., Ltd. as the successful bidder for the first package of the tender which includes the Noldus FaceReader; "(trans. Chongqing University - Details of Bidding Results (CB106112018001170) 重庆大学–竞价结果详情 (CB106112018001170)", dated 15/05/2018, listing Noldus (Beijing) Information Technology Co. Ltd as the successful bidder and The Observer XT as the successful product; Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[180] Response of Noldus to a letter of Amnesty International. Dated 22 June 2020.
[181] Annex to Response of Noldus to a letter of Amnesty International. Dated 22 June 2020; Annex to Response of Noldus to a letter of Amnesty International. Dated 15 September 2020.

Amnesty International is hoping to see the voluntary steps that are now taken by this exporter of emotion recognition technology becoming mandatory for the whole industry.

4.4 IMPLICATIONS OF LACKING EXPORTS REGULATIONS

During this investigation, one thing became very clear: we have only scratched the surface of the EU digital surveillance exports to countries with a poor human rights reputation. The digital surveillance industry is known for not complying with its human rights responsibilities. UN Special Rapporteur on Freedom of Opinion and Expression concluded that "[t]he global surveillance industry … appears to be out of control, unaccountable and unconstrained in providing governments with relatively low-cost access to the sorts of spying tools that only the most advanced state intelligence services previously were able to use."[182] Due to weak regulatory frameworks and oversight, the surveillance industry operates "from the shadows" and continues to "freely sell their technology to countries where human rights are not protected or respected".[183] In previous reports, Amnesty International noted the threats of digital surveillance to human rights defenders and the role of the digital surveillance industry in this process.[184] It is time for the surveillance industry to be regulated. The following Chapter outlines Amnesty International's position on how to adequate tackle the exports of surveillance technologies from the EU member states to mitigate the risks to human rights.

[182] David Kaye, 'The surveillance industry is assisting state suppression. It must be stopped', 26 November 2019, The Guardian, https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware.
[183] Banerji, A Dangerous Alliance: Governments Collaborate with Surveillance Companies to Shrink the Space for Human Rights Work.
[184] Amnesty International, Ending the Targeted Digital Surveillance of Those Who Defend Our Rights.

5. HOW TO INCLUDE HUMAN RIGHTS SAFEGUARDS IN EU EXPORT REGULATION

The involvement of EU digital surveillance companies in the procurement procedures of central actors in the Chinese public security domain and the use of emotion recognition software from the EU in Chinese universities', criminal law enforcement and public security-related investigations and research, reveal major shortcomings of the current export regulation framework of the EU and expose risks to human rights.

The export regulation framework is laid down in what is known as the Dual Use Regulation No 428/2009, which – at the time of writing – is up for revision.[185] In 2015, the European Parliament called upon the EU institutions and member states to secure adequate measures with regard to "the impact of intrusion and surveillance systems on human rights in third countries".[186] The European Parliament additionally pointed out that "as a result [of lacking regulation], private actors play a more active role in assessing the legality of content and in developing cyber-security systems and surveillance systems, which can have a detrimental impact on human rights all over the world."[187] Accordingly, since 2016, the European Union has been in a formal legislative procedure to modernise the export controls and the associated Dual Use Regulation.[188]

At the core of this modernisation is the introduction of greater safeguards to mitigate risks to human rights in third countries.[189] The European Commission and the European Parliament have made ground-breaking proposals to expand the scope of the Regulation. The proposals and amendments to the proposal governed the regulation of a wider range of digital surveillance technologies, prescribed due diligence obligations, included the possibility to put emerging digital surveillance technologies on a European control list, introduced a stronger 'emergency brake' procedure, and more transparency, and secured human rights as a decisive criterion in export authorisation

[185] Council Regulation (EC) No 428/2009 of 5 May 2009.
[186] European Parliament, Report on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries (2014/2232(INI)), June 3, 2015), www.europarl.europa.eu/doceo/document/A-8-2015-0178_EN.html.
[187] European Parliament, Report on 'Human Rights and Technology (2014/2232(INI)), para G.
[188]Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast).
[189] The European Commission initially called it "the human security approach".

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

processes. These changes would follow the EU's long-standing normative commitment to the protection of human rights in international trade and policies.[190]

However, at the time of writing this report, the efforts to secure human rights in the European export regulation framework are blocked by the Council of the European Union, which represents the member states. The Council of the EU has rejected the human rights safeguards that were proposed by the European Commission and amended by the European Parliament.

