Universiteit van Amsterdam

IViR (Institute for Information Law)

The new rules for export control of cyber-surveillance items in the EU

June 2021

Institute for Information Law (IViR)
University of Amsterdam

This report has been commissioned by
the Dutch Ministry of Foreign Affairs.
It has been carried out in full compliance with
the Declaration of Scientific Independence of the
Royal Netherlands Academy of Arts and Sciences.

Institute for Information Law
Faculty of Law
University of Amsterdam
Nieuwe Achtergracht 166
1018 WV Amsterdam

The new rules for export control of cyber-surveillance items in the EU

O.L. van Daalen
J.V.J. van Hoboken
M. Koot
M. Rucz

June 2021
Amsterdam

Contents

1 Introduction

1.1 Introduction and main question

During the Arab spring uprisings, the world's eye was cast on how regimes in power used technologies from European companies to monitor and repress dissent. It was revealed that some of these regimes were using interception technologies from European firms for large-scale surveillance.[1]

Later on, it became clear that these reports were only scratching the surface: revelations on how authoritarian regimes and private organisations are using foreign technologies to spy on people regularly make the news. Saudi Arabia is suspected of hacking phones of its opponents using Israeli-built software – including prominent dissident Khashoggi, who was later murdered in the Saudi Arabian consulate in Istanbul.[2] More recently, the military staging a coup in Myanmar uses powerful tools to hack devices, intercept communications and surveil demonstrations – tools which are reportedly provided by foreign firms, including companies from Europe.[3] Reports have also shown that European companies have exported digital surveillance tools including facial recognition software to Chinese public authorities, that are allegedly used to track and discriminate against the Uyghur population.[4]

Momentum for the regulation of international trade in these technologies as a result has grown over the past decades. This has led to the adoption of export control for specific technologies, such as interception technologies and hacking software, within international export control regimes. Still, these measures only covered a limited set of tools.

In response to calls for broadening the scope of export controls to include more focus on surveillance technologies, the European Union (EU) in 2021 amended its regulatory framework on export control of so-called "dual-use items" – items which can be used for military and non-military purposes. In its amended Dual-Use Regulation (also called the Recast Dual-Use Regulation), the EU has defined a new category of items, "cyber-surveillance items", to which a new regulatory framework applies.

This regulatory framework brings into focus two important challenges for governments and organisations dealing with the export of surveillance technologies. First, export control rules traditionally focus on items which are described in a detailed, technical manner, enumerated in so-called control lists. This new category of cyber-surveillance items, however, is defined partly in non-technical terms – emphasising the capability for "surveillance", a concept strongly related to human rights. Some of the items already defined in the control lists should be considered such cyber-surveillance items, but this open-ended, human rights-related definition also allows for other kinds of non-listed technologies to fall within the purview of the new framework.

As a result, a broad range of digital technologies which in their use can impact human rights may in theory fall within the scope of this new regulatory framework. While many of these technologies can in practice not be easily used to violate human rights, others may be more suited for that purpose. Drawing the line between the two is important, however, not only because it is a necessary condition for triggering

1 European Parliament Directorate-General for External Policies, 'After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy' (July 2012).
2 David D. Kirkpatrick, 'Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says' (New York Times, 2 December 2018). Available at: https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html?searchResultPosition=1.
3 Hannah Beech, 'Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown' (New York Times, 1 March 2021). Available at: https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.
4 See e.g.: Amnesty International, 'Out of Control: Failing EU Laws for Digital Surveillance Export' (2020).

the authorisation requirement. It is also important because the regulatory framework for cyber-surveillance items introduces a due diligence obligation on the part of the exporter, extended co-ordination and transparency obligations between member states and a competence for member states to lower the threshold for when an export authorisation is required.

The second challenge is related to this authorisation requirement. As discussed above, export rules traditionally work with control lists in which specific items are defined. For these items, export authorisation is required, and governments will assess the envisaged use by the recipient when handling authorisation requests. For this category of newly defined cyber-surveillance items, however, the authorisation requirement *itself* depends on the envisaged use: where these items are or may be intended for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law, an export authorisation is required. The question is how this condition should be applied.

Against this background, we answer the following research question:

> Which kind of items fall within the scope of the term "cyber-surveillance items" under the Recast Dual-Use Regulation, and which criteria can be used to determine whether these items are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law?

For the purposes of our analysis, we have picked five kinds of technologies which warrant particular attention. Three of these are new to export control: facial and emotional recognition software, location tracking technologies and software which is used to analyse publicly available information. And two kinds of technologies already fall within the scope of export control, at least partly: communications interception technologies and intrusion software. We selected these five because they represent a diverse range of surveillance tools, which allows us to illustrate the complexities in applying the new rules, and because for some of them, there have been calls to curtail their export for human rights reasons.

1.2 Outline and summary of the report

We answer the main question in three parts. In chapter two, we focus on the potential scope of the term "cyber-surveillance items" and the role of the reference to human rights in the new regulatory framework. This primarily involves an analysis of the legislative history of the regulatory framework. But this regulatory framework should also be understood in the context of internal EU policy relating to surveillance technologies, and how EU external trade policy and foreign policy of its member states is shaped by human rights. The goal of this chapter is to gain an initial understanding of the scope of the new regulatory framework, which principles should be applied when interpreting the new framework and how this framework is positioned in broader EU policy.

The next chapter is dedicated to the role of human rights law and humanitarian law in the new regulatory framework. One part revolves around the meaning of the terms used to determine whether an authorisation requirement applies. As noted above, this is the case where the items in short are, or may be used for "internal repression", "serious violations of international human rights" and "international humanitarian law". These terms are already being used in the context of the export control of military items, and we draw from the guidance from that domain. The other part relates to European case law on surveillance and human rights, which is relevant for the understanding of the scope of "cyber-surveillance items".

These two legal chapters lay the groundwork for the next chapter, in which the five types of surveillance technologies are described. Three types of technologies are new to export control: facial and emotional

recognition, location tracking and open-source intelligence technologies. Two technologies are already subject to export control, because these are described in detail in the control-lists: communications interception technology and intrusion software. This chapter is intended to gain a better understanding of the characteristics of these technologies and of the challenges in their regulation.

These three chapters are then used as input for the last chapter, where we discuss the considerations which are relevant to determine whether certain technologies fall within the new regulatory framework for cyber-surveillance items. The main conclusions are:

- The new framework introduces a new set of rules relating to the export of cyber-surveillance items. It imposes an authorisation requirement for the export under certain circumstances, and it imposes a due diligence requirement on the part of the exporter to assess the risk that their items will be used for internal repression, serious violations of international human rights or international humanitarian law. It also creates a system for co-ordination and consistency between the member states with regard to the export of these items and introduces a new transparency obligation with regard to the export of these items outside of the EU. And lastly, it introduces the possibility for member states to lower the threshold for export authorisation on the basis of due diligence findings. Thus, it is important to determine whether something falls within the scope of the definition of cyber-surveillance items.

- We argue that this term should be understood in light of the aim of the new regulatory framework, which is to prevent human rights infringements. It should be interpreted to encompass technologies whose design includes particular features to covertly surveil natural persons by collecting and using data from information and telecommunications systems. Importantly, this excludes two kinds of items: those which are aimed at the damaging of systems or jamming of communication, and those which do not gain data "from" systems.

- Whether a technology has particular features to covertly surveil natural persons – in other words, whether it has the potential for human rights infringement – should be understood in light of the European human rights case law on surveillance. This is answered more easily for surveillance technologies which are already on the control list, such as communication interception technology and intrusion software. Here, the question is primarily whether the description in the control lists maps to the precise definition of cyber-surveillance items. For technologies which are not yet subject to the control list, this requires an assessment taking into account the criteria set out by the European Court of Human Rights and the European Court of Justice in their surveillance case law. These criteria include the nature of the data being processed, the potential for indiscriminate use, the question whether the data is processed automatically, the possibilities for accessing the data and the security of the system.

- Here, EU domestic policy plays a role as well. Where it is clear from domestic policy that a certain technology allows for potentially problematic surveillance, this will also have to be taken into account when determining whether this technology falls within the definition of cyber-surveillance items. This will often be the case, given the broad definition. The recent EU policy developments on restricting artificial intelligence for biometric surveillance are an example of this.

- Human rights are also relevant in assessing whether authorisation is required for the export of a cyber-surveillance item. This depends on whether items are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law. For this assessment, there already exists detailed guidance in the context of the export control of military items.

Given the identical terminology used, this guidance should also be considered relevant for the interpretation of these terms in the context of the export of cyber-surveillance items.

- All of the five kinds of technologies we discuss potentially fall within the definition of cyber-surveillance items, primarily because of the sensitivity of the data being processed and the possibility to apply the technologies indiscriminately. Exporters may take measures to prevent certain uses, for example to prevent application at scale, but such measures can generally be circumvented.

- We therefore conclude that the due diligence obligations of companies exporting technology which may fall within the definition of cyber-surveillance items, should be read broadly to require the performance of a human rights impact assessment with regard to the export of an item. In this assessment, the exporter must analyse the capability for human rights infringing surveillance of a technology, in addition to the risk that it may be used for these purposes by a certain end user. This human rights impact assessment should also assess the efficacy of the technical and organisational measures taken to prevent human rights infringements. Where an exporter concludes an item does not fall within the scope of the definition of cyber-surveillance items, it shall also document this.

- This also makes it important for the European Commission to publish guidelines on the basis of which such a human rights impact assessment can be performed, in line with Article 5(2) and Article 26 of the Recast Dual-Use Regulation. These will also be relevant for the determination of whether non-listed items should be considered cyber-surveillance items. We suggest to then also harmonise the interpretation of the term "specially designed" across the EU.

- Lastly, member states under the Recast Dual-Use Regulation have room for adopting legislation which strengthens the authorisation requirement for non-listed cyber-surveillance items. Given the broad scope of the definition of cyber-surveillance items, this may include the export of certain facial and emotion recognition technologies outside of the Netherlands.

1.3 Methodology

This report is based on a combination of desk research and expert interviews. In our research we have used available online sources and have held interviews with experts in this field (see the Annex). Before each interview, we have clarified that the information from the interview may be used in the report, but will not be attributed to persons or organisations. Some of the interviewees have shared non-public information with us. Where we base the report on this material, this is mentioned in the relevant references.

2 The regulation of cyber-surveillance items in the Dual-Use Regulation

2.1 The Wassenaar Arrangement and the Dual-Use Regulation

This report is about the use of export controls to prevent human rights abuses in other countries. This is a relatively new phenomenon. Historically, export controls have been primarily used to further the *internal* interests of a country. For example, one important objective of export control has always been to prevent arms falling in the hands of hostile nations: the Republic of the Netherlands during the Eighty Years' War already required a license for the arms trade to foreign countries.[5] Other internal interests can also lead to export restrictions. The European Commission's threat to restrict the export of AstraZeneca's vaccine from the EU was for example spurred by internal public health reasons.[6]

The origins: COCOM and the Wassenaar Arrangement

One of the most important contemporary export control instruments, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA), belies the military roots of export control. The WA is the successor to the Coordinating Committee for Multilateral Export Controls (COCOM). COCOM was founded in 1950 in the wake of the Second World War, with the goal to curtail exports from the West to the Eastern bloc. It was an informal agreement: its members undertook to adopt national export legislation which would restrict the export of those items listed by COCOM.

As the tension between the Western and Eastern bloc declined, COCOM was eventually replaced in 1996 by a new regime, the WA. The WA is open to all countries, and countries from the Eastern bloc such as the Russian Federation, the Czech Republic, Hungary, Poland, and the Slovak Republic participated from the outset, signalling the new nature of this agreement. Since its adoption, the WA has developed into a global instrument: it now has 42 participating states.[7] Still, some countries which are known to have a strong surveillance industry, such as Israel and China, are not a participant.

Participants to the WA agree to control the export of specific items, which are described in an attachment to the WA: the so-called "control lists" mentioned in the introduction. The participants to the WA update these lists every six months. The WA has two lists: one for military items (the Munitions List), and one for items which can be used for military and non-military, or "civil" purposes (the Dual-Use List).

This distinction is made because, for some kinds of items, such as bombs, torpedoes and aircraft missiles, there is no other purpose than a military purpose. For other items, on the other hand, the purpose may differ according to the context. For example: encryption technology may be used by armies to communicate securely (a military purpose), but may also be used by ordinary citizens to protect their information (a non-military purpose). An export control regime which would always treat these kinds of technologies as military technologies would not do justice to their civil use – hence the distinction.

The control lists to the WA contain detailed descriptions of items which the participating countries are obliged to place under export control via their national legislation. For example, computers which are

5 Joop E.D. Voetelink. (2017). *Exportcontrolerecht: Een verkenning*. Militaire Spectator, 186(9), 376-390., p. 379. Available at: http://www.militairespectator.nl/thema/recht/artikel/exportcontrolerecht.

6 Daniel Boffey and Jessica Elgot, 'EU to widen criteria for possible Covid vaccine export bans' (The Guardian, 23 March 2021). Available at: https://www.theguardian.com/society/2021/mar/23/eu-expand-criteria-used-decide-block-covid-vaccine-shipments.

7 See the list of participating countries at https://www.wassenaar.org/.

specially designed to be rated for operation "at an ambient temperature below 228 K (-45°C) or above 358 K (85°C)" should be placed under export control by the participating states, unless they are specially designed for "civil automobile, railway train or 'civil aircraft' applications".[8] These lists are updated periodically and usually copied verbatim by the participating states in their relevant legislation. For the EU, while the Munitions List is transposed nationally, the Dual-Use List is transposed on the EU level.

The Dual-Use Regulation

In the EU, the export control of dual-use items is regulated through the so-called Dual-Use Regulation. The creation of an internal market lies at the heart of the European Union, and export controls at the member state level are potentially at odds with this objective. As a result, the Council already agreed in 1994 on EU-wide rules relating to the trade in dual-use items, even though the EU as such is not a participating entity to the WA (most of its member states are). This instrument was based on the principle that dual-use goods should be able to circulate freely *within* the European Union, but that the *export* of those items outside should be controlled.

The Dual-Use Regulation at a minimum transposes the lists under the WA. The European Union may, however, also provide for additional rules relating to the export of certain dual-use items. It did so with regard to the topic of this study – the export control of cyber-surveillance items – in its most recent update of the Dual-Use Regulation in 2021: the Recast Dual-Use Regulation.[9] This amended regulation is the outcome of a process which was started by the European Commission in 2016, when it published its proposal.[10] It then took almost four years for these institutions to reach a compromise, partly because of disagreement on the regulation of these specific items. We describe this further in the following sections.

2.2 The political debate surrounding the introduction of cyber-surveillance-items in the Recast Dual-Use Regulation

During the Arab Spring uprisings around 2010 and 2011, leaders of the region vehemently pursued protest organisers, human rights defenders and journalists, partly by using technology to censor, monitor and surveil telecommunications and the internet. The complicity of the private surveillance industry soon became clear, with reports showing how European technology companies had sold surveillance technologies to regimes where they were used to crack down on dissent.[11]

In response to the public outcry that ensued from the reports demonstrating the collaboration between European technology companies and the Syrian regime, the EU moved to extend the sanctions imposed on Syria, adding restrictions on export of surveillance equipment that could be used to monitor the internet and telecommunications.[12] Similar restrictions on the export of surveillance technologies within the EU's sanction regime have later also been imposed on Iran and Venezuela.[13]

8 Wassenaar Arrangement Control List, 4.A.1.a.1.
9 Regulation 2021/... of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). At the time of writing of this report, the Regulation was not yet published in the Official Journal of the EU.
10 European Commission, 'Proposal for a regulation of the European Parliament and the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)' COM(2016) 616 final (28 September 2016).
11 European Parliament Directorate-General for External Policies, 'After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy' (July 2012).
12 Council Decision 2011/782/CFSP of 1 December 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP, Official Journal of the European Union (2 December 2012).
13 Council Decision 2012/168/CFSP of 23 March 2012 amending Decision 2011/235/CFSP concerning restrictive measures directed against certain persons and entities in view of the situation in Iran, Official Journal of the European Union (24 March 2012); Council Decision 2017/2074/CFSP of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela (14 November 2017).

However, efforts to grapple with the private surveillance industry's dealings with repressive regimes have been substantially complicated by the lack of transparency and limited public information on this market. What we know publicly, we know mostly from civil society organisations, investigative journalists and academics.[14] For example, Al Jazeera's investigation, *Spy Merchants*, provided a unique glimpse into the operations of certain surveillance companies, and their willingness to export their products to the highest bidder, regardless of export restrictions.[15] Hiding the real purpose of surveillance equipment from required export documentation, and routing the export via a third country with more lax controls, have enabled technology companies to circumvent export regulations and EU sanctions in place. Al Jazeera's investigation shows, for example, an Italian company which is open to selling an internet interception system to the Iranian government. While the official from the company indicates that he is aware of the export restrictions in place for Iran in relation to such surveillance products, he insists this is something that his company "can manage."

In response to the increasing evidence of European technology companies facilitating surveillance by regimes with problematic human rights records, the European Parliament repeatedly emphasised the need to tighten export controls through an update to the Dual-Use Regulation.[16] Simultaneously, on the international level, the WA was updated in 2012 and 2013 to include interception, intrusion and IP network surveillance technologies on its list of controlled items (see further section 5.1). For the European Parliament this was not enough, however, and it insisted in 2015 in its Resolution on Human Rights and Technology in Third Countries that even with the WA updates, the EU dual-use framework is "still very incomplete [...] when it comes to the effective and systematic export control of harmful ICT technologies to non-democratic countries."[17] In 2015, Germany furthermore amended its own national control list, imposing licensing requirements on the export of so-called monitoring centres and data retention systems, with the explicit purpose of preventing the abuse of communication surveillance technologies for internal repression.[18]

Although this was a welcome development, the European Parliament continued to insist that a common European approach on the topic was desirable, for example in its Resolution on the European Defence Union adopted in 2016.[19] At the same time, civil society organisations represented in the Coalition Against Unlawful Surveillance Exports advocated for a uniform EU approach to export control of "strategically chosen, well-defined surveillance technologies" with human rights safeguards incorporated in the Dual-Use Regulation.[20]

The Commission in 2016 attempted to address these calls in a proposal for a recast version of the Dual-Use Regulation. The Commission's proposal was based on a two-pronged approach to cyber-surveillance items. On the one hand, it proposed to regulate "cyber-surveillance technology" not on the control list, that may be used to commit violations of human rights or international humanitarian law via a catch-all clause. Furthermore, it placed "monitoring centres" and "data retention systems" on the control list, following

14 See also: United Nations General Assembly, 'Surveillance and human rights', A/HRC/41/35, para. 1.
15 'How the 'Dual-Use' Ruse is Employed to Sell Spyware' (Al Jazeera, 10 April 2017). Available at: https://www.aljazeera.com /features/2017/4/10/how-the-dual-use-ruse-is-employed-to-sell-spyware.
16 See e.g.: European Parliament, 'Resolution of 8 September 2015 on Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries (2014/2232(INI))' (8 September 2015); European Parliament, 'Resolution of 17 December 2015 on the Annual Report on Human Rights and Democracy in the World 2014 and the European Union's policy on the matter (2015/2229(INI))' (17 December 2015); European Parliament, 'Resolution of 22 November 2016 on the European Defence Union (2016/2052(INI))' (22 November 2016).
17 European Parliament, 'Resolution of 8 September 2015 on Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries (2014/2232(INI))' (8 September 2015).
18 Außenwirtschaftsverordnung, § 52b. BMWI, 'Gabriel: Export von Überwachungstechnik wird stärker kontrolliert' (8 July 2015). Available at: https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2015/20150708-gabriel-export-von -ueberwachungstechnik-wird-staerker-kontrolliert.html.
19 European Parliament, 'Resolution of 22 November 2016 on the European Defence Union (2016/2052(INI))' (22 November 2016), paras. 21, 47.
20 Coalition Against Unlawful Surveillance Exports, 'A critical opportunity: Bringing surveillance technologies within the EU Dual-Use Regulation' (June 2015), p. 12.

the German national amendments. The European Commission's proposal was largely supported by the European Parliament proposal of 2018, as will be further discussed in the following section. However, it was subsequently met with significant opposition by the technology industry as well as Member States. The result is thus the outcome of a political compromise, and as we will see in the following section, this has not contributed to its clarity.

A major point of contention was the so-called 'EU autonomous list' - the introduction of cyber-surveillance items which were not on the control lists of the WA. A number of EU member states expressed their disapproval of the idea of departing from the control list of the Wassenaar Arrangement, and instead asserted that if export regulation of cyber-surveillance items is needed, this should take place at the multilateral level.[21] It was contended by opponents that an autonomous list approach would place the EU at a competitive disadvantage and seriously stifle the European technology sector. Industry groups have also warned that the autonomous list approach would "create a poor environment for digital services in Europe" and thus incentivise technology companies to take their business outside the EU.[22]

The vagueness of the catch-all clause was a further key concern during negotiations. Industry lobby groups argued that catch-all clauses generally create undue legal uncertainty for companies.[23] They contended that performing human rights assessments in the context of everyday export practices would pose too big of a challenge for technology companies.[24] Industry groups, furthermore, warned that the imprecise definition of cyber-surveillance items might lead to an overly broad interpretation of the catch-all provision which might inhibit the export of legitimate, essential technologies.[25]

During the trilogue negotiations between the European Commission, the Council and the European Parliament, protracted by heavy lobbying on both sides of the debate, news of the European private surveillance industry doing business with regimes with poor human rights records continued to pile up. In the Netherlands, the Correspondent reported on two Dutch companies selling facial recognition technology, with the capability to recognize emotions and ethnicity, to the Chinese Ministry of Public Security.[26] Amnesty International then followed up on this in 2020, presenting three case studies of technology companies in France, Sweden and the Netherlands exporting facial recognition technologies to Chinese government-related agencies, that form part of the surveillance apparatus of China.[27] This case was a principal catalyst for the political debate that followed in the Netherlands, revolving around the concern that technologies supplied by Dutch companies might be used for mass surveillance and discrimination against the Uyghur minority in China. In response to a parliamentary resolution in 2019 and further pressure in hearings, the Dutch government in 2020 confirmed that it aims to prevent the involvement of (Dutch) companies in the use of cyber-surveillance goods and cyber-surveillance technology in the violation of human rights.[28]

21 'Working Paper on EU Export Control - Recast of Regulation 428/2009' (29 January 2018). Available at: https://euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf; 'Working Paper on 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' (15 May 2018). Available at: https://euractiv.com/wp-content/uploads/sites/2/2018/06/nine-countries-paper-on-dual-use.pdf.

22 Digital Europe, 'European Commission Proposed Recast of the European Export Control Regime - Making the rules fit for the digital world' (24 February 2017), p. 3.

23 Bundesverband der Deutschen Industrie, 'EC Dual-Use - Review of the EC Dual-Use Regulation' (January 2016), p. 5. Available at: https://bdi.eu/media/topics/global_issues/downloads/201601_FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf.

24 Ibid., pp. 6-7.

25 Digital Europe, 'European Commission Proposed Recast of the European Export Control Regime - Making the rules fit for the digital world' (24 February 2017), p. 3.

26 Maurits Martijn, 'Berucht Chinees veiligheidsministerie gebruikt Nederlandse software die emoties leest' (De Correspondent, 12 July 2019). Available at: https://decorrespondent.nl/10307/berucht-chinees-veiligheidsministerie-gebruikt-nederlandse-software-die-emoties-leest/317002092-cae75d58.

27 Amnesty International, 'Out of Control: Failing EU Laws for Digital Surveillance Export' (September 2020).

28 Letter of Minister of Foreign Affairs of 16 July 2020, *Kamerstukken II* 2019/20, 32 735, nr. 309; *Kamerstukken II* 2019/20, 32 735, nr. 308; *Kamerstukken II* 2019/20, 35 207, nr. 27.

Ultimately, in November 2020, the European Parliament and the Council presented their provisional agreement on the Recast Dual-Use Regulation.[29] This provisional agreement was officially accepted as the Recast Dual-Use Regulation in March 2021 by the European Parliament, and in May 2021 by the Council of the European Union.[30] As we will also see in the next section, the control of cyber-surveillance items has been weakened in the compromise text, compared to the position of the European Commission and the European Parliament. Most importantly, cyber-surveillance items were deleted from the definition of dual-use items, halting the Commission's ambitions for an EU autonomous list of items subject to export control. Instead, additional rules for cyber-surveillance items were introduced. Civil society organisations have already expressed their scepticism about the final text´s ability to adequately tackle human rights concerns of surveillance export, signalling that the political debate in respect of export control of digital surveillance technologies is long from concluded.[31]

2.3 The regulation of cyber-surveillance items in the Recast Dual-Use Regulation

Even though the final compromise does not contain an autonomous list of cyber-surveillance items subject to authorisation, it does introduce a new regulatory framework for these items, where under certain circumstances export authorisation is required for these items. We first discuss the interpretation of the term "cyber-surveillance items", and then discuss what the new regulatory framework implies.

2.3.1 Interpretation in light of the Charter of Fundamental Rights

First, however, a note on interpretation. This is the first time that the Dual-Use Regulation contains a definition of items which are described in functional, human rights-oriented terms, instead of more technical terms. This new definition is furthermore not based on an already existing control framework, such as the Wassenaar Arrangement. As a result, member states applying the new regulation will be less able to draw from experience when interpreting these new terms. We contend that the Charter of Fundamental Rights (Charter) is an important tool when interpreting these new rules in the Dual-Use Regulation. All European legislation needs to be read in light of the Charter, but this is especially so in this case, because the new regulatory framework for cyber-surveillance items is intended to curtail human rights abuses (see also section 2.4.2).

2.3.2 Legislative history of the definition of cyber-surveillance items

The definition of cyber-surveillance items has gone through three iterations – first the European Commission, then the European Parliament, and finally the Council of the European Union. As we will see, the European Commission and the European Parliament were somewhat aligned in their position, whereas the Council was almost diametrically opposed.

29 Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) - Confirmation of the final compromise text with a view to agreement' (13 November 2020).

30 European Parliament, 'European Parliament legislative resolution of 25 March 2021 on the 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) (COM(2016)0616 – C8-0393/2016 – 2016/0295(COD))'. Available at: https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2021/03-25/0101/P9_TA(2021)0101_EN.pdf. Council of the European Union, 'Trade of dual-use items: new EU rules adopted' (10 May 2021). Available at: . https://www.consilium.europa.eu/en/press/press-releases/2021/05/10/trade-of-dual-use-items-new-eu-rules-adopted/.

31 'Urgent call to Council of the EU: Human rights must come first in Dual Use final draft' (November 2020). Available at: https://www.accessnow.org/cms/assets/uploads/2020/11/Open-Letter-to-the-Council-Dual-Use.pdf. See also on the political debate regarding the inclusion of cyber-surveillance items in the Dual-Use Regulation: Mark Bromley, 'Export controls, human security and cyber-surveillance technology: Examining the Proposed Changes to the EU Dual-Use Regulation' (SIPRI, December 2017); Machiko Kannetake. (2019). *The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches*, Business and Human Rights Journal, 4(1); Machiko Kannetake. (2019). *The EU's dual-use export control and human rights risks: the case of cyber surveillance technology.* Europe and the World: A law review; European Parliament, 'Report on human rights and technology: The impact of intrusion and surveillance systems on human rights in third countries' (3 June 2015); Maaike Goslinga, 'How European spy technology falls into the wrong hands' (The Correspondent, 23 February 2017). Available at: https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153.

As mentioned above, the idea of the Commission was to introduce a new kind of item, cyber-surveillance technology, for which an authorisation was required under certain circumstances. In the proposal published by the European Commission, the definition revolved around the control of, in short, hacking tools. It referred to items "specially designed to enable the covert intrusion into information and telecommunication systems with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system" (emphasis added).[32]

In the Commission proposal, human rights twice play a role when assessing whether an authorisation is required. The proposal limited the application of the new framework to cyber-surveillance technology which can be used for the commission of serious violations of human rights or international humanitarian law (or which can pose a threat to international security or the essential security interests of the EU and its Member States).[33] Thus, surveillance technology should have human rights-infringing capability. But this capability in itself was not enough to require an export license: export authorisation would only be required for non-listed cyber-surveillance technology if the exporter has been informed that the items in question are or may be intended for serious violations of human rights or international humanitarian law in situations of armed conflict or internal repression.[34] So surveillance tools should not only be capable of infringing human rights, there should also be a risk that they will be used for these purposes, in order for the new framework to apply.

The European Parliament expanded on this. In its version, it maintained the focus on hacking tools, but proposed to extend the definition to items which "can be used in connection with "the violation of human rights" - meaning that the violation need not be "serious".[35] It also broadened the authorisation requirement to include situations where the use was "connected" with violations of international human rights law or international humanitarian law.[36]

The Council, however, deleted the reference to cyber-surveillance items in the provisions altogether because in its view these should already be considered to fall within the scope of "dual use items" and should not be considered an additional category. It only retained a recital, in which it is considered that in order to address the risk that certain non-listed dual-use items may be misused by persons complicit in or responsible for directing or committing serious violations of human rights or international humanitarian law, it is appropriate to control the export of those items.[37] In the proposed recital, the Council borrowed from the original definition of the European Commission, albeit with one important difference: according to the Council, these non-listed dual-use items which may be misused, includes cyber-surveillance items, which are "dual-use items specially designed to enable the covert surveillance of information and telecommunication systems with a view to monitoring, extracting, collecting or analyzing data". The Council, in other words, replaced the term "covert intrusion" with the term "covert surveillance", but relegated the entire definition to the recitals.

32 In a leaked draft proposal by the European Commission in 2016, the definition mentioned "biometrics", "location tracking devices", "probes" and "DPI systems" as examples of such technology, but in the final draft these were removed. However, other examples were still mentioned: mobile telecommunication interception equipment; intrusion software; monitoring centers; lawful interception systems and data retention systems; and digital forensics. See https://euractiv.com/wp-content/uploads /sites/2/2016/07/dual-use-proposal.pdf.

33 Commission Proposal, Art. 2(1)(b).

34 Ibid., Art. 4(1)(d).

35 It also proposed to clarify (i) the relationship between "intrusion", "monitoring", "exfiltrating", "collecting", "analysing", "incapacitating" and "damaging", (ii) that to the extent that these activities are authorised by the owner of the system, they should not be considered problematic and (iii) proposed to exclude certain security research activities from the definition.

36 European Parliament Report, Amendment 32.

37 Council Mandate, Rec. 5.

2.3.3 Final definition of cyber-surveillance items

Ultimately in trilogue, the different institutions came to a final text, where a new category of "cyber-surveillance items" is defined as:[38]

> "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems".

Two examples are mentioned in the recitals which are relevant to the interpretation of this definition.[39] One example which according to the recitals should be considered to fall within the rules are items "specially designed to enable the covert intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from these systems". Items, on the other hand, which are "used for purely commercial applications such as billing, marketing, quality services, user satisfaction, network security etc." are considered to generally not fall within the scope of the rules. These explanations have only little value for interpretation, because many of the terms used in these recitals, such as "information and telecommunications systems" and "monitoring, extracting, collecting or analysing data", are also used in the definition itself. The question thus remains open what the scope of the definition entails. We discuss this in the next sections.

2.3.4 Interpretation of the different elements

As becomes clear from the legislative history, the scope of the final definition revolves around four important elements:

- "covert surveillance";
- "monitoring, extracting, collecting or analysing data";
- "from information and telecommunication systems"; and
- "specially designed"

We discuss these below.

Surveillance

First, the question is what should be considered "covert surveillance". There are two aspects to this question: what does the term "surveillance" entail, and what is the relevance of the qualifier "covert"?

As to the term "surveillance": this is a word heavy with meaning. It is used often in a variety of contexts, from philosophers arguing about the role of government towards its citizens, to activists protesting tracking by commercial companies. Merriam-Webster defines it as: keeping a close watch over someone or something (as by a detective).[40] Cambridge defines it as: the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected.[41] This relatively narrow understanding of surveillance can be contrasted with how the subject is studied in academia, where "surveillance studies" is the topic of various books and courses. As an example, one author defines it as "regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these", where a "central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category".[42]

38 Recast Dual-Use Regulation, Art. 2(20) and Rec. 2.
39 Recast Dual-Use Regulation, Rec. 8.
40 See: https://www.merriam-webster.com/dictionary/surveillance.
41 See: https://dictionary.cambridge.org/dictionary/english/surveillance.
42 Gary T. Marx. (2015). *Surveillance Studies*. International Encyclopedia of the Social & Behavioral Sciences, 2nd edition, Volume 23, p. 733-741.

We, instead, propose to interpret the term "surveillance" in the Dual-Use Regulation in the context of case law on human rights, because the new regulatory framework for cyber-surveillance items is aimed at protecting human rights. In the context of the new rules, the term "surveillance" should thus serve to distinguish between technology which allows for practices which impinge on human rights, and technology which does not.

The European courts have over the past decades used this term in a variety of settings where different kinds of information on persons are collected and processed. The European Court of Human Rights in the seminal *Klass*-case (1970) reviewed certain German "surveillance measures", which allowed the government to open and inspect mail and post, read telegraphic messages, and listen to and record telephone conversations – communications surveillance, in other words.[43] In this decision, the Court for the first time developed a framework for assessing measures of secret surveillance. We discuss the framework further in section 3.2.2.

Since then, the Court has repeatedly used the term to review various types of privacy-infringing measures, not only secret surveillance of communications. In *Leander* (1987), it considered the classification of someone as a security risk in a register as a form of surveillance.[44] Similarly, in *Rotaru* (2000), the Court assessed the maintenance of a secret register on someone, under the framework it developed for secret surveillance, specifically classifying the gathering and keeping of personal information as a form of surveillance.[45] The Court has further referred to posting at someone's house as a form of "visual" surveillance, and evaluated the installation of a listening device on a suspect's premises under its surveillance review framework.[46] More recently, in *Uzun* (2010), it has considered location tracking with a GPS-device a form of surveillance (but it concluded that the strict framework for reviewing communications surveillance was not appropriate for covert location tracking).[47] It has also reviewed surveillance by private entities, for example assessing the monitoring by an employer of the communications of an employee under the framework first developed in *Klass*.[48] And it has even provided guidance on the review of legislation of the use of "video"-surveillance by employers and in detainees' cells.[49] The European Court of Justice has not had the chance to rule on a similar number of cases on this topic, but where it did, it uses the term "surveillance" also in a broad way.[50]

Given that the term is used in in the Dual-Use Regulation in the context of the prevention of human rights and humanitarian law abuses, the term "surveillance" should be understood in light of the use of the term by the European Court of Human Rights and the European Court of Justice. This means it can refer to a broad range of activities related to the gathering and processing of information on individuals. Such surveillance can not only come from government activities, but also from private actors. This is particularly relevant because in the past, it has been difficult to assess who is behind the use of a certain tool: there are various examples of surveillance tools being used by private interests, where it is not always clear whether there is a link with a government.[51] But to be clear: not all surveillance is a *violation* of human rights. Both Courts have circumscribed the considerations important in determining whether surveillance violates human rights. This case law is further discussed in chapter 3.

43 ECHR 6 September 1978, application number 5029/71 (*Klass*), para. 17.
44 ECHR 26 March 1987, application number 9248/81 (*Leander)*, para. 60.
45 ECHR 4 May 2000, application number 28341/95 (*Rotaru*), para. 47 and further, as well as para. 57. See later: ECHR 6 June 2006, application number 62332/00 (*Segerstedt-Wiberg v. Sweden*).
46 ECHR 25 September 2001, application number 44787/98 (*P.G. and J.H. v. the United Kingdom)*, para. 37; and Khan, para. 22 and further.
47 ECHR 2 September 2010, application number 35623/05 (*Uzun*), para. 66; ECHR 8 Februari 2018, application number 31446/12 (*Ben Faiza*).
48 ECHR 5 September 2017, application number 35623/05 (*Barbulescu*), para. 120.
49 ECHR 17 October 2019, application numbers 1874/13 and 8567/13 (*López Ribalda and Others v. Spain);* ECHR 2 July 2019, applications numbers 27057/06 and 2 others (*Gorlov and others v. Russia*).
50 CJEU 6 October 2020, C-623/17 (*Privacy International*), para. 71; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2*), para. 100; CJEU 8 April 2014, C-293/12 and C-594/12 (*Digital Rights Ireland*), para. 38.
51 See for example the investigations of CitizenLab into the use of intrusion software in Mexico: https://citizenlab.ca/tag/mexico/.

Importantly, what should not be considered "surveillance" under this definition are activities aimed at the distortion of information, jamming of communications and damaging of systems. This is because in the initial definition of the European Commission, technologies used for "incapacitating or damaging the targeted system" were also included in the definition. In the final version, these two activities were removed.

Covert surveillance

The next question is whether the term "covert" has any special significance: does surveillance which is not "covert" fall outside of the definition? This is relevant, because there are examples of surveillance taking place *overtly* - cameras to surveil people in public spaces, for example – which may still entail a human rights violation.

The term "covert" has been present in connection with the term "surveillance" and "intrusion" throughout the various iterations of the definition, but without further explanation. Most of the relevant case law under the Convention and the Charter furthermore revolves around surveillance of which the complainant is not aware - perhaps only later, after being notified (see also section 3.2.2). The European Court of Human Rights has in one case attached importance to the fact that information was gathered *overtly*, arguably considering that a lower threshold for review should apply, but it in the same case suggested that the framework for covert surveillance should also be applied to overt surveillance, given the ambiguity of the states' powers in this case.[52]

Different possible interpretations exist with regards to the meaning of 'covert' in the Recast Dual-Use Regulation. A narrow interpretation would imply that surveillance is covert when the person targeted is unaware that she is being monitored. According to a less narrow interpretation, the emphasis would be on whether the person targeted has consented to the surveillance. A further possible interpretation is that surveillance is covert when the collection of personal data leaves no traces from a technical perspective.

We argue that a different interpretation should apply. Because the goal of the new rules is to prevent human rights violations, and these can also take place if a person is aware in general terms that surveillance is taking place, this term should arguably be read broadly: surveillance is "covert" with regard to a person if that person does not know *whether* and *how* information on her is being used to target her specifically.

Monitoring, extracting, collecting or analysing

The third question is what activities exactly fall under the terms "monitoring, extracting, collecting or analysing". These four activities were already present in the different iterations of the definition, but they were not supported by an explanation and did not garner discussion. In the initial proposal of the European Commission, these activities were linked to "covert intrusion" with a view to monitoring, extracting, collecting and analysing data and/or incapacitating or damaging the targeted system. In the final proposal, these activities were linked to the "covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems". The terms "monitoring", "extraction" and "analysis" have also been used in control lists in the context of controlled surveillance technologies under the WA.[53]

It is likely that these terms should be read broadly to include various steps in the processing of information in a system. Part of these steps relate to the gathering of data on persons: "extraction" and "collection" arguably fall under this header. And the other parts of these steps are more related to the subsequent use of the collected data: "monitoring" and "analysing" arguably fall under this header. Together, these steps

52 ECHR 24 October 2019, application number 43514/15 (*Catt v. the United Kingdom*), para. 114.
53 See e.g.: Wassenaar Arrangement, 5.A.1.f.1 and 2, 5.A.1.j.

encompass a broad range of activities related to the collection and use of data on persons from certain systems. But what systems, exactly?