This legislative process appears to be stuck. Since October 2019, the Recast Dual Use Regulation is being discussed in trialogue negotiations between the members of the European Parliament, the European Commission and representatives of the Council of the EU.[191] The European Commission acts as a mediator in this process. The outcome of the trialogue negotiations is decisive to the future of the impact of the European Union's exports on human rights worldwide. **Amnesty International calls upon the European legislators to secure human rights in the Recast Dual Use Regulation. Amnesty International also calls upon the European Commission – in its role as mediator – to secure in the text of the Recast Dual Use Regulation the commitment of the EU to uphold and promote respect for human rights and to contribute to the protection of human rights as stipulated in Article 2, 3 (5) and 21 of the Treaty of the EU.**

The following Sections discuss necessary human rights safeguards in export regulation and illustrate how the absence of these safeguards has led to significant risks to human rights in the past, including the cases presented in Chapter 4. The future of the export regulation framework must effectively prevent these risks and adequately adjust the legislation. If the changes described below are not made, Amnesty International calls for a moratorium on the export of digital surveillance technology from the EU until a proper human rights regulatory framework is put in place.[192]

5.1 ADOPT TECHNOLOGY-NEUTRAL CRITERIA TO REGULATE EXPORTS OF DIGITAL SURVEILLANCE TECHNOLOGIES

The current EU export regulation framework fails to adequately regulate the human rights impact of a wide range of existing and emerging digital surveillance technologies. Historically, the focus of European export regulation was limited to the regulation of technologies that could be used in a military context.[193] This singular focus is no longer legitimate, since there are many technologies nowadays that "are not specifically designed for military use but nonetheless used for repression" and other human rights violations.[194] Digital surveillance technology is the most prominent example of this. The European Commission proposed to expand the scope of the regulation to "concepts beyond military-related end use"[195] and include 'cyber-surveillance technologies' as a subcategory in the export regulation framework.[196] Amnesty International applauds the introduction of this subcategory.

In order to secure the longevity and effectiveness of export regulation, general legislation such as the Recast Dual Use Regulation should set the criteria for technology that falls under its scope. Therefore, instead of defining 'cyber-surveillance technologies' based on its technical specifications, the European legislators should opt for *technology*

[190] As established in articles 2 and 3(5) of the Consolidated version of the Treaty on European Union (2008/C 115/01), (European Union: December 13, 2007). See also, Charter of Fundamental Rights of the European Union (2012/C 326/02), Official Journal of the European Union, October 26, 2012.
[191] Beatrix Immenkamp, Review of Dual-Use Export Controls, European Parliament Research Service, November 2019, www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf.
[192] Amnesty International, Ending the Targeted Digital Surveillance of Those Who Defend Our Rights, p. 17.
[193] Kanetake Machiko, The EU's Dual-Use Export Control and Human Rights Risks: The Case of Cyber Surveillance Technology, Europe and the World: A Law Review vol. 26, June 2019, p. 5.
[194] Privacy International, The Global Surveillance Industry, p. 8.
[195] Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast), para 8; Kanetake, The EU's Dual-Use Export Control and Human Rights Risks, p. 5.
[196] See the latest: European Commission, Draft Compromise Text - EU Controls on Non-Listed Items, 6 May 2020, art. 2.21.

neutrality in the export regulation framework.[197] A technology-neutral approach ensures that a range of technologies with similar technical specifications are not overregulated and there is no increased regulatory burden on governments nor industry.[198] Instead, the definition should be oriented towards the intended end-use. This way a broad range of current and *future* technologies that pose risks to human rights will fall under the scope of export regulation frameworks. The following criteria should determine the technology-neutral definition of 'cyber-surveillance technologies':

- may consist of hardware, software and related services;
- could be used in connection with the violations of human rights or the commission of violations of human rights law or international humanitarian law; and
- is designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data.

5.2 ESTABLISH EXPEDITIOUS PROCEDURES TO PUT NEW FORMS OF DIGITAL SURVEILLANCE ON THE CONTROL LIST

In the past, civil society groups addressed national governments in a call to impose authorisation requirements on the export of new and emerging digital surveillance technologies that are sold which involve significant risks to human rights.[199] However, member states have shown little interest in regulating exports at a national level. Governments fear being the only EU member state with an authorisation requirement and presume that this will harm "playing level field" and the economy.[200] Even at the *supra* level, some have expressed the concern that implementing EU-specific export restrictions would significantly disadvantage European companies, drawing business out of the EU.