From information and telecommunication systems

Here, the next element becomes important: the meaning of "from information and telecommunication systems". The term "telecommunications systems" is used throughout the WA – it has even one chapter devoted to it. These arguably should include all systems which convey information over a distance – which is the literal meaning of "telecommunications". The term "information systems" is not used in the WA, but arguably should be read to include all systems which process information, excluding telecommunications systems. Together, these two concepts include a broad range of systems transmitting or processing information.

But the term "from" significantly restricts the scope of the entire definition. Because the monitoring, extraction, etc. is focused on gaining and processing data "from" the system, this means that the collection of "offline" data does not fall within the definition. At the same time, there is a fine line between the initial collection and subsequent analysis.

Let's illustrate this with an example: the filming of people with cameras from public spaces. Under this reading, cameras collecting information from public spaces are not covered by the definition of cyber-surveillance items, because information is not collected from these systems. One could perhaps argue that a camera is an "information system", and that technologies which connect to these cameras to monitor or analyse data "from" these cameras should be considered to fall within the definition. That would be quite a stretch, however, as the actual "surveillance" (e.g. the filming of people in public spaces) is not done by collecting data "from" a system – it is done by collecting data from a public space. To argue otherwise, would be stretching the definition beyond recognition.

This is different, however, with regard to technologies which are used to analyse pictures collected *with* such cameras. These technologies could indeed be considered to "analyse" data collected with this surveillance, and thus fall within the scope. For example, software designed to scrape pictures of faces on the internet could fall within the scope of this definition, even if these pictures were initially collected with cameras that do fall outside the definition. We discuss this further in chapter 5.

Specially designed

And lastly, a central question is whether the items are "specially designed" for this. This term has been used for decades. It is already used in the COCOM control lists: under the 1958 COCOM lists, for example, equipment "specially designed" for the production of certain gases in liquid form are already subject to control. In the WA and related export control instruments it is also used abundantly.[54]

These terms have been explicitly defined in the Guidelines for the Drafting of Lists under the WA in 1996, which was later revised in 2007/2008.[55] Under the 1996 Guidelines, "specially designed" means "any object whose design includes particular features to achieve some particular purpose. This will typically involve extensive research and development activity." This is juxtaposed to the term "designed", which means "any object whose design is general in nature to achieve some particular purpose. Typically extensive research and development will not be involved." There are also more recent Guidelines from 2007/2008, but these are not publicly available. We assume these guidelines have remained essentially the same. Evidence which could be used for this assessment are, for example, the context within which the product is developed, as well as the marketing materials.

54 See the Revised List of Goods Subject to Embargo 1958: https://www.scribd.com/document/19647281/CoCom-Lists-1958.
55 Reproduced in Appendix G. See: https://core.ac.uk/download/pdf/288283595.pdf.

We understand that the interpretation of this term is considered to fall within the competence of each member state, and thus may vary across member states. This term is already important for the interpretation of listed items, but will likely gain even more significance in the context of the new rules on cyber-surveillance items. Items on control lists have traditionally been defined in a detailed way, which means that the scope of the definition of each item is already smaller, leaving a limited role to play for the design-criterion to distinguish between controlled and non-controlled items.

As a result of the open-ended definition of cyber-surveillance items under the Dual Use-Regulation, however, the importance of the design-criterion has increased. Since the wide scope of the definition in theory catches a variety of technologies, it becomes more important to distinguish between technologies which in theory can be used for surveillance, and those which have actually been built with that goal in mind.

Thus, we propose to apply a harmonised understanding of the "specially designed"-criterion for the interpretation of cyber-surveillance items across the EU, also aligning with the guidelines developed in the context of the WA. Assuming these WA guidelines have not changed since 1996, this means that items which are "specially designed" to enable the covert surveillance of natural persons, are items whose design includes "particular features to achieve" such surveillance. We discuss in section 3.2.2 what such features could be.

So summing up: the definition of cyber-surveillance items should be interpreted to encompass technologies whose design includes particular features to covertly surveil natural persons by collecting and using data from information and telecommunications systems. We discuss in chapter four the technologies which potentially fall within this definition.

2.3.5 Rules with regard to cyber-surveillance items

As discussed above, specific cyber-surveillance items have in the past years already been added to the control list under the WA and the Dual-Use Regulation. For these particular items, an authorisation is required for their export.[56] We discuss in chapter five which of these items can be considered cyber-surveillance items under the Recast Dual-Use Regulation. But for non-listed technology which falls under the definition of "cyber-surveillance items", an extended framework is created, complementing already existing rules for the export of dual-use items:[57]

- Firstly, under specific conditions, non-listed exports of cyber-surveillance items are subject to authorisation. This is the case if the exporter is "*informed*" by the competent authority that certain cyber-surveillance items "are or may be intended, in their entirety or in part, for use in connection with *internal repression* and/or the commission of *serious violations* of *international human rights* and *international humanitarian law*" (emphasis added). Here, two aspects are relevant. First: when should an exporter be considered to be "informed", because only this triggers the authorisation requirement. This mechanism that being "informed" triggers export control can be found already in the earlier Dual-Use Regulation.[58] In practice, governments will take an administrative decision regarding the need for an authorisation and "inform" an exporter by sending a letter. And second, the question is when there is a risk of use of these items for "internal repression", "serious violations of international human rights" and "international humanitarian law". This is further discussed in chapter 3.

56 Recast Dual-Use Regulation, Art. 3(1).
57 Ibid., Art. 5(1).
58 Dual-Use Regulation (2009), Art. 4.

- As an additional safeguard, if an exporter itself on the basis of its own due diligence is aware that cyber-surveillance items are or may be intended for any of these it uses, it shall notify the competent export authority, which shall then determine whether the export needs to be subject to authorisation. National governments derive an implicit due diligence obligation from this provision. This means that where a company is exporting goods which could fall within the scope of the definition of cyber-surveillance items, they will have to first investigate whether this suspicion is correct. If so, they will then have to review whether the items are or may be intended for any of these uses. And it also has a due diligence obligation when it has received signals that its products might be used for these purposes.

- Lastly, a member state may through national legislation lower the threshold that triggers the authorisation requirement on the basis of due diligence findings of an exporter. While under the Recast Dual-Use Regulation these requirements are triggered when the exporter is aware that a cyber-surveillance item may be used for the purposes mentioned above, this provision grants member states the competence to adopt national legislation that triggers the authorisation requirements when the exporter has grounds for suspecting that an item may be used for these purposes. This specific competence complements the more general power that member states have to prohibit or impose an authorisation requirement on the export of non-listed dual-use items for human rights considerations in general, a power which was already present in earlier versions of the Dual-Use Regulation.[59] This has for example been used by the Netherlands to impose an authorisation requirement for the export of certain chemical dual-use goods to Iraq.[60]

The other part of the framework sets up a *coordination system* between member states with regard to the export control of non-listed cyber-surveillance items:[61]

- Where one member state imposes an authorisation requirement on the basis of the provisions discussed above, it must provide the other member states and the European Commission with relevant information on the requirement, unless the nature or sensitivity of the transaction dictates otherwise. Receiving member states likewise shall give "due consideration" to this information received within thirty working days, which may be extended with another thirty days.

- If all member states are notifying essentially identical transactions to each other, the Commission shall publish in the Official Journal of the European Union information regarding the cyber-surveillance items and, where appropriate, destinations subject to authorisation requirements. This overview shall be reviewed annually by the member states and the European Commission where necessary will update it.

Lastly, the European Commission is already obliged to submit an annual report on the export of items under the Dual-Use Regulation. With regard to (listed and non-listed) cyber-surveillance items, this report must now include "dedicated information on authorisations, in particular on the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications".[62] Because this transparency requirement also covers listed cyber-surveillance items, it is a relevant question which items on Annex 1 fall under this definition. This is further discussed in chapter five.

59 Recast Dual-Use Regulation, Art. 9(1).
60 Regeling goederen voor tweeërlei gebruik Irak.
61 See also: Recast Dual-Use Regulation, Rec. 9 and 10.
62 Recast Dual-Use Regulation, Art. 26(2).

2.4 A human rights informed export control policy

As discussed above, one of the main novelties of the Recast Dual-Use Regulation is the increased emphasis on human rights as a control ground. The Recast Dual-Use Regulation forms part of the EU's so-called Common Commercial Policy, encapsulating all EU policies relating to trade and investment, which is one of the two main dimensions of the EU's external relations (the other being the Common Foreign and Security Policy).

The role of human rights in the EU's external relations is far from clear-cut. In fact, human rights objectives are often at odds with the chief purpose of the Common Commercial Policy. Its driving principle is to "abolish restrictions on international trade", whereas human rights considerations are included in the Recast Dual-Use Regulation for exactly this purpose.[63] Furthermore, while human rights obligations are traditionally intended to apply within a territory, the integration of human rights considerations in the Recast Dual-Use Regulation prompts questions about the EU's extraterritorial human rights obligations.

In the following subsections, we firstly discuss the constitutional basis for the integration of human rights in EU external policy, and secondly explore how the EU's adoption of human rights as external policy objectives has been operationalised in policy instruments.

2.4.1 Constitutional basis for the integration of human rights in EU external policy

Human rights played little role in the inception of the European Community. Despite the absence of reference to human rights in the founding treaties of the EU, the CJEU found fundamental rights to constitute general principles of Community law in 1970.[64] Human rights gradually found expression in successive EU treaties. As human rights became a priority for the internal policies of the EU, the EU also gradually started promoting human rights worldwide, through its external policy. Since then, the EU's commitment to promote human rights in its external policy has been firmly anchored in the Treaty on the Functioning of the EU (TFEU) and the Treaty on EU (TEU).

According to Article 207 TFEU, the "common commercial policy shall be conducted in the context of the principles and objectives of the Union's external action." These principles and objectives are laid down in Article 21 TEU, requiring EU external action to be guided by human rights and fundamental freedoms. Article 3(5) TEU further consolidates this, demanding that the EU contributes to the protection of human rights in its relations with the wider world. The repeated links between human rights and external policy in EU primary law have led scholars to conclude that the integration of human rights in external trade policy is not simply a policy choice, but a fundamental constitutional obligation.[65] As a result, it has been argued that the EU bears human rights obligations "toward individuals outside the territory of its Member States who are affected by its trade and investment policies."[66]

Still, being guided by "human rights" is a broad concept. Since the Lisbon Treaty, however, the EU has also embedded human rights in its EU Charter on Fundamental Rights. As a result, the implementation of these human rights obligations in this context also leads to the question to which extent the EU is bound by human rights standards derived from the Charter when implementing EU trade policies.

63 Treaty on the Functioning of the EU, Article 206.
64 CJEU 17 December 1970, 11/70 *(Internationale Handelsgesellschaf*).
65 Peter Van Elsuwege. (2020). *The Nexus between the Common Commercial Policy and Human Rights: Implications of the Lisbon Treaty*. Law and Practice of the Common Commercial Policy, Brill Nijhoff, 416-433, p. 417. See also: Antal Berkes. (2018). *The extraterritorial human rights obligations of the EU in its external trade and investment policies*. Europe and the World: A law review, pp. 3-6.
66 Antal Berkes. (2018). *The extraterritorial human rights obligations of the EU in its external trade and investment policies*. Europe and the World: A law review, p. 20.

The Charter does not include a provision on territorial scope, in contrast to other human rights instruments. Article 51(1) specifies that the provisions of the Charter are addressed to institutions and Member States of the Union, when implementing EU law. Thus, the scope of application of the Charter is defined solely by whether a situation is governed by EU law.[67] The lack of a provision on territorial scope has led scholars to conclude that the Charter "tracks all EU activities, as well as Member State action when implementing EU law."[68]

2.4.2 Operationalisation of human rights commitments in trade policy instruments

In practice, the EU has in an increasing number of policy instruments giving effect to its commitment to promote human rights in external policy. In 2015, the Commission outlined in its *Trade for All* Communication that EU trade policy must be instrumentalised for the promotion of European values, and recognised trade policy as a "powerful tool to further the advancement of human rights in third countries."[69] The Commission's Directorate-General for Trade employed similar language in its Strategic Plan for 2020-2024, describing trade policy as a "vehicle for promoting European values."[70] The Human Rights Action Plan for 2020-2024, dedicated to operationalise the EU's human rights commitments in its external relations, sets out that the EU will promote human rights and democracy "consistently and coherently in all areas of EU external action."[71] The EU commits to advancing a "global system for human rights."[72] Free Trade Agreements concluded by the EU with third countries include progressively extensive human rights clauses.[73] Moreover, the EU Human Rights Guidelines on Freedom of Expression, adopted in 2014, sets out to promote freedom of opinion and expression in all EU external actions.[74] For this purpose, the Guidelines envision the promotion of action "to prevent the sale of surveillance or censorship technology to authoritarian regimes."

In 2015, the Commission furthermore adopted the Guidelines on the analysis of human rights impacts in impact assessments for trade-related policy initiatives, aiming to provide further substance to the constitutional references to human rights in external policy. According to the Guidelines, respect for the Charter is a "binding legal requirement in relation to both internal and external policies."[75] In the Commission's view, when a human rights assessment is conducted in the context of international trade, this assessment is to be performed against the human rights obligations as set out in the Charter.[76] This position has also been confirmed by the EU's High Representative for Foreign Affairs and Security Policy, declaring that "EU external action has to comply with the rights contained in the EU Charter of Fundamental Rights."[77]

67 Eva Kassoti. (2020). *The extraterritorial applicability of the EU charter of fundamental rights: some reflections in the aftermath of the Front Polisario saga*. European journal of legal studies, p. 130; Thomas von Danwitz, and Katherina Paraschas. (2012). *A Fresh Start for the Charter: Fundamental Questions on the Application of the European Charter of Fundamental Rights*. Fordham International Law Journal, volume 35, p. 1399.

68 Violeta Moreno-Lax and Cathryn Costello. (2014). *The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model*. in Steven Peers et al. (eds), T*he EU Charter of Fundamental Rights: A Commentary,* 2014, p. 1658. In Frente Polisario, the General Court asserted that the EU has extraterritorial human rights obligations derived from the Charter when acting within the external policy. On appeal, the Advocate General dismissed the extraterritorial applicability of the Charter, while the Grand Chamber did not reflect on this question. See: CJEU 10 December 2015, T-512/12 (*Frente Polisario*).

69 European Commission, 'Trade for All: Towards a More Responsible Trade and Investment Policy' (14 October 2015), para. 4.2.5.

70 European Commission Directorate-General for Trade, 'Strategic Plan 2020-2024' (19 November 2020) p. 19.

71 Council of the European Union, 'Council Conclusions on the EU Action Plan on Human Rights and Democracy 2020-2024' (18 November 2020), p. 1.

72 Ibid., pp. 24, 26.

73 See e.g.: Lorand Bartels. (2013). *Human rights and sustainable development obligations in EU free trade agreements*. Legal Issues of Economic Integration, volume 40, no. 4; Nicolas Hachez. (2015). *Essential Element Clauses in EU Trade Agreements Making Trade Work in a Way That Helps Human Rights?.* Leuven Centre for Global Governance Studies, Working Paper No. 158; Clair Gammage. (2018). *A critique of the extraterritorial obligations of the EU in relation to human rights clauses and social norms in EU free trade agreements*. Europe and the World: A law review.

74 Council of the European Union, 'EU Human Rights Guidelines on Freedom of Expression Online and Offline' (12 May 2014). Available at: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf.

75 European Commission, 'Guidelines on the analysis of human rights impacts in impact assessments for trade-related policy initiatives' (2015), p. 5.

76 Ibid., p. 2.

77 European Commission High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication on Human Rights and Democracy at the Heart of EU External Action - Towards a More Effective Approach' (12 December 2011), p. 7.

Moreover, there are increasing calls to strengthen the legal liability of European companies when they cause or contribute to human rights violations outside the EU. The European Parliament's Resolution on Corporate Due Diligence and Corporate Accountability, adopted in March 2021, urged the European Commission to introduce a legislative initiative that imposes binding requirements on corporations to identify, prevent and remediate potential adverse human rights impacts of their value chains, including abroad.[78] In the Resolution, the Parliament emphasised that the fundamental rights enshrined in the Charter should inform this due diligence process.[79]

While the specificities of the extraterritorial application of the Charter in EU trade policy remain contested, it is clear that at the very least the EU Charter of Fundamental Rights is an important source for the interpretation of any EU policy, whether internal or external. The Charter is, therefore, also a relevant guiding authority for the interpretation of the Recast Dual-Use Regulation, forming part of the EU's external policy. This is especially so with regard to the new regulatory framework of cyber-surveillance items in the Dual-Use Regulation, given the emphasis on human rights in this framework. This means that this framework should be read in light of the relevant provisions of the Charter, most notably those on privacy and freedom of expression (further discussed in chapter 3).

2.5 Synergies between the Recast Dual-Use Regulation and other EU policy developments

Bringing cyber-surveillance items under the scope of the Recast Dual-Use Regulation reflects a broader trend of subjecting technologies with a potential for surveillance to regulation. This trend can also be seen *within* the EU: with the increasing recognition of the potential of digital technologies to interfere with human rights, the EU has increased its efforts to regulate the development and use of digital technologies under a legal framework.

Thus, when applying the Dual-Use Regulation, it is important to also take note of the human rights standards developed in the context of the EU's internal policy for technologies such as AI and biometric surveillance. Given the extraterritorial application of the Charter, these internal debates should also be considered guiding for the human rights assessment of the technologies likely to fall within the scope of the export control of cyber-surveillance items under the Recast Dual-Use Regulation.

An important example of this, is the debate around the regulation of artificial intelligence (AI) within the EU, in particular for biometric surveillance. The Commission in April 2021 published its proposal for a Regulation on AI.[80] The proposal embraces a risk-based approach, seeking to impose a set of obligations on high-risk applications (such as predictive policing tools or AI in asylum procedures), including obligations relating to the quality of training data, documentation, record keeping, transparency, human oversight, accuracy, robustness and security.[81] On top of this, the proposal seeks to introduce a list of prohibited AI practices. Among these prohibited AI practices, the proposal includes "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement".[82] This prohibition is subject to a number of relatively wide exceptions, for example law enforcement may use such systems in order to find the suspect or perpetrator of a criminal offence that is punishable by a minimum 3-year sentence. Moreover, the ban on biometric systems only covers law enforcement uses of these technologies, and it is limited to systems with 'real-time' identification. Due to the combination

78 European Parliament, 'European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability (2020/2129(INL))' (10 March 2021). Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0073_EN.pdf.
79 Ibid., G.
80 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (21 April 2021).
81 Ibid., Art. 8-15.
82 Ibid., Art. 5(1)(d).

of these restrictions on the scope of the prohibition, civil society organisations already asserted that the proposal does not impose such a ban on biometric surveillance as has been demanded by the Reclaim Your Face coalition.[83]

The proposal specifies that the rules adopted under the EU legislation on AI will only apply to AI systems that are put on the market in the EU.[84] AI applications marketed outside the EU would thus fall outside this scope. The question is, however, to what extent these domestic controls within the EU are relevant for the application of the export framework for cyber-surveillance items.