The EU export regulation framework is dependent on the decisions made by a multilateral export control forum: the Wassenaar Arrangement (WA). The WA members meet once a year to discuss the amendments to the list of controlled items.[201] To illustrate: in 2004, Amnesty International highlighted the need to regulate telecommunications systems that facilitate "interception".[202] The export of this type of technology was discussed only nine years later and appeared on the WA control list in December 2013.[203] It took another year, until 31 December 2014, before the WA control list was officially incorporated into the EU exports control list. In total, 10 years after the human rights risks of interception software were brought to the attention of national legislators, the export of interception technology was finally regulated.[204] Considering the rapid emergence of new forms of surveillance technologies each year, a procedure that potentially lasts 10 years is unacceptably slow.

[197] The European legislature has chosen this path before, e.g. with the General Data Protection Regulation; see GDPR, recital 15. Experts say that the technology-neutral approach of the GDPR is one of the key aspects that make the regulation successful in the protection of fundamental rights while facilitating a level playing field for innovation and the free flow of information.
[198] European Commission, Data and information collection for EU dual-use export control policy review, p.203.
[199] 'Open NGO Letter to EU member states and Institutions Regarding the Export of Surveillance Equipment', July 2017, www.accessnow.org/cms/assets/uploads/2017/07/NGOlettertoEUmemberstatesonsurveillanceexports.pdf; and Amnesty International, An Open Letter to the Members of the Wassenaar Arrangement, 2 December 2014.
[200] In May of 2018, 11 member states expressed the concerns that an autonomous control list "could seriously undermine the competitiveness of EU-based industry" as stricter "controls on EU exports without parallel measures in the other major economies would serve only to push the development and production of relevant technologies outside of the EU". Working Paper on the EU Export Control – Paper for Discussion.
[201] 'Home - The Wassenaar Arrangement', accessed 30 November 2019, https://www.wassenaar.org/.
[202] Amnesty International, Undermining Global Security: The European Union's Arms Exports, 2004, p. 62.
[203] Wassenaar Arrangement, The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technology, 4 December 2013, www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf.
[204] European Commission, Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014 Amending Council Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items, 22 October 2014, para. 13, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R1382&from=EN.

It is, therefore, important that export regulation frameworks include expeditious and effective procedures to put new forms of digital surveillance on the control list.[205] In the EU, it should be possible for member states, a group of member states or the institutions of the European Union to initiate legislative procedures to control certain items. The institutions should not have to wait until the industry identifies risks to human rights to block the exports of certain items. The legislative bodies must have the ability to start the process of adding new items to the control list based on their own investigations or those of others, including of civil society. When it comes to the approvals process for adding new items to the expeditious EU control list, the procedure must allow human rights risks to be addressed swiftly and efficiently as soon as a Member State or the EU institutions become aware of the risk.

The EU institutions and member states should initiate and prioritize the addition of biometric surveillance items that pose significant risks to human rights, such as facial recognition technology and ethnicity recognition technology to the EU control list, once the framework has been established. Amnesty International invites member states and EU institutions to adapt to the rapidly changing landscape of digital surveillance technologies and implement expeditious and effective procedures to put new forms of such technologies on the control lists.

5.3 INCLUDE HUMAN RIGHTS IN THE AUTHORISATION DECISION

When an item is placed on the control list, its export to outside the EU must be authorised. In this authorisation process, the licensing authority reviews compliance with various assessment criteria. In the current EU export regulation framework, digital surveillance items that are on the list (i.e. intrusion and interception software) are not held to the standards of international human rights, and the related risks to human rights do not play a role in their export authorisation.[206] EU law does not require licensing authorities to take human rights into account in their decisions when authorising export of non-military items or to non-military end-users, such as digital surveillance items that will be used by domestic public security bureaus or by law enforcement agencies that uphold laws and regulations that violate human rights. This is unacceptable. Authorisation decisions should, amongst other criteria, take into account the human rights situation in the country of the end-use or the human rights record of the end-user.

In the authorisation process for exports of listed items, licensing authorities must take into account the occurrence of domestic and international violations of human rights law, the legal safeguards to ensure human rights protections, and compliance with international humanitarian and human rights law in the country of final

[205] Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast). The autonomous control list aims to address the controls of items that have not (yet) been included in the Wassenaar Agreement. In the previous proposal of the Parliament, the required threshold to deny the addition of an item to the EU autonomous list was at least four member states representing at least 35% of the population of the Union. European Commission, Draft Compromise Text - EU Controls on Non-Listed Items, art. 4(6). The 'EU autonomous list' may potentially adopt new items to the regulatory framework before they are even discussed at the WA meeting. The 'EU autonomous list' has come to be a dividing topic in the Council. Most recently, the Commission proposed that the items should be added to the (autonomous) control list upon the agreement of all member states.