We conclude that these are relevant in two ways. Firstly, domestic policy is relevant for the assessment whether something should be considered a cyber-surveillance item – whether it has human rights infringing capability. Where it is clear from domestic policy that a certain technology allows for potentially problematic surveillance, this will also have to be taken into account when determining whether this technology falls within the definition of cyber-surveillance items. This will often be the case, given the broad definition. In addition, the fact that domestic policy is intended to mitigate the potential human rights problems of a technology internally, may also play a role in the determination whether a technology can be exported, by assessing to what extent the legislation of the importing country provides similar safeguards.

83 See e.g.: EDRi, ' New AI law proposal calls out harms of biometric mass surveillance, but does not resolve them' (April 2021). Available at: https://edri.org/our-work/new-ai-law-proposal-calls-out-harms-of-biometric-mass-surveillance-but-does-not-resolve-them/.

84 AI Regulation Proposal, Art. 2(1).

3 The human rights framework

As noted above, what sets the provisions on cyber-surveillance in the Recast Dual-Use Regulation apart from the rest of the provisions, is that they have the goal of preventing human rights violations. To be clear, this is not entirely new: the Dual-Use Regulation since 2000 has provided that a member state may prohibit or impose an authorisation requirement on the export of non-listed dual-use items for human rights considerations.[85] As already noted above, this has for example been used by the Netherlands to impose an authorisation requirement for the export of certain chemical dual-use goods to Iraq.[86]

Moreover, the regulation has provided since 2009 that a member state when deciding on an export authorisation, shall take into account all relevant considerations, including their obligations under the so-called "Common Position" which regulates the arms trade, discussed further below.[87] But it is the first time that export regulations to specific items in the Dual-Use Regulation are explicitly linked to human rights considerations.

The applicable human rights framework thus is relevant for the understanding of these provisions in two ways. First, as noted above, the Charter is an important guideline for the interpretation and application of the new regulatory framework for cyber-surveillance items. Second, the regulation itself refers explicitly to the concepts of human rights, humanitarian law and (prevention of) internal repression. In this chapter, we explore the relationship between the Dual-Use Regulation and the human rights framework further.

3.1 Internal repression and serious violations of human rights or of humanitarian law

As noted in chapter 2, the authorisation requirement is triggered where there is a risk that cyber-surveillance items may be used in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law. These three concepts of "internal repression", "serious human rights violations" and "international humanitarian law" are not new. They stem from an already existing European export control instrument which is also aimed at preventing human rights abuses: arms export control.

In 2008, the Council adopted a so-called "Common Position" regarding the export control of military technology and equipment, under which member states must assess the export on the basis of certain criteria.[88] One of these criteria is respect for human rights in the country of final destination as well as respect by that country of "international humanitarian law", specifying that "internal repression" should be considered a violation.[89] Because the terms used in the Recast Dual-Use Regulation are exactly the same as those used in the Common Position, it makes sense to interpret them in line with the Common Position. One important guideline for interpretation is the User's Guide to the Common Position (the Guide).[90] Where useful, this report will also draw on the interpretation of these terms in the Guide.

85 Dual-Use Regulation 2009 and 2020, Art. 8; Dual-Use Regulation 2000, Art. 5.
86 Regeling goederen voor tweeërlei gebruik Irak.
87 Dual-Use Regulation 2009, Art. 12.
88 Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment). Similar phrasing was later used in the Arms Trade Treaty.
89 Common Position, Art. 2(2).
90 User's Guide to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment, 10858/15 (20 July 2015).

3.2 International human rights instruments

3.2.1 Surveillance and international human rights law

Human rights are relevant in the context of the new rules on cyber-surveillance items in the Recast Dual-Use Regulation in two ways: first, for the interpretation of the concept of cyber-surveillance items, and second, for the assessment of whether an item may be used in connection with serious violations of human rights. This section will discuss international human rights law and international human rights instruments in which the human rights compatibility of a wide range of surveillance practices have been discussed.

Surveillance may negatively impact the exercise and enjoyment of a broad spectrum of human rights.[91] At its core, surveillance may interfere with the right to privacy. Arbitrary or unlawful surveillance may also violate other rights, such as the right to freedom of opinion and expression and the right to peaceful assembly. Digital surveillance technologies coupled with automated profiling capabilities have been shown to engender arbitrary or unlawful discrimination. Furthermore, it has been repeatedly demonstrated that surveillance of human rights defenders and journalists may lead to arbitrary detention, torture or even extrajudicial killings.

The International Covenant on Civil and Political Rights (ICCPR) is the most comprehensive international treaty protecting civil and political rights, and the primary point of reference for global standards of human rights. Surveillance measures have been repeatedly assessed in light of various provisions of the ICCPR, particularly in the context of limitation clauses of various rights. Article 17 ICCPR enshrines the right to privacy, providing that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." According to Frank La Rue, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the right to privacy entails 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."[92]

The scope of the right to privacy has dynamically evolved, in accordance with societal and technological change. In a report dedicated to unpacking the scope of the right to privacy in the digital age, the High Commissioner for Human Rights explained that "informational privacy, covering information that exists or can be derived about a person and her or his life and the decisions based on that information, is of particular importance" in the digital environment.[93] Furthermore, the right to privacy, as protected by Article 17 ICCPR, extends not only to content-related information but also to metadata.[94] While Article 17 ICCPR does not include a limitation clause, it is universally accepted that limitations on the right are permissible as long as they are provided by (accessible and precise) law, they pursue a legitimate aim, and they meet the test of necessity and proportionality.[95]

91 UN General Assembly, 'Resolution adopted by the General Assembly on 18 December 2013', A/RES/68/167; UN General Assembly, 'Resolution adopted by the General Assembly on 19 December 2016', A/RES/71/199.
92 UN General Assembly, '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, para. 22.
93 UN General Assembly, 'The right to privacy in the digital age', A/HRC/39/29, para. 5.
94 Ibid., para. 6.
95 UN General Assembly, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism', A/69/397, para. 30.

The General Assembly and the Human Rights Council have repeatedly expressed their concern about the danger surveillance technologies pose to the protection and promotion of the right to privacy.[96] Indiscriminate mass surveillance has been held to be incompatible with Article 17.[97] Furthermore, "the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy."[98] The High Commissioner for Human Rights has found the creation of mass databases of biometric data to raise "significant human rights concerns".[99] As summarized by Frank La Rue, the lack of judicial oversight, "vague and unspecified" national security exemptions and new surveillance capabilities falling outside existing legal frameworks have rendered the system of protection of the right to privacy against digital surveillance weak.[100]

The right to privacy is understood as an "essential requirement" for the protection of the right to freedom of expression, enshrined in Article 19 of the ICCPR.[101] Interferences with the right to privacy limit the exchange of ideas and may create chilling effects against free expression. Surveillance technologies may be abused to track, intimidate and silence dissent. In this way, digital surveillance "directly undermines the ability of journalists and human rights defenders to conduct investigations."[102] Furthermore, digital surveillance has also been found to lead to interferences with freedom of association and assembly, unlawful discrimination, torture and even extrajudicial killings.[103]

In order to protect individuals against the human rights implications of digital surveillance, States not only have a negative duty to refrain from interfering with the rights enshrined in the ICCPR, but also a positive duty to "prevent, investigate, punish and redress" human rights abuses by third parties emanating from digital surveillance.[104] According to the High Commissioner for Human Rights, this includes a duty to put in place "export control regimes applicable to surveillance technology" that take into account the human rights impact of the technologies in question.[105] Furthermore, in accordance with the non-binding UN Guiding Principles on Business and Human Rights, corporations have a responsibility to "avoid infringing on the human rights of others and address adverse human rights impacts with which they are involved", regardless of where the individuals affected are located.[106] As explained by the High Commissioner for Human Rights, manufacturing and selling digital surveillance technologies that are used for infringements on the right to privacy trigger this responsibility.[107]

Drawing on the principles sketched out above, Frank La Rue's successor as the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, devoted a full report to surveillance export and its corresponding implications for international human rights law. He problematised how private corporations have been "selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society."[108]

96 See e.g.: UN General Assembly, 'Resolution adopted by the General Assembly on 18 December 2013', A/RES/68/167; UN General Assembly, 'Resolution adopted by the General Assembly on 18 December 2014', A/RES/69/166; UN General Assembly, 'Resolution adopted by the Human Rights Council', A/HRC/RES/28/16; UN General Assembly, 'Resolution adopted by the Human Rights Council on 23 March 2017', A/HRC/RES/34/7.
97 UN General Assembly, 'Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism', A/HRC/33/29, para. 58.
98 UN General Assembly, 'The right to privacy in the digital age', A/HRC/39/29, para. 7.
99 Ibid., para. 14.
100 UN General Assembly, '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, paras. 54-63.
101 Ibid., para. 24.
102 UN General Assembly, 'Surveillance and human rights', A/HRC/41/35, para. 26.
103 UN General Assembly, 'The right to privacy in the digital age', A/HRC/39/29, para. 11; UN General Assembly, 'Surveillance and human rights', A/HRC/41/35, para. 1.
104 UN General Assembly, 'The right to privacy in the digital age', A/HRC/39/29, para. 24.
105 Ibid., para. 25.
106 Ibid., para. 42.
107 Ibid., para. 43.
108 UN General Assembly, 'Surveillance and human rights', A/HRC/41/35, para. 48.

This has exposed the inadequacy of the Wassenaar Arrangement to meaningfully address the risks associated with export of surveillance technologies.[109] As explained by David Kaye, export controls that include a robust human rights assessment are crucial in order to bring the operations of the private surveillance industry in compliance with international human rights law. For this purpose, he outlined that states need to "condition private sector participation in the surveillance tools market – from research and development to marketing, sale, transfer and maintenance – on human rights due diligence and a track record of compliance with human rights norms."[110] In addition, asserting that the export of surveillance technologies to repressive regimes brings about an "extraordinary risk" for human rights, the Special Rapporteur also called on States to implement an "immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools."[111] In light of the overwhelming evidence that the private surveillance industry has provided tools to repressive regimes for "manifestly illegitimate purposes", the Special Rapporteur considered it crucial to halt all export of surveillance technologies until evidence shows that the use of the technology in question is limited for lawful purposes only.[112]

3.2.2 Surveillance under the ECHR and the Charter

Above, we have discussed international human rights instruments. For the European Union, the two most relevant human rights instruments are the European Convention for Human Rights (the Convention) and the Charter of Fundamental Rights (the Charter). The European Convention was adopted in 1950 by the members of the Council of Europe and is adjudicated by the European Court of Human Rights (ECHR). The Charter was adopted in 2007 as the culmination of the European Union's ambition to ensure respect for human rights within its territory. It is adjudicated by the European Court of Justice (CJEU).

In the Convention, the right to privacy is protected (Article 8). In the Charter, the right to privacy and the right to data protection are protected separately (Articles 7 and 8). Both instruments also protect the right to freedom of expression (Articles 10 and 11 respectively), the prohibition of discrimination (Articles 14 and 21 respectively), and the right to freedom of assembly (Articles 11 and 12 respectively). The Charter provides at least the same level of protection as the Convention, but may provide additional protection.

The Convention case law on surveillance goes back decades, starting with the seminal *Klass*-case of 1972, already discussed above. The Court in this case outlined two basic principles which have since become the bedrock on fundamental rights case law on surveillance. First, it is not only the application of these measures to individual persons which affects the rights to privacy and communications freedom, but also the "menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services" (par. 41). And second, the Court noted that secret surveillance is allowed under certain circumstances, but, "being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" (par. 49). Central to the assessment what measures are "appropriate", the Court requires that "whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse" (par. 50).

Since then, this starting point has been worked out in numerous decisions, not only by the European Court of Human Rights but also by the European Court of Justice. The most relevant decision of the European Court of Human Rights is *Zakharov* (2015), in which the Court summarised its earlier body of case law on surveillance measures. In short, this assessment firstly tests whether the measures are set out in sufficient detail.[113] The Court secondly tests whether the measures are necessary in a democratic society

109 Ibid., para. 37.
110 Ibid., para. 46.
111 Ibid., paras. 33, 66.
112 Ibid., para. 49.
113 ECHR 4 December 2015, application number 47143/06 (*Zakharov*), para. 231.

and proportionate to the legitimate aim pursued, which depend on all the circumstances of the case, such as the nature of the measures and the oversight in place.[114] Around the same time, the European Court of Justice has also started issuing decisions on surveillance measures. Together, the courts have in the past decades developed a number of criteria relevant to proportionality assessment of these measures. For our purposes, those which have a potential bearing on the technology are most relevant.

This non-exhaustive list of criteria, derived from the jurisprudence of the European Court of Justice and the European Court of Human Rights, includes:

- **The nature of the data collected:** Although the processing of all types of personal data triggers the protection of the right to privacy, the more sensitive the data that is collected, the more serious the interference is considered to be. The collection of special categories of data, such as data relating to racial or ethnic origin or genetic data, will in almost all cases be problematic.[115] In respect of the nature of the data collected in the case of communications surveillance, both courts also distinguished between surveillance of the content of communications and surveillance of communications metadata. The surveillance of the content of communications has in the past been considered more problematic than the monitoring of communications metadata.[116] However, this does not mean that surveillance of communications data is necessarily harmless. When metadata such as location data, Internet browsing activity and communication patterns are systematically monitored, the interference may even be more serious than when content of communications is surveilled.[117]

- **The nature of the information derived from the data collected:** When the data collected is not sensitive itself, but there is a potential that sensitive information can be inferred from it, the interference with the right to privacy will furthermore be considered more serious. In this respect, the European Court of Human Rights for example emphasised that when there is a possibility to draw inferences as to ethnic origin, the surveillance practice will be considered particularly problematic.[118]

- **The scale of surveillance:** The greater the scale of a surveillance practice, and thus the more personal data collected, the more problematic it is from a privacy perspective, and the more pressing the need for adequate guarantees safeguarding against abuse.[119] Indiscriminate, bulk surveillance has been considered a particularly serious interference. For example, the European Court of Justice considers the untargeted retention of communications data for the purpose of fighting crime to be disproportionate.[120] Targeted data retention for fighting crime can on the other hand be compatible with the Charter if the authority is sufficiently clear and there are sufficient safeguards against abuse.[121] And indiscriminate data retention can be ordered for limited period of time to protect national security.[122] Targeted surveillance, however, does not necessarily constitute a less serious interference and its necessity and proportionality need to be assessed along the other criteria.

- **The way the data is processed:** A surveillance practice is considered more serious when the collected data is processed through automated means. Because automated processing allows

114 *Zakharov*, para. 232.
115 ECHR 4 December 20008, application number 30562/04 and 30566/04 (*Marper*).
116 See *Digital Rights Ireland*, *Schrems I*.
117 ECHR 13 September 2018, application numbers 58170/13, 62322/14 and 24960/15 (*Big Brother Watch*), para. 356; *Digital Rights Ireland*, paras. 26-27.
118 *Marper*, para. 76.
119 ECHR 13 November 2012, application number 24029/07 (*M. M. v. the United Kingdom*), paras. 199-200.
120 *Digital Rights Ireland*, *Tele2*.
121 *Tele2*, para. 109.
122 CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18 (*La Quadrature*).

authorities to go "well beyond neutral identification" and make inferences that would otherwise not be possible, it has been asserted by both courts that the implementation of adequate safeguards is particularly important when automated processing is used to analyse the collected information.[123]

- **The way the data can be accessed:** Where communications metadata retained by a company is accessed directly by the state, this makes the interference more problematic.[124] Instead, the retention legislation must be based on objective criteria in order to define the circumstances and conditions under which the authorities are granted access to the retained data.[125] Put more generally: where access is easier, the potential impact of surveillance is greater.

- **The security of the data:** Lastly, surveillance is considered more problematic when the security of the data is not protected sufficiently against abuse and unlawful access.[126] For this purpose, effective technical and organisation measures have to be implemented.[127] According to the European Court of Justice, when a large volume of data are collected or sensitive data is processed, a "particularly high level" of security needs to be guaranteed.[128]

These criteria are important for this report because, as discussed in chapter 2, the definition of cyber-surveillance items relates around items "specially designed" for covert surveillance. This means that design includes particular features to perform covert surveillance. The above criteria are an important factor in determining whether a certain item has such particular features. We will apply these criteria to a number of surveillance technologies in chapter 5, although as we will see, it is difficult to assess the last three criteria without an in-depth assessment.

Other criteria for the assessment of human rights violations developed by the Courts have more to do with the rules in place, and less with the technology being used. For example, a proper oversight regime and notification of persons being surveilled needs to safeguard against abuse of the powers. The laws circumscribing the application of surveillance in a country are relevant for the assessment of the risk of human rights violations in a particular case, which will be discussed in the next section.

3.2.3 Assessing human rights violations for export control

Whereas the previous section elaborated on how digital surveillance is regulated by international human rights law, this section will provide further guidance regarding how to assess human rights violations in the context of the Recast Dual-Use Regulation. The Recast Regulation imposes a license requirement on the export of cyber-surveillance items which may be used for "internal repression" or "serious violations of human rights" (and serious violations of international humanitarian law, discussed in section 3.4). As noted above, these terms were already used in the context of another export control instrument, the Council Common Position. The guidelines developed in respect of the assessment of "internal repression" and "serious violations of human rights" will be discussed in this section, because these may also provide guidance for the interpretation of these terms in the context of the Recast Dual-Use Regulation.

Internal repression under the Common Position

Under the Common Position, a license for a specific export shall be denied if there is a "clear risk" that the items might be used for "internal repression".[129] According to the Common Position, this concept of "internal repression" includes, "torture and other cruel, inhuman and degrading treatment or

123 *Marper*, para. 75; *Digital Rights Ireland*, para. 55; CJEU 26 July 2017, Opinion 1/15, para. 141.
124 *Privacy Internationa*l, *Tele2*.
125 *Tele2*, para. 119.
126 *Digital Rights Ireland*, para. 66.
127 Ibid., para. 67.
128 *Tele2*, para. 122.
129 Common Position, Art. 2(2).

punishment, summary or arbitrary executions, disappearances, arbitrary detentions and other major violations of human rights and fundamental freedoms as set out in relevant international human rights instruments, including the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights". When assessing this risk, evidence that these or similar items are used for internal repression by the proposed end-user should be taken into account. This is also the case, where there is reason to believe that the items will be diverted from their stated purpose and instead used for internal repression. The nature of items should also be considered carefully, particularly if it is intended for internal security purposes.

In the Guide, these criteria are further worked out. This assessment must be based on a case-by-case consideration. One part of this assessment has to do with the country to which the items are being exported. The Guide mentions various criteria, of which the "current and past record of the proposed end-user with regard to respect for human rights and that of the recipient country in general" is an important criterion.[130] This depends on issues such as a government's policy on human rights, constitutional protection, human rights training and repercussions for human rights violations.[131] The past, present and future developments in the country should also be taken into account. For example, if there are forthcoming elections, this might be fertile soil for repressive actions. Another part has to do with the nature of the items, which can be assessed on the basis of their track record. For example, communications/surveillance equipment can have a strong role in facilitating repression, according to the Guide.[132] Third, the end-user is relevant, which requires a careful analysis of questions such as the role of the end-user in the state, and whether the end-user has been involved in repression.[133]

Serious human rights violations under the Common Position

While under the Common Position an export license shall simply be denied in the case of a clear risk of internal repression, a lower threshold applies for exports to countries where "serious violations of human rights" have been established by the competent bodies of the United Nations, by the European Union or by the Council of Europe. In that case, member states are required to exercise "special caution and vigilance" in issuing export licenses.

A crucial question pertaining to this criterion is what human rights violations should be considered as "serious". According to the Guide, while all circumstances need to be taken into account, one relevant factor is "the character/nature and consequences of the actual violation in question".[134] Where there are "systematic and/or widespread violations", this underlines the seriousness. But violations do not of course have to be systematic or widespread in order to be considered as "serious".

Reference to serious violations of human rights is included in a further export control instrument, adopted under the auspices of the United Nations. Pursuant to the Arms Trade Treaty (ATT), the export of conventional weapons within the scope of the ATT should be assessed on the basis of their potential to be used to commit or facilitate a serious violation of international human rights law.[135] The Geneva Academy developed guidelines in respect of the assessment of the seriousness of a human rights violation for the purposes of the ATT, which may provide further guidance regarding the interpretation of this term in the context of the Recast Dual-Use Regulation.[136]

130 User's Guide to the Common Position, p. 43.
131 Ibid., p. 43.
132 Ibid., para. 2.8.
133 Ibid., para. 2.9.
134 Ibid., para. 2.6.
135 United Nations, The Arms Trade Treaty (24 December 2014), Art. 7.
136 Geneva Academy of International Humanitarian Law and Human Rights, 'What amounts to 'a serious violation of international human rights law'? An analysis of practice and expert opinion for the purpose of the 2013 Arms Trade Treaty' (August 2014).

As noted by the Geneva Academy, there is no authoritative definition of the term 'serious violation' under international human rights law.[137] The term has often been used interchangeably or cumulatively with other qualifiers such as 'gross', 'flagrant' or 'egregious'.[138] Analysing the use of the term 'serious violation' in various human rights instruments, the Geneva Academy concluded that 'seriousness' sets a low threshold, and 'seriousness' can be found in respect of violations of most rights protected under international human rights law.[139] Whereas violations of some rights are intrinsically serious (such as the violation on the prohibition of torture), the seriousness of violations of other rights need to be assessed by the context and circumstances.[140] The character of the right, the magnitude of the violation, the type and vulnerability of the victim and the impact of the violation need to be taken into account when making a holistic evaluation of the seriousness of a violation. But to be sure: the surveillance of one dissident can already have a chilling effect on others, and where that dissident may subsequently be tortured or murdered, this one case should already be sufficient for a violation to be "serious".

One particular kind of human rights violation, namely unlawful surveillance, requires further attention. Under European data protection rules, personal data may not be transferred outside of the European Economic Area unless it falls under one of the exceptions outlined in the General Data Protection Regulation (GDPR). One exception is where the European Commission has determined that an importing country is providing a level of data protection which is essentially equivalent to the level of data protection afforded under the GDPR. Where it has been established that a particular surveillance power in a country is, however, not considered to provide such sufficient safeguards against abuse, for example by a court, the export of items to the government of this country for such surveillance should be considered to be used in connection with violations of international human rights law. Whether these violations are sufficiently grave to be considered "serious violations" depends on the scope of the powers in question. In the case of the United States, the European Court of Justice determined in *Schrems II* that the surveillance powers with regard to EU-citizens affected the essence of the rights to privacy and judicial protection under the Charter.[141] In that case, it could be argued that such surveillance constitutes a "serious violation of international human rights law".

3.3 International humanitarian law

Although the inclusion of cyber-surveillance items in the Recast Dual-Use Regulation has been justified predominantly because of the human rights risks associated with these technologies, the regulation also conditions the export of cyber-surveillance items on considerations relating to international humanitarian law (IHL). While the goal of both human rights law and IHL is to protect individuals, they are distinct bodies of law. IHL – sometimes referred to as the Law of Armed Conflict or the Law of War – regulates the treatment of persons who are not, or are no longer, taking part in an armed conflict (such as civilians, prisoners of war, the injured and sick), and restricts the means and methods of warfare. Human rights law applies both in peace times and during hostilities, whereas IHL serves as *lex specialis* during an armed conflict.[142] As IHL operates with distinct rules and logic, the following section explores how the use of cyber-surveillance items is regulated by IHL and how a violation of IHL is to be assessed in the context of the Recast Dual-Use Regulation.

137 Ibid., p. 11.
138 Ibid., p. 34.
139 Ibid., pp. 5, 34.
140 Ibid., p. 34.
141 CJEU 16 July 2020, C-311/18 (*Schrems II*), para. 187; CJEU 6 October 2015, C-362/14 (*Schrems*), paras. 94, 95.
142 International Court of Justice, Advisory Opinion of 8 July 1996 on the Legality of the Threat or Use of Nuclear Weapons, para. 25; International Court of Justice, Advisory Opinion on 9 July 2004 on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, para. 106.

3.3.1 Cyber-surveillance and international humanitarian law

International humanitarian law has been developed through a range of international treaties, most importantly the Hague Regulations, the Geneva Conventions and their two Additional Protocols of 1977. From these instruments, a number of IHL principles can be inferred which are relevant for our purposes. These also constitute rules of customary international law. The *principle of distinction* establishes an obligation to differentiate between military objectives and civilians, and only target attacks against the former. Closely related to this, the *principle of precaution* prescribes that constant care has to be taken to spare civilians or civilian objects. The *principle of military necessity* dictates that only the use of force that is necessary to achieve a legitimate military objective is allowed. And the *principle of proportionality* prohibits the use of disproportionate force and the causing of unnecessary suffering.

Whether and how IHL applies in cyberspace has been the subject of intense, decades-long discussions. The International Court of Justice noted in 1996 that the core IHL principles apply "to all forms of warfare and to all kinds of weapons", including "those of the future."[143] The two Tallinn Manuals on International Law Applicable to Cyber Operations demonstrate that there is significant international consensus that IHL applies to cyberoperations in the context of an armed conflict.[144] The principles of distinction, precaution and military necessity, thus, restrict cyberoperations during an armed conflict.

The International Committee of the Red Cross (ICRC) emphasizes that cyberattacks cannot be directed at civilian infrastructures, in particular to "hospitals and objects indispensable to the survival of the civilian population during armed conflicts."[145] However, it notes that the interconnectivity that characterizes cyberspace complicates the practical implementation of this principle.[146] In respect of internet-related attacks, it is particularly difficult to make a distinction between civilian infrastructure and military infrastructure, as everyone uses the same internet. Firstly, attackers will use civilian network nodes, such as vulnerable appliances, to hide their identity. Second, even if they only attack military installations, such as uranium enrichment facilities, an attack may have repercussions on other systems and thus may cause indiscriminate harm. Third, it is becoming increasingly common to attack civilian targets covertly – not only to spy but also to disrupt operations. Because of the difficulties with applying the principle of distinction to cyberattacks, the ICRC concluded that there is a "real risk" that cybertechnologies are not deployed in compliance with IHL.[147]

Cybertechnologies are only governed by IHL when they are deployed as means and methods of warfare in the context of an armed conflict. This means that a cyberoperation has to form part of, and have a clear "nexus" to, an armed conflict that is waged with traditional weapons in order to fall within the scope of IHL.[148] In addition, since most rules stemming from the core principles of IHL only apply to operations that constitute an 'attack', it is crucial to delineate the types of cyberoperations that would qualify as 'attacks' for the purposes of IHL.[149] The Tallinn Manuals specify that a cyberoperation constitutes an attack if it is "expected to cause death or injury to persons or damage or destruction to objects."[150]

143 International Court of Justice, Advisory Opinion of 8 July 1996 on the Legality of the Threat or Use of Nuclear Weapons, para. 86.
144 Michael N. Schmitt (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press; Michael N. Schmitt and Liis Vihul (eds). (2017). *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*. 2nd ed., Cambridge University Press.
145 International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations During Armed Conflicts: ICRC Position Paper* (November 2019), p. 2.
146 Ibid.
147 Ibid., p. 5.
148 Laurent Gisel, Tilman Rodenhauser and Knut Dormann. (2020*). Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*. International Review of the Red Cross, pp. 16-17.
149 'Attack' is defined in IHL in Additional Protocol I, see: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) (8 June 1977), Art. 49.
150 *Tallinn Manual 2.0,* Rule 92.

Since there is a strong emphasis on the violent effects of an operation, the mere spying or surveillance are generally not recognized as attacks under IHL.[151]

The ICRC has increasingly focused on the implications of developments in AI and robotics for armed conflict.[152] Autonomous weapon systems, with the ability to identify and attack targets without human intervention, have raised new questions with regard to loss of control and lack of reliability. The growing investment in AI by military powers foreshadows the increasing deployment of facial recognition or gait recognition technologies to carry out automatic target recognition. The ICRC has already asserted that when such technologies are used during an armed conflict, IHL applies, and thus their deployment has to meet the principles of distinction, precaution and military necessity.[153]

Since IHL predominantly governs operations that constitute an attack, and therefore involve physical violence, digital surveillance traditionally falls outside the scope of IHL. However, in recent years the ICRC is exploring the application of IHL in these areas as well. The ICRC has asserted that due to the "all-pervading" nature of the Internet, disrupting the Internet for civilian populations during an armed conflict is prohibited by the principle of distinction, even if the disruption does not have effects that would qualify it as an attack.[154] Furthermore, according to the ICRC, IHL also applies to "psychological operations."[155] In this respect, the ICRC specifically problematized the "unprecedented levels of surveillance of the civilian population" facilitated by digital technologies.[156] While mass surveillance of civilians is not per se within the scope of, and thus restricted by, IHL, IHL does prohibit this if the primary purpose is to "spread terror among the civilian population" during an armed conflict.[157]

3.3.2 Assessing violations of international humanitarian law

Pursuant the Recast Dual-Use Regulation, cyber-surveillance items are subject to export control if the exporter is informed (in some cases after it has performed its own due diligence and notified the competent authorities), that the item in question may be used for the commission of serious violations of IHL. The Council Common Position includes similar language for the export of arms, so the guidelines developed in the User's Guide in relation to the assessment of a serious violation of IHL are relevant for the purposes of the Recast Dual-Use Regulation.

According to the Guide, an assessment of the risk to IHL should be based on the "recipient's past and present record of respect for international humanitarian law, the recipient's intentions as expressed through formal commitments and the recipient's capacity to ensure that the equipment or technology transferred is used in a manner consistent with international humanitarian law and is not diverted or transferred to other destinations where it might be used for serious violations of this law."[158] It is further noted that "[i]solated incidents of international humanitarian law violations are not necessarily indicative of the recipient country's attitude towards international humanitarian law and may not by themselves be considered to constitute a basis for denying an arms transfer. Where a certain pattern of violations can be discerned or the recipient country has not taken appropriate steps to punish violations, this should give cause for serious concern."[159] Various factors are further mentioned in the Guide, including the presence of national legislation prohibiting violations of international humanitarian law, including enforcement

151 Laurent Gisel, Tilman Rodenhauser and Knut Dormann. (2020*). Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*. International Review of the Red Cross, p. 30.
152 Neil Davidson, 'A legal perspective: Autonomous weapon systems under international humanitarian law' (2018); International Committee of the Red Cross, 'Autonomy, artificial intelligence and robotics: Technical aspects of human control' (2019).
153 Neil Davidson, 'A legal perspective: Autonomous weapon systems under international humanitarian law' (2018), p. 7.
154 Laurent Gisel, Tilman Rodenhauser and Knut Dormann. (2020*). Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*. International Review of the Red Cross, p. 39.
155 Ibid., p. 40.
156 International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts: Recommitting to protection in armed conflict on the 70th anniversary of the Geneva Conventions' (October 2019), p. 21.
157 Ibid.
158 User's Guide to the Common Position, p. 54.
159 Ibid.

and prosecution, training of the military, the risk of disintegration of state structures, corruption, and illicit arms trafficking.[160]

The International Committee of the Red Cross have provided guidelines in respect of the assessment of IHL violations for export control purposes. According to the ICRC, "[v]iolations of IHL are serious if they endanger protected persons (e.g. civilians, prisoners of war, the wounded and sick) or objects (e.g. civilian objects or infrastructure) or if they breach important universal values."[161] War crimes, for example, constitute serious violations of IHL.[162] The ICRC further mentions similar factors to be considered as the User's Guide, including formal commitments to apply rules of IHL, appropriate measures ensuring accountability for IHL violations, IHL training for the military, and prohibition of recruiting children for armed forces.[163]

160 Ibid., pp. 55-57.
161 International Committee of Red Cross, 'Arms Transfer Decisions Applying International Humanitarian Law and International Human Rights Law Criteria' (August 2016), p. 10.
162 Ibid.
163 Ibid., pp. 14-21.

4 The offering of cyber-surveillance items

4.1 General remarks

In the preceding chapters, we discussed the new regulatory framework for cyber-surveillance items. The central question in this report is what the scope of the definition of cyber-surveillance items is – both listed and non-listed items. In order to provide further guidance on the application of this new framework, we have chosen five kinds of technologies which potentially fall within the scope of the definition. We selected these technologies because they represent a broad range of surveillance tools, and because for some of them, there have been explicit calls to curtail their export and use. In this chapter, we discuss the considerations which are relevant for that assessment, also focusing on edge cases. For each technology, we describe the technology and its potential for abuse.

One important note when reading this assessment is that, even though we discuss certain technologies in isolation, the impact of these technologies should also be assessed when used in combination with other technologies. The entire human rights risk of a system can be greater than the sum of its parts. For example, the presence of so-called 'interfaces' that a system provides for integrations with other systems can be a relevant aspect in gauging its potential risks.

Furthermore, in many cases, the deployment and operation of the types of technology described in this report requires technical assistance from the vendor, given their specialized and complex nature. This assistance can include the installation, configuration, testing and maintenance of a system, but also the training of administrators and operators. This is not discussed in-depth in this report, but merits attention in practice.

Lastly, this chapter includes examples of companies providing these technologies. The vendors are included to give an impression of markets for technology that, depending on product- or vendor-specific characteristics and the maturity of oversight and accountability in countries that use the technology, *might* warrant attention. It is possible, and in some cases publicly known, that vendors have internal policies that forbid sales to certain countries for reasons that include human rights.

4.2 Artificial intelligence for facial and emotion recognition

As noted in chapter 2, artificial intelligence (AI) technologies are under heightened scrutiny from policymakers, including in the EU. This is particularly the case when these technologies are used for facial and emotional recognition. This is because persons cannot choose their face nor their emotions, and thus are forced to expose both wherever they go. Yet, it is uncertain to which extent these kinds of technologies fall under the definition of cyber-surveillance items.

4.2.1 Technology

AI technologies and systems encompass a broad range of technologies. One definition of AI refers to an "artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication or physical action," and another to "any artificial system that performs tasks under varying and unpredictable circumstances

without significant human oversight, or that can learn from experience and improve performance when exposed to data sets."[164]

One important application of AI is pattern recognition: recognising that one thing, such as a picture of a banana, is similar to another thing, such as a picture of another banana. This is done through machine learning (ML) methods, such as supervised or unsupervised learning, deep neural networks or reinforcement learning.

Automated facial recognition and automated emotion recognition are examples of AI applications. These technologies apply pattern recognition methods to pictures or videos of humans, for example to try identify persons within a camera feed or to try to predict whether someone is happy or angry.

A facial recognition or emotion recognition system will generally require the following components:

- **Algorithms implemented in software and/or hardware** (e.g. neural processing units and tensor processing units). The mathematics of pattern recognition can be programmed in software that runs on general-purpose processor chips (CPUs). To boost performance, parts of this processing may be offloaded to specially designed AI processor chips, also referred to as AI-accelerators. The combination of AI code and processor chips form the heart of an AI system.

- **User interfaces** (e.g. search functionality and functional workflows). User-interfaces define how a system can in practice be operated. The user-interface of an AI system that has the capability to detect ethnicity and gender, for instance, may or may not allow the operator to explicitly select and search by those criteria. This can be compared to limitations imposed by user-interfaces on access to databases, such as a civil servant being required by the user-interface to supply a correct combination of a person's social security number and date of birth to access further information about that person as opposed to a user-interface that allows the user to search by just a person's name alone. This reduces the potential for unauthorized access to information about partners, friends, family, celebrities, and so on.

- **Training data.** Training data is a key determinant for the accuracy of AI systems in practice. Restrictions on access to training data and pretrained AI systems could be considered in cases where the necessary training data is not already available outside the export control regime.

- **Cameras.** General-purpose (high-resolution) cameras will suffice for most applications.

- **Data processing, storage & communication equipment.** General-purpose data processing, storage & communication equipment can suffice for most applications.

Not all of these components have to be provided by the same vendor. In particular, cameras, and data processing, storage and communications equipment will generally be bought separately. The algorithms and the user interface will sometimes be offered in combination, but it is also possible that the algorithms provide a software interface (called an API), so that a customer can develop its own user interface to work with the algorithm. Moreover, sometimes the system will not work with camera feeds, but can use images or video which have already been collected.

164 No scientific consensus exists on a single definition. For the purposes of this report, two out of four definitions are included from a U.S.-based source: Section 238(g) of the John S. McCain National Defense Authorization Act, 2019 (Pub. L. 115-232). The four definitions in there are used by the National Institute for Standards and Technology (NIST).

According to global market research information, key players in facial recognition come from across the globe, including the Netherlands.[165] Emotion recognition software appears to be a less crowded space, but also includes companies from the Netherlands.[166]

4.2.2 Potential for abuse

Facial and emotion recognition software have various applications, some of which are innocuous and some of which are problematic from a human rights perspective. An innocuous application of facial recognition technology is the software which is used to unlock phones: these kinds of authentication mechanisms harbour little potential for abuse.

The use of facial recognition on images in public spaces is an application of the technology that is more problematic from a human rights perspective, and more prone to abuse. The use of facial recognition software in supermarkets, for instance, has been the subject of widespread criticism due to human rights concerns. Certain supermarkets in the UK have been reportedly using facial recognition technology for real-time analysis of CCTV footage, in order to reduce shoplifting.[167] Facial images picked up by the camera in the supermarkets are compared against a database of 'suspects', and upon a match, the person in question is asked to leave the shop. In this case, a 1-to-many matching is employed, where facial images are matched against a database of faces of identified persons. Such use of facial recognition technologies, especially in public spaces, may raise significant human rights concerns due to their indiscriminate nature (everyone who enters the supermarket is subject to biometric surveillance), and these concerns are only amplified by the sensitive nature of facial biometric data.

The use of emotion recognition can also raise particular human rights concerns when deployed as an assistance for lie detection. Emotion recognition technology was deployed this way for migration control under the EU's iBorderCTRL project between 2016 and 2019. Under this project, people entering a country (Greece, Hungary and Poland took part in the project) were asked certain questions with a camera recording their face while answering. The recording was then analysed with emotion recognition software, with the apparent aim of assessing whether they were deceitful or not. The project has been widely criticised for its lack of accuracy and its potential to lead to unlawful discrimination.[168] A more fundamental concern is that deception detection may be at odds with the right to non-incrimination.