[206] Human rights are only taken into account when "military technology or equipment" is exported. Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, art. 2(2)(a). Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items, art 12; Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment, art. 2(1). Currently, licensing authorities may stop exports of items that violate commitments to non-proliferation regimes, violate export control arrangements, or are prohibited under sanctions. Particularly relevant to this discussion is Criterion 2: "Respect for human rights in the country of final destination". Council Common Position 2008/944/CFSP of 8 December 2008 Defining Common Rules Governing Control of Exports of Military Technology and Equipment" Art. 2(2). Additionally, Criterion 7 as it stands today postulates that an export license may be granted after considering "intended end use and the risk of diversion". In the context of the current regulation, the undesirable "end use" or "end user" are limited to "purely 'military' WMD [Weapons of Mass Destruction] proliferation-related" risks. European Commission, Commission Staff Working Document Impact Assessment. Report on the EU Export Control Policy Review, 28 September 2016, para. 28, https://trade.ec.europa.eu/doclib/docs/2016/october/tradoc_155008.pdf. The risks that an undesirable end-use will target civilians is not amongst the current licensing considerations.

destination.[207] Authorisation must be denied when a significant risk is identified that the exported item might be used in connection with human rights violations.

5.4 ADOPT DUE DILIGENCE OBLIGATIONS FOR EXPORTING COMPANIES

Businesses have the responsibility to respect all human rights wherever they operate, including throughout their operations and supply chain, as already mentioned in Section 4.4. To fulfil human rights-related responsibilities, companies should conduct human rights due diligence to address the impacts of their products, operations, and business partners in the supply chain on human rights. A recent study in the EU shows that the current international voluntary due diligence framework is unsatisfactory to significantly change the way businesses manage human rights impacts.[208] Only about 1/3 of the exporting companies conduct some form of human rights impacts review, and the procedures are not systematic.[209] This trend can also be observed amongst the businesses investigated by Amnesty International (see Section 4.4.). In the Recast Dual Use Regulation, the European Commission and the Parliament supported the introduction of due diligence *obligations*.[210] In April 2020, Justice Commissioner, Didier Reynders, announced EU human rights due diligence legislation and underlined the need for mandatory rules that will also sanction those businesses that fail to address risks to human rights.[211] This commitment was since then reinforced and supported by the European Parliament who said that "business enterprises [should] have an obligation to identify, prevent, mitigate, monitor and account for potential and actual human rights abuses and environmental harm in their entire global value chains".[212] Mandatory human rights due diligence rules in the Recast Dual Use Regulation can be the first steps in that direction.[213] This sector specific first step is needed due to the specific risks that are posed by the export of digital surveillance technology and to limit human rights abuses during the legislative process of the generic due diligence legislation. However, the negotiation mandate for the trialogue meetings of the Council of the EU shows that the member states are not willing to fulfil their duties to establish and enforce adequate policies, legislation, and regulations to effectively address the risk of business involvement in human rights abuses in the context of exports of digital surveillance technologies.[214] This is unacceptable.

Given the human rights risks associated with the export of digital surveillance technology, export regulation frameworks should obligate exporting companies to identify, prevent, mitigate, and account for how they address their actual and potential impacts on human rights, associated with their operations, services and products, including through their supply chain. After the identification of potential or actual human rights abuses through a business relationship companies must take adequate action to prevent adverse human rights impacts as an integral part of business decision-making and risk management systems. This obligation should apply equally to the exports

[207] European Parliament, Amendments Adopted by the European Parliament on 17 January 2018 on the Proposal for a Regulation Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast), art. 14(1)(b) amended; Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast), art. 14(1)(b).

[208] Lise Smit et al., Study on Due Diligence Requirements through the Supply Chain, European Commission, January 2020, p. 16. The issue of voluntary due diligence is also discussed in Amnesty International, Injustice Incorporated: Corporate Abuses and the Human Right to Remedy, 2014, pp. 157–170.

[209] Smit et al., Study on Due Diligence Requirements through the Supply Chain.

[210] Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast), art. 4(2).

[211] 'EU Commissioner for Justice commits to legislation on mandatory due diligence for companies', Business & Human Rights Resource Centre, 29 April 2020, https://www.business-humanrights.org/en/latest-news/eu-commissioner-for-justice-commits-to-legislation-on-mandatory-due-diligence-for-companies/.

[212] Letter to the Commissioner Didier Reynders 'EU is well placed to show leadership with its future due diligence legislation', European Parliament Working Group on Responsible Business Conduct, 27 May 2020, https://responsiblebusinessconduct.eu/wp/2020/05/27/ep-rbc-working-group-eu-is-well-placed-to-show-leadership-with-its-future-due-diligence-legislation/.

[213] Amnesty International Public Statement (EUR 01/2252/2020), 30 April 2020, www.amnesty.org/download/Documents/EUR0122522020ENGLISH.pdf; see also: www.business-humanrights.org/en/eu-commissioner-for-justice-commits-to-legislation-on-mandatory-due-diligence-for-companies.

[214] UNGP, para. 3–4 & 14. In April 2020, Commissioner D. Reynders committed to implementing EU-wide "mandatory, cross-sectoral" due diligence requirements and proposed possible sanctions on not fulfilling this obligation by companies. Didier Reynders, 'Presentation and discussion with Commissioner for Justice on Due Diligence Study', Responsible Business Conduct Working Group, 29 April 2020.

of listed as well as non-listed digital surveillance technologies. If, during their due diligence procedure, a company becomes aware of a significant risk to human rights, they should immediately notify the component licensing authorities, who may abruptly prevent the exports of non-listed items that form the significant risk to human rights (see more in Section 5.5). In a case where the company *cannot* prevent the abuses, it should mitigate the risks or refrain from engaging in a business relationship. Companies should provide transparency regarding human rights due diligence procedures (see more in Section 5.6) and provide effective remedy to people who have suffered human rights harms linked to the company's products and services.

5.5 ESTABLISH AN 'EMERGENCY BRAKE' PROCEDURE FOR ANTICIPATED EXPORTS OF NON-LISTED ITEMS THAT POSE A SIGNIFICANT RISK TO HUMAN RIGHTS

An export regulation framework ought to include an 'emergency brake' procedure for exports of non-listed items that pose a significant risk to human rights. Under the EU export regulation framework such a procedure is called the 'catch-all provision'. The catch-all provision works much like an 'emergency brake' procedure, which means that the licensing authority may abruptly control and if necessary deny exports of non-listed items.[215] If future exports of similar digital surveillance items lead to similar risks for human rights, the emergency brake procedure is ideally followed by placing the export of similar digital surveillance items on the EU control list as a more sustainable and durable solution.

Licensing authorities should be in a position to use various sources of information to base their emergency brake decision on, including information from civil society groups. If, during their due diligence procedures, companies become aware of a significant risk to human rights, the companies should notify the competent authorities, who then have the possibility to temporarily stop the export of that type of non-listed digital surveillance item, in order to avoid the end-user from trying to buy the items at a different supplier. Member State authorities should share this information with each other in order to improve the effectiveness of this procedure in protecting human rights.

5.6 ENHANCE TRANSPARENCY OF EXPORTS

As the last step to achieving an effective export regulation framework, it is important to establish measures that improve transparency and accountability. Under the current EU export regulation framework, member states are only obliged to share information about authorisations that the authority has denied.[216] Therefore, the public disclosure of information regarding the authorisations is at the discretion of the government.[217] Currently, the practice of sharing licensing decisions differs greatly from one Member State to another. In many cases, the information remains undisclosed.

Enhanced transparency in authorisation decisions and emergency brake decisions would improve a harmonised implementation of the export policy. As early as 2014, the European Commission concluded that "transparency and coordinated outreach could be critical steps to provide clarity on requirements, support operators' compliance efforts and improve their capacity to implement controls."[218] The European Commission further argued that

[215] Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-Use Items, art. 4; Sebastiaan Bennink and Gonnie van Dam, Catch Me If You Can: Toward a Common Policy on EU Catch-All Controls, WorldECR, December 2019, p. 19, batradelaw.com/wp-content/uploads/2019/12/EU_catch_all_controls_policy.pdf. This provision has also been referred to as the 'end-use controls', since it controls items that are or may be intended for the development of chemical, biological or nuclear weapons, or if the country of destination is subject to an arms embargo. This is contrary to the controls of listed items, which are denied licenses based on their technical qualifications.

[216] Bennink and van Dam, Catch Me If You Can: Toward a Common Policy on EU Catch-All Controls.

[217] Bennink and van Dam, Catch Me If You Can: Toward a Common Policy on EU Catch-All Controls.

[218] European Commission, Communication from the Commission to the Council and the European Parliament. The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World, 24 April 2014, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0244&from=en.

enhancing transparency would provide businesses with an "integrated approach" and thus also clarity on the exports regulation.[219]

Amnesty International supports greater transparency in the export licensing decisions, and calls upon the European Commission, the European Parliament, and member states to further enhance transparency and ensure it is enshrined into the practice of every licensing authority in the EU. Greater transparency should entail a public disclosure of information related to authorisation decisions including information on exports volume and the nature, value and destination of the intended export of listed digital surveillance items for which an authorisation has been requested and on authorisation processes of non-listed digital surveillance technologies under the emergency brake procedure.[220]

[219] Communication from the Commission to the Council and the European Parliament. The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World. Article 24 of the Commission's proposal asks states to submit annual reports and share best practices. Proposal for a Regulation of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (Recast), art. 24.
[220] Including the authorization decisions based on art. 4 and 8 of the (Recast) Dual Use Regulation.