The fact that certain facial recognition technologies have a potential to be abused for serious human rights violations has been demonstrated by the way these technologies have been used, and integrated, in the surveillance regime of China. As reported by the New York Times, facial recognition technology

165 'The global facial recognition market size is expected to grow from an estimated value of USD 3.8 billion in 2020 to USD 8.5 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 17.2%' (Globe Newswire, 9 December 2020). Available at: https://www.globenewswire.com/news-release/2020/12/09/2141965/0/en/The-global-facial-recognition-market-size-is-expected-to-grow-from-an-estimated-value-of-USD-3-8-billion-in-2020-to-USD-8-5-billion-by-2025-at-a-Compound-Annual-Growth-Rate-CAGR-of.html. These include NEC Corporation (NEC) (Japan), Aware, Inc. (Aware) (US), Ayonix Corporation (Ayonix) (Japan), Cognitec Systems GmbH (Cognitec Systems) (Germany), NVISO SA (nViso) (Switzerland), Animetrics (US), Neurotechnology (Lithuania), Daon (Ireland), Stereovision Imaging, Inc. (SVI) (US), Techno Brain (Dubai), Innovatrics (Bratislava), id3 Technologies (id3) (Israel), Thales (France), Idemia (France), Nuance Communications, Inc. (Nuance) (US), BioID (Germany), Fulcrum Biometrics, LLC. (Fulcrum Biometrics) (US), TrueFace.AI (US), Amazon (US), FacePhi (Spain), Herta Security (Herta) (Spain), Kairos AR, Inc. (Kairos) (US), SightCorp Inc. (SightCorp) (The Netherlands), and Microsoft Corporation (Microsoft) (US). Further players include Accenture, Axis Communications, Certibio, Fujitsu, HYPR, Leidos, M2SYS, Phonexia, and Smilepass.

166 These include Vicar Vision (FaceReader creator), Noldus Information Technology (FaceReader distributor), VisageTechnologies (FaceAnalysis; also detects age and gender) and MorphCast (EmotionalTracking).

167 Matt Burgess, 'Some UK Stores Are Using Facial Recognition to Track Shoppers' (Wired, 20 December 2020). Available at: https://www.wired.com/story/uk-stores-facial-recognition-track-shoppers/. See also: Privacy International, 'Cooperating With Who?! Answers Needed as UK Retailer Southern Co-Op Tests Facewatch' (9 December 2020). Available at: https://privacyinternational.org/advocacy/4342/cooperating-who-answers-needed-uk-retailer-southern-co-op-tests-facewatch.

168 Natasha Lomas, "Orwellian' AI Lie Detector Project Challenged in EU Court' (Tech Crunch, 5 February 2021). Available at: https://techcrunch.com/2021/02/05/orwellian-ai-lie-detector-project-challenged-in-eu-court/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLm5sLw&guce_referrer_sig=AQAAAII3919cqisw-rYw1E1uunn2R0pT0aF_peLYm1Ym5G7ewekrRDyor2Kjk5IESZKgXuoAow2CtxQyMAktNGmyOhAkVDpSFevo36y6NGGqLNiJBMFCWSW2gtdcnfZt13RnDlFV5FHlUM1hQO5CBBs9n_mDcC-exBWOPLxwoEXbrnI6; Umberto Bacchi, 'EU's lie-detecting virtual border guards face court scrutiny' (Reuters, 5 February 2021). Available at: https://www.reuters.com/article/europe-tech-court-idUSL8N2KB2GT.

has been deployed on a mass scale to identify and track individuals belonging to the Uighur minority in certain parts of China.[169] The purpose of the use of facial recognition is to try identify "unsafe" actors who are then potentially sent to detention centres.[170] This case aptly illustrates how applying facial recognition on images in public spaces has the potential to lead to mass surveillance and ethnic profiling, resulting in serious interferences with the right to privacy (due to the indiscriminate nature of surveillance and the highly sensitive nature of ethnic data), and can pave the way for unlawful discrimination and subsequent human rights abuses (such as unlawful detention).

In Belarus, facial recognition technologies have furthermore been used to track down political dissidents. A prominent political activist known for his vocal criticism of the Belarusian government was reportedly hiding in a safe house when the country's security services tracked a close acquaintance of his with the use of facial recognition technology, leading to his hiding place and resulting in his arrest.[171] The case highlights the potential of facial recognition technologies to be abused to crack down on dissent, engendering chilling effects on the right to freedom of expression and freedom of assembly, and stifling participation in public debate.

Issues concerning the accuracy of AI for facial and emotion recognition further exacerbate the potential negative implications of the deployment of these technologies. Not all AI functions may work under all real-life circumstances, for instance due to algorithmic deficiencies (e.g. errors in facial recognition when a person wears glasses, a mouth-covering scarf) and due to emergent behaviour caused by issues with the training data that was used to train the algorithm. In 2018, a well-known study of three commercial facial recognition systems in the U.S. showed that systems were far less accurate in detecting faces of black women (error rate of 37.4%) than white men (error rate of 0.7%).[172] This was due to the algorithms being trained with 'unbalanced' training data that included statistically significantly more male than female persons, and significantly more white persons than non-white persons.[173]

Emotion recognition systems have limitations too: systems designed for use in laboratory settings may not function properly, or at all, when a person does not look straight at the camera, or when the background is moving. In that case, it is in practice impossible to use that specific technology in conjunction with video feeds from security cameras in public spaces in attempt to detect emotions of people in crowds. Moreover, research shows that AI for emotion recognition consistently judges faces of black persons to be angrier and more arrogant than faces of white persons.[174] The lack of accuracy of facial and emotion recognition technologies has, thus, the potential to aggravate existing discrimination against marginalised groups in society.[175]

169 Paul Mozur, 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority' (New York Times, 14 April 2019). Available at: https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

170 Darren Byler, 'China's Hi-Tech War on its Muslim Minority' (The Guardian, 11 April 2019). Available at: https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.

171 Megi Hakobjanyan, Abigail Buhrman and Samuel Rubenfeld, 'Used by Repressive Governments, Belarusian Facial Recognition Software Tracks Dissidents' (10 March 2021). Available at: https://brief.kharon.com/updates/used-by-repressive-governments-belarusian-facial-recognition-software-tracks-dissidents/.

172 Joy Buolamwini and Timnit Gebru. (2018). *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, pp. 77-91.

173 In 2020, another study on bias in facial recognition also did not yet show promising results. See: Tomáš Sixta et al. (2020). *FairFace Challenge at ECCV 2020: Analyzing Bias in Face Recognition*. arXiv:2009.07838 [cs.CV].

174 Lauren Rhue. (2018). *Racial influence on automated perceptions of emotions.* Available at SSRN 3281765.

175 See e.g.: Ella Jakubowska, 'Mass facial recognition is the apparatus of police states and must be regulated' (EDRi, 17 February 2021). Available at: https://edri.org/our-work/mass-facial-recognition-police-states/.

Issues with regard to accuracy can be addressed by improving the technology, though. In particular, it should be ensured that AI systems are tested under circumstances that are representative of the real-world situation in which they are deployed. [176] But this doesn't address the more fundamental human rights problems with the use of facial and emotion recognition – in fact, a higher accuracy could actually exacerbate the more fundamental human rights issues by making surveillance technologies more effective.

4.3 Location tracking devices

Location-tracking devices allow tracking of the physical location of a device over time. While facial and emotion recognition technologies may be relatively recent inventions, location tracking technologies have already been in use for quite some time by law enforcement and intelligence agencies: attaching a beacon to a vehicle is for example already being done for decades. However, as smartphones have become ubiquitous and tracking technologies have become more advanced, it has become much easier to do, also at scale.

In this section we discuss a number of commonly used location tracking technologies, with quite significant differences in the way they work.[177] As a result, some of them may be more likely to fall under the header of cyber-surveillance items than others.

We also mention the accuracy of the location tracking technology in the section below. We do this only to give a rough idea about the potential coarseness of location positioning. In practice, the accuracy depends on many circumstances, notably how the technology is in practice deployed, configured and used.

A location-tracking system might involve devices that actively emit location data, either semi-continuously (e.g. once per minute) or in bursts (e.g. one bulk-like transmission once per day or week), to an external system. A location-tracking system may or may not provide the possibility to show locations in real-time.

4.3.1 Technology

Satellite-based location tracking

The most important development in location tracking is the general availability of satellite-based location services. This kind of tracking can rely on different satellite systems, co-ordinated by different countries: GPS (U.S.), Galileo (EU), Glonass (Russia), BeiDou (China), and/or QZSS (Japan).[178]

Satellite location-tracking devices based on, for instance, GPS can be readily bought online. On various Chinese online markets these devices are available at low prices. These are also resold within the EU,

176 The accuracy of facial recognition systems could be benchmarked, as is done by for instance NIST in their (ongoing) Face Recognition Vendor Test and their 2017 study, entitled *Face In Video Evaluation: Face Recognition of Non-Cooperative Subjects*. The latter is especially relevant from a human rights perspective, as it focussed on systems that aim to solve the so-called 'open-set identification' problem in video streams: that is, facial recognition being applied to video streams of public security cameras. The datasets used for benchmarking and the benchmarking process itself could be designed such that chances of unintentional discriminatory effects remaining undetected are reduced. This does, however, not rule out the possibility that local AI systems engineers could intentionally retrain a system with unbalanced data with the intent of increasing bias. NIST, 'Face Recognition Vendor Test (FRVT) Ongoing' (2021). Available at: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing; Patrick Grother, George Quinn and Mei Ngan. (2017). *Face In Video Evaluation (FIVE): Face Recognition of Non-Cooperative Subjects*. NISTIR 8173, DOI: https://doi.org/10.6028/NIST.IR.8173.

177 We will not discuss Automated Number Plate Recognition (ANPR), location tracking through device fingerprinting and IP addresses more exotic methods for location tracking exist that could become more widely adopted, such as audio-based positioning (data collected from a microphone can be matched to data known to be associated with a particular location at that time).

178 According to global market information, major players in GPS-based location tracking devices are CalAmp Corporation, Orbcomm Inc., Sierra Wireless, ATrack Technology, Geotab, Concox Information, Trackimo, Meitrack Group, and Ruptela UAB. No market information could readily be found for other categories of location-tracking technology. 'GPS Tracking Device Market Report: Trends, Forecast and Competitive Analysis' (Globe Newswire, 4 March 2021). Available at: https://www.globenewswire.com/news-release/2021/03/04/2187240/0/en/GPS-Tracking-Device-Market-Report-Trends-Forecast-and-Competitive-Analysis.html.

including the Netherlands. If you want to track a person covertly, you can, for example place such a tracking device under a car or in a bag.

The question then is how the location will be collected. Such a device registers its location coordinates in time intervals (e.g. one location datum per minute, per hour, or per day). For some devices, you have to physically gain access to the device to extract this location history data. There are, however, also tracking devices that connect to a mobile network, which allow for the transmission of location information in real-time. The accuracy of positioning varies per satellite system. For commercial GPS receivers, the U.S. government claims an error margin of slightly less than 8 meters.[179] For Galileo, the European Space Agency claims an error margin of 4 to 15 meters depending on whether one (15m) or two (4m) frequencies are used.[180]

Many targets, however, already carry a satellite-based tracking device with them: a smartphone. Most of the phones will have tracking capability turned on by default on the operating system level. Mobile apps on the phone can then use the location interface offered by the operating system; this offers a new angle for intelligence collection. Any widely used mobile app that requires location permissions can be a goldmine for intelligence collection; this can't be overemphasized. Furthermore, most new cars also have satellite-based location tracking built in. The functionality of these in-vehicle systems can be limited to in-car route planning, but also involve live mobile data connections to transmit information back to a car vendor or third party, for instance to improve machine learning models for automated driving.

Cell tower-based location tracking

Another technology often used by intelligence and law enforcement agencies is cell tower-based location tracking. This works as follows. Mobile devices have unique identifiers: an IMEI identifies a device and an IMSI identifies the subscriber. These mobile devices connect to cell towers (so called "base stations"), which are identified by a "cell-id" that is unique within a mobile network. Activity on mobile devices, such as calls, text messages and data use generate Call Detail Records (CDRs) and Event Detail Records (EDRs) that are stored within the operator's network for billing and troubleshooting. These records also contain the cell towers with which the device connected. And since a cell-id can be mapped to the geographic location of the tower, one can also derive an indication of the location of the user. The accuracy of positioning using only a single cell-id depends on the size of the area covered by the particular cell tower that a device is connected to. A rough indication is that the radius varies between 2km and 50km. However, through post-processing of data from multiple antennas, a more precise location can be obtained, for instance at the level of a street or house block.

The technologies that make up different generations of mobile communication – 2G, 3G, 4G, 5G – each have different properties that can be used for localization. 2G, for instance, includes timing information that allows gauging the distance of a device to a specific antenna. With the emergence of 5G networks, it is expected that many smaller-sized cells will be deployed, especially in urban areas, which translates to a higher accuracy in location positioning that can be up to several meter or less.

Barring actors who have access to CDR and EDR records, such as telecom companies themselves and potentially their government, two other methods of location tracking based on cell towers can be distinguished. First, there is the possibility of local positioning via fake cell towers ("IMSI catchers"): to identify devices that are present in proximity of a particular physical location, a temporary fake cell tower can be covertly set up in that location. If the signal of the fake tower is stronger than that of real cell towers, devices will

179 U.S. National Coordination Office for Space-Based Positioning, Navigation, and Timing, 'GPS Accuracy' (2020). Available at: https://www.gps.gov/systems/gps/performance/accuracy/.
180 European Space Agency, 'Galileo Performance'. Available at: https://gssc.esa.int/navipedia/index.php/Galileo_Performances.

connect to the fake tower instead. This allows the operator of the fake tower to obtain, among others, the unique identifiers of all devices in that area. This can be used to assert that a particular device was at that location at that time, or to identify potential unknown suspects for further investigation.

Second, there is the possibility of remote positioning via the international mobile network's core Signalling System 7 (SS7) protocol stack. This protocol was designed under the (implicit) assumption that only authorized persons and equipment can access SS7 networks. It is considered insecure today, but is still the backbone of international mobile communication, and will remain so in at least the early years of 5G. In networks that lack measures such as an SS7 firewall – which is most networks –, a remote attacker (elsewhere in the world) can remotely 'ping' a mobile device to obtain the cell-id of the tower to which the device is connected. This situation is known to be exploited for both legal and non-legal objectives. Services that exploit it are available on government-restricted markets, and the attack technique has been demonstrated at public hacker conferences. To perform location positioning via SS7, access to an SS7 gateway is required. Whereas such access used to be restricted to the operators of physical network infrastructure, the emergence of so-called 'mobile virtual network operators' (MVNOs) enabled commercial access to SS7 infrastructure. An actor can set up, or co-opt, a MVNO to obtain the access that is necessary to carry out SS7 attacks, including rogue remote location positioning (or intercepting text messages, and so on).

Wi-Fi/Bluetooth based location tracking

Another technology used to determine the location of devices is Wi-Fi and Bluetooth-based location tracking. Whereas satellites obviously have a transmission range of multiple kilometres and cell towers a range of tens of meters, Wi-Fi and Bluetooth transceivers have a much shorter range. Transceivers in devices have a unique hardware identifier ("BSSID" or "MAC address") that, if enabled, emits signals that may be used to uniquely identify (and track) devices. By involving information about signal strengths, the location positioning can be made more accurate.

There are two ways in which these technologies can be used for location tracking. First, individual devices can be tracked by deploying beacons and 'listening' for devices that pass by, for example in public spaces. It is possible to implement anti-tracking measures against this, for example by rotating the MAC-address. The denser the beacon network is, the more precise can the location tracking be. And since the tracking is dependent on the placement of beacons, the coverage of the tracking is limited to those places where a beacon can be placed. This is cost-intensive.

But location tracking also works the other way around. Wi-Fi access points, or "hotspots", broadcast network names ("SSIDs", e.g. "MyHomeNetwork"). Open-source databases such as https://wigle.net/ or https://fon.com/maps/ allow anyone to identify (potential) geolocations of Wi-Fi networks by searching for hardware identifiers (MAC) or network names (SSID). Thus, if a mobile app has permissions to 'listen' for Wi-Fi networks and sends lists of detected network names and hardware identifiers of the hotspots to a central server, this may allow the owner of that server to determine where a device was at what time.

Whether or not this type of tracking is effective in practice depends on what (if any) restrictions the device's operating system imposes to prevent tracking, as well as the coverage and actuality of the public hotspot databases for a particular region. This technology is often used by an operating system to refine the location obtained via satellite-tracking. For Bluetooth, the accuracy can be expected to be in the range of one to a few dozen meters. For Wi-Fi, it may vary between a few meters up to several hundred meters.

4.3.2 Potential for abuse

Location is a highly sensitive category of data, as it reveals a lot about behaviour, and, similar to your

face and expression, cannot be easily faked. Non-problematic uses of location are finding a lost device, as Apple for example offers, tracking your pet and navigation software.[181]

But given the information which can be gleaned from this data, governments and companies also take a keen interest in this information. Law enforcement agencies use it to collect evidence in the course of an investigation. This will generally be targeted. And intelligence agencies also use it to track suspects and to reveal links between different persons in the same location. The NSA reportedly collected 5 billion phone records daily, which included locations of devices – and hence users – based on cell-id's and identified links between users on the basis of that location.[182]

Companies also are known to use location tracking for commercial purposes. There are companies who use it to provide reports on aggregated movement patterns, for example in shopping streets. There are also companies which use the data for more targeted purposes. Employers use it to track their employees who are working off-site.[183] And location-based advertising is already being touted as the next innovation in marketing, allowing advertisers to present an advertisement for a certain clothing brand to a smartphone user when this person is at near a store of the brand.[184] One US-based firm even touts it can provide real-time locations of specific cars in nearly any country on Earth to its customers.[185]

For satellite-based location tracking with specialised location-tracking devices, it is difficult to do location tracking at scale, because the devices need to be physically placed near a target. These devices are more suitable for targeted surveillance – for example by law enforcement or intelligence agencies (covertly), or by employers tracking their employees on the road (overtly). that require their user to allow location services can pose a risk when an app was created with the (covert) intent to make user location data available to third parties.

But satellite-based location tracking via apps in smartphones is a much more accessible technology, which can also be used at scale. An innocent-looking mobile app, such as a running app or game, can in fact be a means of covert intelligence collection in support of objectives that oppose the interests of certain groups of users.[186] Furthermore, an app's creator might be legally forced to provide its users' location data to a government agency, or location data might be stored on vulnerable IT infrastructure that can be accessed by unauthorized parties such as criminal hackers or corrupt IT operators. Because of the possibility to use location data covertly and at scale, location tracking via mobile apps on smartphones has the potential of being prone to indiscriminate use. An app could be created that provides legitimate location-related functionality that is attractive to many people, or certain groups of people, who then voluntarily install the app and give it location permissions, without knowing that the app covertly transmits the user's location to a central server for nefarious purposes.

Furthermore, cell tower-based location tracking can be prone to indiscriminate use. This is particularly the case for records stored at telecommunication providers, because of the central collection point. And

181 See e.g. on tracking of a pet: Nia Martin, 'We've Located the 8 Best Dog GPS Collar Trackers—Plus Non-GPS Options' (12 March 2021). Available at: https://www.rover.com/blog/reviews/dog-gps-collar/.

182 See the NSA's Co-Traveler programme revealed by Snowden: Barton Gellman, 'NSA tracking cellphone locations worldwide' (The Washington Post, 4 December 2013). Available at: https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

183 See the numerous articles on the "best" apps for employee tracking. See e.g.: Aigerim Berzinya, 'A Complete Guide to the Top Ten Employee GPS Tracking Systems' (Turtler, 1 September 2020). Available at: https://turtler.io/news/a-complete-guide-to-the-top-ten-employee-gps-tracking-systems.

184 See e.g.: 'Location Based Advertising (LBA) - A Complete Guide' (Knorex, 9 November 2019). Available at: https://www.knorex.com/blog/articles/location-based-mobile-advertising.

185 Joseph Cox, 'Cars Have Your Location. This Spy Firm Wants to Sell It to the U.S. Military' (Vice, 17 March 2021). Available at: https://www.vice.com/en/article/k7adn9/car-location-data-telematics-us-military-ulysses-group.

186 Sabrina Blasi, 'Information warfare and military camouflage: between revival and innovation' (Finabel – European Army Interoperability Centre, 23 June 2020). Available at: https://finabel.org/information-warfare-and-military-camouflage/.

while records may be retained initially for commercial purposes, they can then later be also used for law enforcement and intelligence agencies, also for mass surveillance. For IMSI catchers, this risk is still present, although it is limited because an IMSI catcher can only collect data on users in its vicinity. Lastly, SS7 tracking allows for real-time location tracking at scale and thus is also highly problematic from a human rights perspective.

Lastly, Wi-Fi- and Bluetooth-based tracking can be problematic from a human rights perspective, but less so. Firstly, it only works if the target has a device that has this connectivity enabled. Second, most Android and iOS devices implement anti-tracking measures, notably randomizing the unique identifier once a day or at every device reboot. Lastly, this type of location tracking requires a dense and wide-spanning network of beacons, which is costly.

4.4 Open-source intelligence software

Open-source intelligence (OSINT) refers to the domain of intelligence produced through the collection and analysis of information from sources that are freely accessible to any person or organization, either paid (commercial) or unpaid. Most of the information in OSINT nowadays comes from digital sources, such as online social media, satellite imagery, real-time camera footage, and leaked, dumped or commercially available databases. And while much intelligence will still be produced by persons browsing through online databases, since the information is in digital form, it has also become increasingly easy to do software-based automated collection and analysis of these sources, in real-time and at scale. This section is about the software used to do OSINT on the basis of online sources.

4.4.1 Technology

OSINT software consists of three components. The first component collects information online, for example with automated scripts which browse social media feeds and store new messages. The second performs the analysis, for example classifying certain messages as problematic, identifying certain relationships between people or recognising faces and emotions. And the third involves the presentation of the analysis through a user interface, for example showing a "social graph" of a network of persons of interest. OSINT software is dependent on access to online sources, ideally in a structured format which can be analysed at scale.

According to global market information, key players in OSINT are Thales SA, Dassault Systemes, Digimind, CybelAngel, Expert System, Sail Labs, Recorded Future, Inc., KB Crawl, Verint Systems, Dataiku, Palantir Technologies, Inc., NICE Ltd and Intrinsec Security.[187] Another vendor is Paterva, the supplier of the general-purpose graphing tool Maltego, which has uses in law enforcement and intelligence, but also to human rights lawyers.[188] Certain third-party plugins for that software are specially designed to collect as much information about persons as possible from hundreds of OSINT sources at once. Combined with social network graphing, this can yield an amount of information that exceeds what persons expect to be knowable about them, even if only open sources are queried. Plugins exist that can be used to find people who, by their last name or other selectors, may match a certain ethnicity, to then build data profiles of those people in the context of keeping track of persons by ethnicity.

187 'Open-Source Intelligence (OSINT) Market Is Expected To Reach USD 11.86 Billion By 2026, Registering A CAGR Of 17.4% | Global OSINT Market to Expand its Reach by Uncovering Hidden Patterns' (Globe Newswire, 8 February 2021). Available at: https://www.globenewswire.com/news-release/2021/02/08/2171407/0/en/Open-Source-Intelligence-OSINT-Market-Is-Expected-To-Reach-USD-11-86-Billion-By-2026-Registering-A-CAGR-Of-17-4-Global-OSINT-Market-to-Expand-its-Reach-by-Uncovering-Hidden-Pattern.html.

188 Tom Longley and Sam Smith, 'Primer: Support Technologies for Human Rights Lawyers' (Open Society Foundations, December 2013). Available at: https://www.opensocietyfoundations.org/uploads/9cfce31b-b933-4592-8726-d3325ae91d1d/primer-support-technologies-for-human-rights-lawyers-20140210.pdf.

4.4.2 Potential for abuse

Given the broad range of data which can be harvested and analysed online, the potential for abuse is significant. Some of the use may be less problematic - not entirely unproblematic, though. For example, software for sentiment analysis is becoming increasingly popular as a tool for companies to understand their customers. This software may automatically analyse opinions and emotions on social media, such as Twitter on a broad scale. A company can then use this information to improve its product or service. This application can already also raise concerns, for example when a company uses the insight not to improve its product but instead merely steer the online conversation away from the flaws of its product.

But when, instead, sentiment analysis is used for political purposes, its use rapidly becomes problematic from a human rights perspective. A government can, for example, check public posts on Facebook and Twitter to quickly identify people organising protests against a regime and then arrest those people. It can also use posts as evidence of participation in protests and use it to prosecute protesters. This latter application will use facial recognition software as part of the analysis (see section 4.2). One paper presents a system "to identify and characterise public safety related incidents from social media, and enrich the situational awareness that law enforcement entities have on potentially unreported activities happening in a city", demonstrating its "usefulness in detecting, from Twitter, public safety related incidents occurred in New York City during the Occupy WallStreet protests".[189]

4.5 Communication interception technologies

The discovery of communication interception technologies in Libya spurred the first wave of export controls of surveillance technologies (see section 4.5.2). This is not surprising: historically, communications interception technologies have been an important tool in the hands of governments. As the importance of the internet has grown over the years, the scope of these technologies has expanded, from voice interception to more data-based surveillance. In this section, we provide a broad overview of important communications interception technologies.

4.5.1 Technology

In most countries, including European member states, the confidentiality of communications is protected by law. Private organisations are in many cases prohibited to intercept communications. Governments may, however, under certain circumstances access communications.

The latter is referred to as Lawful Interception (LI): the electronic surveillance of communication by government authorities as authorized within a legal framework. Because communication services are nowadays provided by companies, lawful interception relies on cooperation between government and these companies. This cooperation is typically mandated by provisions in law that impose a requirement on providers to facilitate access to their networks.

LI is intended to be covert: a person whose communication is subject to interception should be unable to detect that their communication is intercepted at any given time.

Prior to the digital era, phone calls were transmitted in unencrypted form and could be readily intercepted at the telecom provider by placing taps on telephony switches. The digital era, notably the emergence of mobile phones and the internet, has posed new challenges in ensuring LI. To address these challenges, representatives of governments, communication providers, telecommunication equipment vendors and LI solution vendors work together in international standardization bodies such as ETSI (Europe),

189 Michele Berlingerio et.al. (2013). *SaferCity: A System for Detecting and Analyzing Incidents from Social Media*. 2013 IEEE 13th International Conference on Data Mining Workshops, pp. 1077-1080.

CALEA (US) and 3GPP (worldwide) to develop interception standards that describe architectural, functional and technical requirements. Some countries have their own national lawful interception standard, such as Russia (SORM).

The ETSI Technical Standard (TS) 102 232, for instance, describes technical interfaces through which communication service providers can transmit signalling data and content to a law enforcement monitoring facility. The standard consists of multiple parts that cover different communication services, such as IP-based connections (Wi-Fi and fixed-line internet connections), email (POP3, IMAP, SMTP) and IP-based voice communication (VoIP, RCS, VoLTE, VoWIFI). Such standards can be implemented by vendors of telecommunications software and hardware and by vendors of LI solutions, depending on the markets (countries) they want to serve. The description of communications interception items in the control list under the dual use regimes specifically refers to this standard.

According to global market research information, key players in LI are Utimaco GmbH (Germany), Vocal Technologies (US), AQSACOM, Inc. (France), Verint (US), BAE Systems (UK), Cisco Systems (US), Ericsson (Sweden), Atos (France), SS8 Networks, Inc. (US), Trovicor Networks (UAE), Matison (Croatia), Shoghi Communications Ltd (India), Comint Systems and Solutions Pvt Ltd. (India), Signalogic (US), IPS S.P.A (Rome), Tracespan Communications (Israel), Accuris Networks Inc. (Ireland), EVE Compliancy Solutions (Netherlands), and Squire Technologies Ltd. (Netherlands).[190]

Access Now in 2015 further identified the following "systems and components" as warranting heightened scrutiny in regarding "IP Network Surveillance": ETI Group's EVIDENT Investigator, SS8 Communications Insight (Intellego), Area SpA MCR Studio, Amesys's EAGLE GLINT (now Nexa Technologies SAS), AMECS's Analys, Narus nSystem, Vastech ZEBRA, Group 2000's Lawful Monitoring Centre, Glimmerglass CyberSweep Sapience, ATIS Klarios Monitoring Centre, Trovicor (fka Siemens Intelligence Platform), Verint, AQSACOM Aqumen, and Nice Systems.[191]

4.5.2 Potential for abuse

Prior to the digital era, interception generally relied on physical access to equipment and cables, such as telephony switches that carried unencrypted analogue signals. As this involved physical, manual activities, interception of analogue communication was not prone to wholesale surveillance. The digital era ushered in the possibility for using interception technologies on a mass scale.

The use of the interception tools of the French company, Amesys (now known as Nexa Technologies), by the Libyan regime has drawn widespread criticism, and has acutely highlighted the potential to deploy these technologies on a mass scale. The company itself advertised its services as a shift "From Lawful to Massive Interception", which have been allegedly deployed on mass scale against political dissidents, human rights defenders and journalists in Libya, underscoring the significant human rights risks associated with interception technologies.[192]

190 'Global Lawful Interception Market Worth $3.6B in 2020 is Projected to Cross $8.8B by 2025 - Increase in Subversive Activities & Terrorism, and Cybercrimes in the Era of Digitalization' (Globe Newswire, 27 March 2020). Available at: https://www.globenewswire.com/news-release/2020/03/27/2007515/0/en/Global-Lawful-Interception-Market-Worth-3-6B-in-2020-is-Projected-to-Cross-8-8B-by-2025-Increase-in-Subversive-Activities-Terrorism-and-Cybercrimes-in-the-Era-of-Digitalization.html.

191 See e.g.: Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillence Technologies' (Access Now, 2015). Available at: https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf.

192 Margaret Coker and Paul Sonne, 'Life Under the Gaze of Gadhafi's Spies' (The Wall Street Journal, 14 December 2011). Available at: https://www.wsj.com/articles/SB10001424052970203764804577056230832805896.

The capabilities of interception software to be deployed on a mass scale and with high-capacity performance is evident from the advertisements of a range of vendors in the sector.[193] No technical details about these systems are publicly available, but general-purpose technology can be used to build such systems. To obtain high-capacity performance, such systems may include application-specific FGPAs (chips) to boost the number of packets or communication sessions that can be processed per second.

Regarding surveillance of IP networks, it must be noted that most internet-based communication is now typically encrypted by default, using secret keys that are not known to telecom providers or internet access providers.[194] Therefore, while (bulk or targeted) interception of communication at an internet access provider may still yield *some* unencrypted data, it will typically only be a fraction of everything that a government may want to access.

It is however still possible to intercept traffic data (metadata) about communication, such as IP addresses and frequency and sizes of data exchange. And, importantly, domain name lookups are still unencrypted, because Domain Name System (DNS) protocols do not provide confidentiality of those lookups. As a result, an IP network surveillance system at an internet access provider can still be used to perform indiscriminate search of (bulk) communication to identify links between persons and the domain names they interact with. This can serve legitimate purposes, such as identifying persons who visit domains associated with criminal or terrorist content. The same technology can however also be used to identify persons who frequent websites that are associated with certain political or religious views, sexual preference, and so on.

In countries that have legislative safeguards to protect citizen's rights, such as strong oversight and accountability, these capabilities can serve legitimate needs. From a human rights perspective, however, these systems warrant heightened attention when they are exported to countries that lack such safeguards.

4.6 Intrusion software

4.6.1 Technology

Informally, 'intrusion software' can be understood to refer to software that allows its operator to covertly obtain remote access to an electronic device, such as a smartphone, laptop, server or an Internet of Things gadget. This allows the operator to obtain data stored on the device, to eavesdrop via a camera or microphone built in or connected to the device, and to use the device as a stepping stone to carry out attacks on equipment to which the device connects, or against contacts of the user ('hacking via third-party devices'). These kinds of technologies are also on control lists, so will be discussed more succinctly.

Intrusion software as meant here is distinct from digital forensics tools that can be used to obtain local access, that is, in circumstances where the operator has (temporary) physical access to the device. Such tools can for instance include circumvention of access controls on a device, such as a passcode to unlock a smartphone, to obtain evidence from the device. These tools are, by the way, also controlled – and fall within the definition of cyber-surveillance items as is further analysed in section 5.1.

193 See e.g.: 'Intellexa Alliance' (Nexa Technologies, 16 February 2019). Available at: https://www.nexatech.fr/intellexa-alliance-press-news; 'Intelligence Solutions' (Intellexa). Available at: https://intellexa.com/intelligence-solutions/; 'Deep LI – Lawful Interception Software' (Signalogic). Available at: https://www.signalogic.com/index.pl?page=deepli_lawful_interception_software; 'CS Intercept' (iSOLV Technologies). Available at: https://www.isolvtech.com/product/cs-intercept/.

194 For instance, when a person uses GMail, the content of the email messages can be read at the user's own computer and Google's servers, but not at intermediate systems. A tap at the user's internet access provider or telecom provider may reveal the fact that a user connects to Gmail, but will not reveal the content of the communication. Furthermore, some applications implement end-to-end encryption, which if designed and implemented securely, results in content being accessible only on the devices of the sender(s) and receiver(s) of communication; not even to the application provider.

No (public) global market information specifically about intrusion software is known, but Access Now identified in 2015 a number of vendors and products as aligning with the Wassenaar definition of "intrusion software", but these may be partly outdated.[195] Other market players are NSO Group (Pegasus) and Wintego (WINT Cyber Data Extractor).

4.6.2 Potential for abuse

The combination of remote and covert nature of intrusion software, combined with the information available on a device, makes this technology problematic from a human rights perspective, with a serious potential for abuse. Some uses of intrusion software may be considered benign. For example, general-purpose 'remote access software' that is used for purposes such as remote support from IT departments can be considered a legitimate and harmless use of the technology. However, even this software can be abused for intrusion purposes when combined with social-engineering or covert installation.[196] Because remote access software has benign uses, its presence does not always trigger anti-virus software to generate an alarm, which can be abused for malicious purposes to remain undetected.

Using intrusion software to purposefully exploit vulnerabilities with a so-called 'exploit code' and covertly gain access to targeted devices raises serious human rights concerns. To maintain intrusion capability, intrusion software vendors do not disclose the vulnerability to software vendors; the vulnerabilities are kept secret and are only known to the intrusion software vendor and their customers. These are so-called 'zero day' vulnerabilities and are discovered by vulnerability researchers employed at intrusion software vendors or acquired from sellers on the zero-day market.

The holy grails for intrusion software are exploits – in practice often *chains* of exploits – that can provide remote access without requiring the target to open a specific message or website. These are called 'no click' or 'zero click' exploits. One example is a security vulnerability in the voice-calling software library used by WhatsApp: in May 2019, WhatsApp-owner Facebook announced that they detected targeted attacks that abused a previously unknown vulnerability.[197] The attack only required an initiation of a call to the target's device, without the target having to answer the call. When the exploit triggered, the attacker obtained access to WhatsApp messages on that device, hence circumventing the protection that the end-to-end encryption of WhatsApp messages aims to provide.

It has been well documented how intrusion software has been used and abused in order to commit human rights violations. For example, Citizen Lab documented that an award-winning Moroccan journalism project, critical of the Moroccan government, was the victim of a targeted attack using intrusion software.[198] The journalists of the project received a message, ostensibly hinting at a major scoop, containing surveillance malware which enabled secretly taking screenshots, intercepting emails and capturing data through the webcam and microphone. In another case, an internationally recognized

195 FinFisher (formerly Gamma Group), Hacking Team, DigiTask, AGLAYA, RCS Lab, Gr Sistemi (Dark Eagle), Clear-Trail Technologies (QuickTrail), Stratign (Spy Phone), SS8 (Interceptor), and iPS (ITACA). See: Collin Anderson, 'Considerations on Wassenaar Arrangement Control List Additions for Surveillence Technologies' (Access Now, 2015). Available at: . https://www.accessnow.org/cms/assets/uploads/archive/Access%20Wassenaar%20Surveillance%20Export%20Controls%202015.pdf.

196 According to global market research information, key players in this field are AnyDesk Software GmbH, LogMeIn, Inc., TeamViewer, Splashtop Inc., BeyondTrust Corporation, Zoho Corporation, Microsoft, Kaseya Limited, IDrive Inc. RemotePC™, and Remote Utilities LLC. See: 'Global Remote Access Software Market 2020-2025 - Global Market Forecast to Grow at a CAGR of 15.71%, Reaching US$3.829 billion in 2025' (Globe Newswire, 11 August 2020). Available at: https://www.globenewswire.com/news-release/2020/08/11/2076141/0/en/Global-Remote-Access-Software-Market-2020-2025-Global-Market-Forecast-to-Grow-at-a-CAGR-of-15-71-Reaching-US-3-829-billion-in-2025.html.

197 Facebook, 'CVE-2019-3568: A buffer overflow vulnerability in WhatsApp VOIP stack allowed remote code execution via specially crafted series of RTCP packets sent to a target phone number' (May 2019). Available at: https://www.facebook.com/security/advisories/cve-2019-3568.

198 Morgan Marquis-Boire, 'Backdoors are Forever Hacking Team and the Targeting of Dissent?' (Citizen Lab, 10 October 2012). Available at: https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/; Ryan Gallagher, 'How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists' (Slate, 20 August 2012). Available at: https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html.

human rights defender in the United Arab Emirates was the victim of a similar attack numerous times.[199] In both cases, the intrusion software was traced back to an Italian company called Hacking Team.

Even though intrusion software can, in terms of the business model of commercial providers, be generally characterized as a targeted means (it is usually licensed as 'pay per target or investigatory case' rather than a flat-fee tariff that allows unlimited targets), its adverse human rights implications are far reaching and evident. The very purpose of intrusion software is most often to remain undetected by anti-virus software and invisible to the target, leaving activists, human rights defenders and journalists, like in the above cases, vulnerable to being secretly spied on. The covert nature of this surveillance, coupled with the magnitude of information possibly collected, result in grave breaches of the right to privacy and may seriously undermine the right to freedom of expression.

Possible criteria to assess when evaluating whether software warrants heightened attention are whether it can be used indiscriminately and/or covertly. By ensuring that the number of uses and/or the number of acquired licenses for use of the software is registered and audited, the potential risk for large-scale, indiscriminate use can be reduced. In respect of the potential for covert use of the technology, it needs to be assessed whether the user whose computer can be remotely controlled need to provide explicit consent every time the remote control is activated, and whether the state of the remote control - active or inactive – is clearly and immutably known to the user, for instance by visual or auditory clues.

Suppliers of intrusion software and suppliers of remote access software can apply software- and hardware-based controls to prevent the circumvention of license restrictions or restrictions built into a product to prevent indiscriminate and covert use. In general, however, it should be considered possible for well-resourced entities to bypass or remove such controls. This has happened in practice to commercial software that can be used in support of remote computer intrusion for lawful purposes, which subsequently could (and still can) be downloaded by anyone from various online forums and is known to then have been used for unlawful purposes. Two examples of such software – which is legitimate software that is widely in use for authorized IT security testing – are Cobalt Strike and Immunity Canvas.