CONCLUSIONS AND RECOMMENDATIONS

The digital surveillance industry is constantly evolving. Historically, digital surveillance has primarily been associated with interferences in the right to privacy. Emerging forms and applications of surveillance are now shifting the impact to the freedom of assembly, speech and religion and the right to equality and non-discrimination. This is certainly the case for biometric surveillance technologies that are deployed in public spaces to single out people based on their ethnicity, which violates the rights to equality and non-discrimination (see Chapter 2).

The use of biometric surveillance technologies is rising in China. Large surveillance networks that deploy cameras are increasingly connected to biometric surveillance technologies, enabling the Chinese authorities to identify individuals in public spaces with the help of, for example, facial recognition. Many of the Chinese surveillance efforts are in violation of international human rights law because they fail to meet internationally recognised standards of necessity, legality, and proportionality. Chinese privacy and surveillance laws lack adequate safeguards and clear protection guidelines. Chinese laws exploit concepts such as 'national security' and 'terrorism' to provide broad discretionary powers to the public authorities to conduct mass and targeted surveillance and restrict the exercise of freedom of speech, religion, and assembly. Surveillance projects, such as the Sharp Eyes and Skynet projects, are conducted without a reasonable suspicion or a possibility to 'opt out', which amounts to indiscriminate mass surveillance. Projects that conduct indiscriminate mass surveillance can never be proportionate or necessary in relation to the envisaged aims, even in matters of national security. Moreover, digital surveillance technology can facilitate automated and systematic discrimination. With the use of biometric technologies, ethnic minorities such as the Uyghur population are singled out and are receiving different treatment throughout the country. This violates the rights to equality and non-discrimination and affects the rights to freedom of expression, association, religion or belief, and cultural life (see Chapter 3).

Yet companies based in the EU continue to export digital surveillance technologies to Chinese Public Security Bureaus to be deployed, or at risk of being deployed, in connection with indiscriminate mass surveillance, like the Skynet and Sharp Eyes projects. EU companies are also exporting biometric surveillance technology to research institutions that are connected to key players in the Chinese surveillance domain or to be used in support of enforcing law that violate human rights. These exports pose a significant risk to human rights. As is often the case for the surveillance industry (see Chapter 4), the exporting companies identified in this report did not fulfil their responsibilities for human rights due diligence under international human rights law.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

The results presented in this report show a system that fails to protect human rights in the export of digital surveillance technology from the European Union. This system needs fixing, and it needs it fast.

The results presented in this report show a system that fails to protect human rights in the export of digital surveillance technology from the European Union. This system needs fixing, and it needs it fast. At the time of writing this report, the EU legislature is in the last phase of revising the EU framework for the regulation of surveillance exports, known as the Recast Dual Use Regulation. In order to assure the longevity of the revised rules as well as to protect human rights at all phases of the export process, Amnesty International urges the European legislators to adopt technology-neutral criteria to define the object of the regulation: the export of digital surveillance technology to countries outside the EU. The framework must facilitate expeditious procedures to put emerging digital surveillance technologies on the control list. Biometric surveillance technologies should be included on the list. In particular, regulating systems that enable ethnicity and facial recognition must be a priority.

Accordingly, national licensing authorities should ensure that export authorisations take into account the occurrence of domestic and international violations of human rights law, fundamental freedoms and international humanitarian law in the country of final destination. The framework must impose obligations on the exporting companies of listed and non-listed digital surveillance technologies to identify, prevent and mitigate the actual and potential impacts on human rights associated with their operations, services, and products. The exporting company should take adequate measures to prevent adverse impacts on human rights. In cases where that is not possible, where the company identified a significant risk to human rights and was unable to mitigate the risk, the company should have an obligation to notify the national licensing authorities. Licensing authorities should have the power to impose immediate bans on exports of non-listed items due to actual or potential risks to human rights. Lastly, the EU export regulation framework should require every licensing authority in the EU to publicly and regularly disclose information that relates to authorisation decisions, including information on exports volume, nature, value and destination of the intended export of listed digital surveillance items for which an authorisation has been requested and on authorisation processes of non-listed digital surveillance technologies under the emergency brake procedure (see Chapter 5). If the above is not implemented, Amnesty International calls for a moratorium on the sale and transfer of surveillance equipment until a proper human rights regulatory framework is put in place.