199 Bill Marczak and John Scott-Railton, 'The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender' (Citizen Lab, 24 August 2016). Available at: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

5 Synthesis: applying the new regulation

The new regulatory framework for cyber-surveillance items revolves around two separate human rights tests. The first is whether an item is capable of human rights infringing cyber-surveillance. The second is whether, in the case of a certain export, there is a risk that an item will be used to infringe human rights. The first step is relevant for the question whether something falls within the definition of cyber-surveillance items. The second is relevant for determining whether an authorisation is required for a certain export.

This report has mainly focused on the first step: the determination of whether something falls within the scope of the definition of cyber-surveillance items. This determination is important for four reasons. Under circumstances, an authorisation is required for the export of such items which are not listed. In addition, a due diligence obligation is triggered on the part of the exporter in certain cases. Moreover, the new rules provide for an extended co-ordination and transparency obligation. And lastly, member states have the possibility to adopt national law that lowers the authorisation requirement threshold on the basis of due diligence findings. The question thus is, what the scope of the definition cyber-surveillance items is. We discuss this first. Then we analyse the implications of the new framework further, including the second human rights test.

5.1 Listed cyber-surveillance items which fall under the definition

Given the wide scope of the definition of cyber-surveillance items in the new Dual-Use Regulation, several listed items certainly fall within the scope of the new rules described above. Recall that the final definition of cyber-surveillance items specifies these as "dual-use items specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analysing data from information and telecommunication systems". Furthermore, in the recitals it has been clarified that items "specially designed to enable the covert intrusion or deep packet inspection into information and telecommunications systems in order to conduct covert surveillance of natural persons by monitoring, extracting, collecting or analysing data, including biometrics data, from these systems" fall within the definition.[200] From this, it can be concluded that the following listed items should be considered to fall within the definition of cyber-surveillance items:

- **Intrusion software** (4D004). This encompasses software for the generation, command and control, or delivery of software which is designed to avoid detection and circumvent protection, and extract data from a device. We discussed this kind of software in section 4.6. Again, the software as described in the control list enables the "covert surveillance of natural persons" (namely, computer or smartphone users), because these devices contain a lot of information of their user. Moreover, it does so by "extracting" this data from devices. This interpretation is furthermore supported by the recitals which confirm that items designed to enable the "covert intrusion" into information systems fall within the scope of the definition of cyber-surveillance items. To the extent, however, that intrusion software does not collect information, and instead merely modifies the system, this kind of software arguably *does* fall within the control list, but should *not* be considered a cyber-surveillance item.

200 Recast Dual-Use Regulation, Rec. 8.

- **Mobile telecommunications interception equipment, and related monitoring equipment** (5A001.f). This definition firstly includes interception equipment for the extraction of voice or data as well as subscriber identifiers and other metadata transmitted over the air, and radiofrequency monitoring equipment. This is because this equipment enables "covert surveillance of natural persons": communications interception is a classical form of surveillance and the people whose communications are being intercepted will generally not be aware of this. And this equipment does this by "monitoring" and "extracting" data, such as voice and subscriber data, from "telecommunications systems" (namely – over the air telecommunications).

- **IP network communications surveillance systems or equipment** (5A001.j). These are items which operate on a "carrier class IP network (e.g. national grade IP backbone)", and do analysis, extraction and indexing of transmitted metadata content (voice, video, messages, attachments) and should be specially designed to search on the basis of "hard selectors" and map the relational network of people. These items perform "covert surveillance" because a person will not be aware of the communications interception. Furthermore, they "collect", "extract" and "analyse" intercepted data. The communications interception technology described in section 4.5 also falls within this definition. This is also supported by the recitals, in which it is clarified that items specially designed to enable "deep packet inspection" into telecommunications systems fall within the definition. However, not all such interception equipment will also be outfitted with software to search and map the data being collected in line with the definition in the control list. One could therefore argue that some of this equipment *does* fall within the definition of cyber-surveillance items, but is *not* on the control list. This depends on whether mere interception equipment without such analysis tools should be considered a "specially designed component" for the equipment described in the control list. In most of the cases, it will be.

- **Software for monitoring or analysis by law enforcement** (5D001.e). This is software which allows for searches on the basis of "hard selectors" of communication content or metadata acquired from a communications service provider using an interface for lawful interception and mapping the relational network or tracking the movement of targeted individuals based on the results of searches. This software is intended for "covert surveillance", because it uses data collected from the interception of communications without persons being aware of it. It furthermore "analyses" data collected via "telecommunications systems". Because this also relates to the "tracking" of individuals, certain technologies used for the monitoring of celltower based location tracking described in section 4.3 should also fall within this definition.

- **Items used to perform cryptanalysis** (5A004.a). This includes functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys (see the technical note). Cryptography is used to safeguard the confidentiality of information in transit and at rest. Cryptanalysis is used to defeat this confidentiality. This technology therefore "enables" covert surveillance by monitoring, extracting, collecting or analysing data from information and telecommunication systems.

- **Tools to extract raw data from a device by circumventing an authentication mechanism** (5A004.b). These are tools which, for example, allow law enforcement agencies to recover data from a smartphone without the passcode. This should also be considered a form of "covert surveillance", because the owner of a device does not know in advance whether and how information on her is being used to target her specifically. It furthermore involves the "extraction" of data from an information system (a device).

However, other surveillance-related technologies which are on the list should not be considered to fall within the definition:

- **Mobile telecommunications jamming equipment** (5A001.f). This because as mentioned in section 2.4.3, the final definition of "cyber-surveillance items" does not include activities aimed at damaging or disrupting communications or systems.

- **Intrusion software which modifies a system** (4D004). The definition of intrusion software also includes software which modifies "the standard execution path of a program or process in order to allow the execution of externally provided instructions". This activity not necessarily involves "monitoring, extracting, collecting or analysing" of data on a system, so this falls outside of the scope of cyber-surveillance items.

- **Laser acoustic detection equipment** (6A005.g). This item works by collecting audio with a laser – allowing for listening to conversations at a distance, sometimes called a "laser microphone". This technology is obviously intended for covert surveillance, but it is not doing so by using data "from information and telecommunications systems".

5.2 Non-listed cyber-surveillance items

In section 2.3.4., we analysed the scope of the definition of cyber-surveillance items. We concluded that the definition of cyber-surveillance items should be interpreted broadly to encompass technologies whose design includes particular features to conduct covert surveillance of natural persons by collecting and using data from information and telecommunications systems. Some of these are listed items – these were discussed in section 5.1 – but cyber-surveillance items also include non-listed items.

In chapter 4, we have discussed several technologies which potentially fall within the definition of cyber-surveillance items. For the communications interception technology discussed in section 4.5 and the intrusion software discussed in section 4.6, this analysis has already been done above in section 5.1 for listed items. For the other technologies, facial and emotion recognition, location tracking and open-source intelligence, this is less clear. We discuss each item separately.

Whether these technologies actually fall within the definition of cyber-surveillance items, depends on a number of factors. One important question is whether its design includes particular features to achieve covert surveillance. We discussed in section 2.3.4 that the term "covert surveillance" should be read broadly, also in light of the aim, which is to ensure the protection of human rights outside of the EU. And in section 3.2.2, we discussed criteria which can be used to determine whether a certain technology or application is problematic from a human rights perspective:

- the nature of the data processed;
- the nature of the information derived from the data collected;
- the scale of surveillance;
- the way the data is processed;
- the way the data can be accessed; and
- the security of the data.

In the following sections, we apply these criteria to the three non-listed technologies described in chapter four. The way data can be accessed and the security of the data very much depends on the specifics of the implementation and the exporter, and will only partly be assessed. Furthermore, where it is clear from domestic policy that a certain technology allows for potentially problematic surveillance from a human

rights perspective, this will also have to be taken into account when determining whether this technology falls within the definition of cyber-surveillance items.

It is important to note that the application of these criteria to specific items is highly context dependent and requires a case-by-case analysis. In reality this application will need to take into account the specific characteristics of a specific item, which are difficult to generalise to entire groups of technology. And of course, the technical capabilities of certain technologies are only one part of the assessment in handling a licensing request, because in the authorisation phase the "end use", and "end user" will also feed into the evaluation of the human rights risks of specific exports.

As the above analysis shows, whether a technology is specially designed for covert surveillance depends on the potential for human rights-infringing surveillance, and this is *also* highly-fact specific. Since the new regulatory framework should be read in light of the EU Charter, we argue that for those cases where it is uncertain whether a technology is specially designed for covert surveillance, an exporter has to perform a human rights impact assessment, taking into account the criteria set out above (see also section 3.2.2), to determine whether a certain item should be considered a cyber-surveillance item, in particular whether it is "specially designed" for "covert surveillance".

Domestic policy plays a role in this assessment as well. This is firstly relevant for the assessment whether something should be considered a cyber-surveillance item, where domestic policy contains safeguards intended to curtail the human rights infringing effect of such an item. This may also inform the determination whether a technology can be exported, by assessing to what extent the legislation of the importing country provides similar safeguards.

Furthermore, an exporter might take technical and organisation measures to prevent a technology from being used to violate human rights, for example by limiting the number of queries that can be run per minute, the number of search results, and/or the number of results that can be exported from the system for use outside any controls/constraints that the system imposes on the user. Where an exporter imposes such technical limitations to prevent human rights abuse, it in the course of this due diligence also has the obligation to demonstrate the efficacy of such technological limitations.

5.2.1 Facial and emotion recognition technologies

As discussed in chapter 4, facial and emotion recognition technologies can be used for various purposes, including covert surveillance. And some of the particular features of these technologies are suitable for human rights infringing surveillance:

- The **nature of the data** which is collected and can be derived is highly sensitive – revealing information about characteristics such as identity, ethnicity and emotion – while it is nearly impossible to fake the data.

- The technologies can be applied **indiscriminately**: generally speaking, there is no inherent limitation in the number of images or persons which may be processed by such technologies. It may, however, be that the training data is focused on a particular use-case, for example authentication, which does not lend itself to other applications, such as facial recognition in public spaces. Where technologies are provided in such a way that the user can develop a custom interface for interacting with it, exposing collection and search functionality through an API, the risks of indiscriminate use become bigger. But to be clear: even targeted applications can already be problematic from a human rights perspective, for example when emotion recognition software is used for the detection of lies.

- The **way the data is processed** also raises concerns, given the courts' tendency to label "automated processing" as problematic. This technology uses pattern recognition to automatically label images or a video feed. This inherent to the fact that the technology is based on AI.

- The **way data can be accessed** very much depends on the specifics of the implementation and the exporter. In this respect, the search functionality is an important element. Where it is possible to search for one characteristic through a large set of data, such as searching the system's history of recently recognized persons/faces by ethnicity or gender, this makes it more problematic from a human rights perspective. Where the functionality is exposed through an API, this is more problematic, especially if this API is tailored to use by a third party, such as a government. As noted in section 3.2.2, this criterion in the case law of the courts has more to do with access by governments, but the underlying concern is that the easier the access, the more problematic it is.

- The **security of the data** also very much depends on the specifics of the implementation and the exporter. If we are concerned about the security of the training data: it will generally be impossible to retrieve the initial input (e.g. the training images) from a neural network. However, other security aspects, such as the protection afforded against unlawful access of the analysis *derived from* the facial recognition are highly technology-specific.

Many of the facial and emotion technologies will also tick the more technically-oriented elements of the definition. These technologies only work when they "collect" data from "information systems" and then "analyse" it. The only question is, what in this context should be considered an "information system". Arguably, cameras themselves should not be considered such a system. But where software is developed to automatically scrape and analyse online sources of images, this indeed can be considered to fall within the definition – the source, in that case, can be considered an "information system". This leads to non-intuitive conclusions, such as that, a recognition technology which is specially designed for use with cameras arguably would not fall within the definition, whereas a system that can work with a variety of sources would. We suggest that policymakers further explore this potential gap.

Given the above, we conclude that exporters who export the algorithm and user interface components of facial and emotion recognition technologies should perform a human rights impact assessment to assess the potential for abuse of their technology in line with the criteria set out in section 3.2.2. This will allow them to determine whether their technology should in fact be considered a cyber-surveillance item, and thus, whether the new regulatory framework applies.

5.2.2 Location tracking technologies

The kinds of location tracking technologies discussed in chapter four will almost always fall within the definition of cyber-surveillance items. First, in many cases the design contains particular features to achieve covert surveillance:

- The **nature of the data**: Location data are in general highly sensitive. They reveal information about behaviour. They can also be used to infer other kinds of data: for example whether someone has visited a mosque or an abortion clinic. And similar to facial and emotion recognition, they are hard to fake. The sensitivity, however, depends to a certain extent on the precision of location tracking, the frequency (time interval) with which location records are generated/kept, and the coverage (in terms of geography and/or inhabitants). As discussed in section 4.3, satellite-based tracking is precise, whereas celltower based tracking and Wi-fi/Bluetooth tracking are not so precise. Satellite-based tracking furthermore potentially has a global reach, especially when tracking is done via a smartphone. Cell tower based tracking through telecommunications providers will at least allow for tracking through the antennas of a certain provider, but when a subscriber is roaming with other providers, in order to obtain a full picture it may also be

necessary to obtain information from these other providers. Wi-fi/Bluetooth tracking has the lowest coverage: this will depend on the number of beacons installed to perform such tracking.

- Most of the technologies can further be applied **indiscriminately**. Satellite-based tracking with a beacon will be difficult to do on a large scale, because this requires the installation of a tracking device at a target. But satellite-based tracking with apps on devices or vehicles can be easily done indiscriminately. Celltower based tracking is by nature indiscriminate: location records are generated as a result of using the service. Similarly, tracking with IMSI catchers and Wi-fi/Bluetooth beacons will be confined to a certain territory, but within this territory everyone may be tracked.

- The **way the data is processed** also is problematic, but perhaps a bit less compared to facial and emotion recognition. The emphasis for these technologies lies more with the "mere" collection of location data than with the analysis of the data. One shouldn't exclude the analysis part entirely, though: recall the NSA programme identifying relationship between persons on the basis of their smartphone locations described above. Where a system also offers these kinds of analytic capabilities, it should quickly be considered to have particular features to achieve covert surveillance.

Furthermore, many of the location tracking technologies described above also fulfil the technical requirements of the definition. Portable satellite-based tracking devices which do not transmit location in real-time, may not fall within the scope, because they do not collect data "from" an "information system" (perhaps one could argue that a satellite is such a system, but this stretches the definition). Satellite-based tracking via apps on smartphones on the other hand "collect" location data from an "information system" and therefore fall within the definition. Celltower-based location tracking "collects" location data from a "telecommunications system". And wifi/bluetooth based tracking technologies "collect" identification data (the MAC-address) from an "information system" (such as a smartphone) and determine its location on the basis of this.

Given the above, we conclude that exporters who export location tracking technologies (except for satellite-based beacons) should perform a human rights impact assessment to assess the potential for abuse of their technology in line with the criteria discussed above.

5.2.3 Open-source intelligence software

The kinds of open-source intelligence software discussed in chapter four will almost always fall within the definition of cyber-surveillance items. First, in many cases the design contains particular features to achieve covert surveillance:

- The **nature of the data** can be quite sensitive. The fact that the information is publicly available does not mean that the data is not sensitive: for example, pictures collected online, can reveal ethnicity, religion and sexual orientation. But it is not only the information which in isolation is sensitive: what sets this technology apart is the vastness of the information which can be collected. These technologies can easily combine images with online messages throughout the web to form a complete picture of a person.

- Most of the technologies can further be applied **indiscriminately**. These technologies are intended to collect data at scale which can then be easily searched. The collection and indexing of scraped data is inherently indiscriminate – the searching by nature is as well.

- The **way the data is processed**. This technology is highly dependent on automation: automation in collection, indexing and analysis. The information is scraped automatically from public sources, is then indexed automatically and the analysis of the information also takes place automatically.

Many of the OSINT software technologies described above also fulfil the technical requirements of the definition. The technologies work by "collecting" and "analysing" data from "information systems" (e.g. online websites, such as social media).

Given the above, we conclude that exporters who export OSINT software should perform a human rights impact assessment to assess the potential for abuse of their technology in line with the criteria set out in section 3.2.2.

5.3 Due diligence and export authorisation

For non-listed items, where an item falls under the definition of cyber-surveillance items, two new obligations come into play. First, an export authorisation is required if an exporter is informed that items are or may be intended, in their entirety or in part, for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law. This means that member states need to have a general picture of categories of items which may fall within the scope of this definition. It is advisable to aim for consistency in the interpretation of this term "cyber-surveillance items", which can be done through the mechanisms described in the next section.

Second, exporting a cyber-surveillance item triggers a due diligence obligation on the part of the exporter to review whether the items are or may be intended, in their entirety or in part, for use in connection with these purposes. Where this is the case, the exporter shall notify the competent export authority, which shall then determine whether the export needs to be subject to authorisation.

5.4 Coordination and transparency

The other part of the framework sets up a coordination system between member states with regard to the export control of non-listed cyber-surveillance items. Each member state has to inform the others of export authorisation requirements for such items, and the others shall take this information in consideration. Where essentially identical transactions are notified, the European Commission shall publish a list of those.

We recommend that the member states approach this issue proactively and together with the European Commision develop guidelines for determining whether specific technologies fall within the scope of cyber-surveillance items, in line with Articles 5 and 26(2) of the Recast Dual-Use Regulation.

For listed and non-listed items, the European Commission is obliged to provide information in its annual report on the export of items on authorisations, in particular on the number of applications received by items, the issuing Member State and the destinations concerned by these applications, and on the decisions taken on these applications.

Transparency is an essential element for ensuring that cyber-surveillance items are not exported to violate human rights. It is therefore important that member states in the context of these provisions give due consideration to the wide scope of the definition, read in light of the ECHR and the EU Charter. This is particularly so where it is uncertain whether an item may fall within the definition. In that case, a member state should for the sake of coordination and transparency publish its considerations with regard to its determination.

5.5 National legislation

Lastly, a member state may adopt national legislation to impose the above-mentioned authorisation requirement on the export of non-listed cyber-surveillance items if the exporter has grounds for suspecting that those items are or may be intended, in their entirety or in part, for any of these uses. Given the above analysis, the Netherlands has the option to apply this power to the export of certain facial and emotion recognition technologies.

Annex: interviewees

- Yvo Amar, partner at AmarBennink
- Siena Anstis, senior legal advisor at CitizenLab
- Stephane Chardon, chairman of the EU dual use co-ordination group on dual use export control at the European Commission
- Paul Diegel, policy advisor to MEP Gregorova
- Tim van Essen, senior policy advisor at the Dutch Ministry of Foreign Affairs
- Milan Godin, legal advisor at the export control unit in the Belgian Ministry of Foreign Affairs
- Tessa de Haan, legal advisor at the export control unit in the Dutch Ministry of Foreign Affairs
- Jeroen van der Ham, Senior Researcher at NCSC-NL
- Merel Koning, policy officer of human rights and technology at Amnesty International
- Barry McKeon, policy manager for trade and competition at DigitalEurope
- Lucas Noldus, founder and CEO of Noldus Information Technology
- Magnus Nordeus, head of trade compliance at Ericsson
- Edin Omanovic, advocacy director at Privacy International
- Adrian Toschev, former head of the German division on dual use export control
- Tim den Uyl, managing director at VicarVision
- Sabine Visser, policy advisor at the arms export control unit in the Dutch Ministry of Foreign Affairs

IViR - Institute for Information Law
P.O. Box 15514, 1001 NA Amsterdam, the Netherlands

https://www.ivir.nl/