TO THE COUNCIL OF THE EUROPEAN UNION, THE EUROPEAN PARLIAMENT AND THE EUROPEAN COMMISSION:

1) **Secure in the text of the Recast Dual Use Regulation the commitment of the EU to uphold and promote respect for human rights and to contribute to the protection of human rights** as stipulated in Article 2, Article 3 (5) and Article 21 of the Treaty of the EU.
2) **Define the scope of the Recast Dual Use Regulation in a technology-neutral manner in order to ensure that present and future digital surveillance technologies can be brought under it**. The following criteria should determine the definition of cyber-surveillance technologies. The technologies may consist of hardware, software and related services; could be used in connection with the violations of human rights or the commission of violations of human rights law or international humanitarian law; and are designed to enable covert and non-covert surveillance by and of digital systems with a view to monitor, extract, collect and/or analyse data, including biometric surveillance technologies.
3) **Establish expeditious procedures to put new forms of digital surveillance items on the control list** that can be initiated by member states, a group of member states or the institutions of the European Union, without

depending on surveillance companies for flagging the human rights risks. These procedures must allow for human rights risks to be addressed swiftly and efficiently as soon as a Member State or the EU institutions become aware of the risk.

4) **Include the obligation for licensing authorities that decide on an authorisation of exports of digital surveillance technologies** to take into account the occurrence of domestic and international violations of human rights law, fundamental freedoms and international humanitarian law in the country of final destination and/or by the end-user and/or if the legal framework in the destination country fails to provide adequate safeguards against human rights abuses. An authorisation must be denied when a significant risk is identified that the exported item might be used in connection with human rights violations.

5) **Introduce obligations for companies to identify, prevent, mitigate and account for how they address the actual and potential impacts on human rights** associated with their operations, services and products, as well as the supply chain. The obligation to conduct human rights due diligence must apply equally to all exporting companies, regardless of their size, location or structure. Victims of human rights harm should have access to judicial remedy, followed by adequate sanctions. When a company has identified significant risks to human rights and was unable to mitigate those risks, companies must be obligated to refrain from export and notify the licensing authorities, regardless of whether the item in question is on the export control list or not.

6) **Establish an emergency brake procedure for anticipated exports of non-listed items that pose a significant risk to human rights**.

7) **Include the obligation for licensing authorities in the EU to publicly and regularly disclose the information on authorisation decisions**, including information on export volume and the nature, value and destination of the intended export of listed digital surveillance items for which an authorisation has been requested, and on authorisation processes of non-listed digital surveillance technologies under the emergency brake procedure.

8) **Initiate and prioritize the addition of biometric surveillance items** that pose significant risks to human rights, such as facial recognition technology and ethnicity recognition technology to the EU control list, once the framework has been established.

TO THE EUROPEAN MEMBER STATES:

1) **Ensure that all exports of digital surveillance technologies are scrutinised prior to transfer.**

2) **Deny export authorisation where there is a significant risk that the export in question could be used in connection with domestic and international violations of human rights law**, fundamental freedoms and international humanitarian law in the country of final destination and/or by the end-user and/or if the legal framework in the destination country fails to provide adequate safeguards against human rights abuses.

3) **Ensure adequate mechanisms for domestic legal redress in cases of unlawful surveillance.**

4) **Until the applicability of the Recast Dual Use Regulation and the addition of these items on the EU control list**, impose – pursuant to Article 8 Dual Use Regulation – national authorisation requirements on the export of biometric surveillance items that pose significant risks to human rights, such as ethnicity recognition technology, and prohibit the export of facial recognition technology for identification purposes.

5) **Incorporate human rights due diligence assessments by companies into the licensing process**. For each potential transfer, companies should have to demonstrate that they have thoroughly identified and addressed their actual and potential human rights impacts.

6) **Deny all future export authorisations for export by digital surveillance companies** that are credibly accused of (contributing to) human rights abuses and that refuse to cooperate in addressing the situation.

7) **Ensure that all credible accusations of human rights abuses are thoroughly investigated** and, where appropriate, lead to criminal prosecutions.

8) **Provide regular transparency on authorisation decisions**, including information on export volume and the nature, value and destination of the intended export of listed digital surveillance items for which an authorisation has been requested, and on authorisation processes of non-listed digital surveillance technologies under the emergency brake procedure.

9) **Share all relevant information about human rights risks with licensing authorities** in other EU member states, and when confronted with information about the human rights risks of digital surveillance technologies of a specific transfer of these items, take appropriate measures to control the export.

TO DIGITAL SURVEILLANCE COMPANIES:

1) **Commit to respect human rights and put in place robust human rights due diligence policies** and processes which cover human rights risks and abuses connected with the use of company products, services and supply chain. Companies have responsibilities, independent of legal obligations imposed by home states, to identify and address the potential and actual human rights risks connected with the use of their products and services, such as digital surveillance items and related servicing contracts.

2) **Identify, prevent, mitigate, and account for the human rights impact** of company operations, products, and services, as well as supply chain, before, during and after transfer. The implementation of human rights policies and processes through due diligence needs to be on-going, proactive and dynamic, covering all aspects of the business relationship and product lifecycle (including end-use). Risks can change rapidly in countries that lack a legal framework that adequately protects human rights or countries that are experiencing conflict and internal upheaval, and digital surveillance companies must have policies and processes in place that allow them to adapt and respond to potential and emerging human rights threats. Expectations of compliance with human rights law need to be built into the way commercial contracts are drawn up and then tracked through product transfer and use.

3) **Take action to address human rights risks and abuses.** Once risks or abuses are identified, they need to be addressed through concrete actions. These could include consulting with relevant stakeholders and applying leverage to clients, e.g. refraining, threatening to suspend, suspending or ceasing supply.

4) **Publicly communicate risks that are identified and how they are being addressed in the fullest way possible.** Companies should be as transparent as possible about their human rights impacts and the measures they are taking to identify and address them. This must include information on the company's policies and processes and how it has identified and addressed specific human rights risks and abuses arising in its operations. It must also include regular updates – particularly in relation to situations of heightened risk, such as countries involved in armed conflicts or internal upheaval or countries that lack adequate human rights protection within their jurisdiction. When a company has identified significant risks to human rights and was unable to mitigate those risks, companies must notify the licensing authorities, regardless of whether the item is question is on the export control list or not.

5) **Refrain from lobbying in favour of relaxation of licensing requirements** where such a relaxation poses a risk of increased human rights abuses or against initiatives which could reduce surveillance-related abuses. In their efforts to respect human rights, companies should strive for policy coherence and not undermine states' abilities to meet their own human rights obligations.

6) **Enable effective remedies where necessary.** If a company's product does contribute to human rights violations or serious violations of international humanitarian law, the company must endeavour to provide or facilitate prompt and effective remedy, including through reparations such as restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition.

TO THE CHINESE AUTHORITIES:

1) **Adopt legislation that protects the right to privacy, in line with international human rights law and standards, and ensure effective implementation.** Ensure that any legal provisions to protect national security, including those that allow for interference with the right to privacy, are clearly and strictly defined, and conform to international human rights law and international standards.

2) **Refrain from indiscriminate mass surveillance. Ensure that state surveillance projects are in line with international human rights law and international standards.** Establish effective regulatory safeguards, and ensure surveillance serves a well-defined legitimate aim and meets the standards of necessity, legality, and proportionality. Ensure that no surveillance practices are conducted without a reasonable suspicion of involvement in internationally recognised offences, a possibility to 'opt out' or the awareness of individuals. Ensure adequate mechanisms for domestic legal redress in cases of unlawful surveillance.

3) **Halt the targeted discriminatory surveillance of the Uyghur population.** Ensure that any manner of targeted surveillance is in line with international human rights law and standards. Ensure that targeted surveillance is always based on a reasonable suspicion of involvement in internationally recognised offences, in accordance with the law, is strictly necessary to meet a legitimate aim, and is conducted in a manner that is proportionate to that aim and non-discriminatory.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH
amnesty.org

4)

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL

OUT OF CONTROL

FAILING EU LAWS FOR DIGITAL SURVEILLANCE EXPORT

Digital surveillance technology, such as facial recognition, affect the right to privacy, fair-trial rights, the freedom of assembly, speech and religion and the right to equality and non-discrimination. European companies have been repeatedly found to provide surveillance technologies to third countries with poor human rights records. This report uncovers that EU companies sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus. In some cases, the export was directly for use in China's indiscriminate mass surveillance programmes, with the risk of being used against Uyghurs throughout the country.

The current European Union export regulation framework fails to protect human rights. Amnesty International calls upon the European Union to include all digital surveillance items under its regulatory framework, strengthen the human rights considerations in the licensing decisions, introduce 'emergency brake' procedures to regulate and prevent export of non-listed items with significant risks for human rights, ensure all companies are obligated to conduct human rights due diligence, and enhance transparency of the licensing decisions. Proposed measures aim to minimise the contribution of the EU and the European surveillance industry to human rights violations elsewhere in the world.

INDEX: EUR 01/2556/2020
SEPTEMBER 2020
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL