EUROPEAN DIGITAL RIGHTS

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware Draft Recommendation to the Council and the Commission

EDRi comments and recommendations

Table of Contents

Contributors

This document is based on EDRi's position paper 'State access to encrypted data. A digital rights perspective' and on contributions and amendments proposed by the following EDRi members and staff:

- Chloé Berthélémy, EDRi
- Jesper Lund, IT-Pol
- Fanny Hidvegi, Access Now
- Julie Fuchs, Access Now
- Andre Meister, individual observer
- Ilia Siatitsa, Privacy International
- Ioannis Kouvakas, Privacy International

Introduction

European Digital Rights (EDRi) welcomes the draft report and draft recommendation on and following the investigation of alleged contraventions and maladministration in the application of

Union law in relation to the use of Pegasus and equivalent surveillance spyware by Rapporteur Ms Sophie In't Veld. With this work, the European Parliament is showing a strong commitment to uncovering Member States' abuses of their surveillance powers and holding them to account for the use of dangerous spyware against journalists, activists, and political dissidents worldwide, that compromise their privacy and safety.

This document lay outs our network's comments on the 'European Parliament Draft Recommendation to the Council and the Commission' of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA).[1] We aim to contribute to debate over what actions the European Union (EU) can take in face of the spyware scandals and support the Members of the Committee in calling for effective measures to protect people's fundamental rights and freedoms against serious attacks by governments, strengthen the rule of law in this field and safeguard the vitality of the civic space.[2] We do not however address the content of the Draft Report.[3]

We stress that surveillance and state hacking in particular is a genuine European political issue. The EU has the opportunity and the possibility to act.[4] The recent case law of the Court of Justice of the European Union (CJEU) on the issue of communications and traffic data retention confirmed that the objective of safeguarding national security cannot serve to justify the automatic and irrevocable exclusion of EU competence.[5] The national security exception cannot become the rule and render inapplicable the protections afforded by EU secondary law read in the light of Articles 7, 8 and 11 and Article 52(1) of the EU Charter of Fundamental Rights. Member States may therefore only implement surveillance measures if they are consistent with EU law.

Whatever actions the EU will take to regulate state hacking practices, it will likely have an important impact on the debates and political developments taking place at international level. It is therefore crucial to reiterate Europe's leadership in privacy and data protection and build a strong and clear legal framework that can serve as a benchmark internationally. For that, the EU must not shy away from drawing strict red lines by prohibiting methods and practices that are

---

1 'European Parliament Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware' (B9-0000/2023) (04 January 2023) https://www.europarl.europa.eu/doceo/document/PEGA-RD-740554_EN.pdf

2 Brett Solomon, 'Digital civic space under attack' Access Now (29 August 2019) https://www.accessnow.org/digital-civic-space-under-attack/

3 'Draft Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware' (2022/2077(INI)) (28 November 2022) https://www.europarl.europa.eu/doceo/document/PEGA-PR-738492_EN.pdf

4 IT-Pol, 'PEGA hearing about spyware and ePrivacy" EDRi (16 November 2022) https://edri.org/our-work/pega-hearing-spyware-and-eprivacy/

5 Joined Cases 511/18, C-512/18 and 520/18 La Quadrature du Net and Others v Premier ministre and Others [2020]

irreconcilable with fundamental rights standards and international legal instruments.

Among draft recommendations, we welcome:

- **26** on support to third countries with surveillance capabilities, imposing human and fundamental risks assessments.
- **35** condemning the extensive use of 'national security' as pretext for the abuse of spyware.
- **36** calling for a common legal definition of national security.
- **39** on a necessary and strict implementation and enforcement of the Union legal framework on data protection.
- **49** on the inclusion of spyware in the definition of cyber-surveillance items in the recast Dual-use Regulation.
- **59** calling for a ban on commercial trade in vulnerabilities, and an obligation to disclose the findings of vulnerability research.
- **84** highlighting the issues of rule of law in certain Member States, making the problem of spyware surveillance more acute.
- **85** calling on the Commission to act more proactively against those Member States that undermine the rule of law and fundamental rights.
- **87-92** assessing the current actions by the different EU institutions so far in reaction to the spyware revelations.
- **93** calling for a legislative action at EU level.

We provide a non-exhaustive list of amendments for the following themes:

EU support to third countries

Draft Recommendation	EDRi amendment
New	**26a. Ensure development assistance and pre-accession funds support within third countries compliance with international human rights standards and other protections governing the use of surveillance technologies;**

Comments

EU funds particularly within the 'Neighbourhood, Development and International Cooperation instrument – Global Europe' (NDICI) and the pre-accession instruments have significant potential

to improve legal frameworks, governance standards and other protections in third countries. Such support may include for example legal assistance aimed at ensuring legislation is in line with international standards, financial support to civil society or technical support to regulatory and other bodies such as data protection agencies and the judiciary.

EU standards regulating the use of spyware by Member States

Draft Recommendation	EDRi amendments
27. Takes the position that the trade in, and use of spyware needs to be regulated strictly; recognising however, that the legislative process will take considerable time, calls for the immediate adoption of a conditional moratorium on the sale, acquisition, transfer and use of spyware, that must be lifted on a country-by-country basis if the following conditions have been met:	27. Takes the position that **the development,** trade in, and use of spyware **technologies that risk affecting the essence of or that excessively interfere with fundamental rights must be prohibited as soon as possible in the European Union.**
(a) all cases of alleged abuse of spyware are fully investigated and resolved without delay by the appropriate law enforcement, prosecutorial and judicial authorities; and	**27a. Spyware technologies are affecting the essence of or excessively interfering with fundamental rights if:**
(b) proof that the framework governing the use of spyware is in line with the standards laid down by the Venice Commission and relevant case-law by the CJEU and ECtHR; and	**(a) they grant full unlimited access to personal data stored on the targeted device; or**
(c) the explicit commitment to grant any request by Europol pursuant to Art 6(1a) of the Europol Regulation relating to investigations into allegations of illegitimate use of spyware; and	**(b) they grant full unlimited control of the hardware features or software applications of the targeted device; or**
(d) repealing all export licences that are not fully in line with both the letter and the spirit of the Dual-Use Regulation;	**(c) they can be deployed remotely, without physical access to the targeted device; or**
	(d) they allow to indiscriminately and simultaneously target a large number of devices; or
	(e) they rely on impersonation or any other type of deceptive techniques, such as phishing links, to be deployed;

Comments

In its 2022 position paper 'State access to encrypted data. A digital rights perspective'[6], EDRi is calling for the ban on state hacking unless the operation meets eleven fundamental, cumulative and non-negotiable conditions. We firmly believe that many hacking methods developed and currently available on the market, including the use of spyware as investigated by the PEGA

6 EDRi 'State access to encrypted data. A digital rights perspective.' (21 October 2022) https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf

Committee, do not meet *by nature* these eleven conditions, in particular the necessity and proportionality test (3.2.2). Their intrusiveness is such that they affect the essence of the right of privacy (as stated by the EDPS in its preliminary remarks on modern spyware and in recital AE of this Draft Report). No safeguard can mitigate the human rights violations they entail. Therefore, we strongly encourage the PEGA Committee to call for a ban on spyware technologies that risk affecting the essence of or that excessively interfere with fundamental rights as soon as possible in the European Union. For that, we suggest a list of characteristics that, based on our current knowledge of the market, usually make the recipe for such disproportionate interference in order to guide the European Commission in delimiting the scope of the ban.

Draft Recommendation	EDRi amendments
27. Takes the position that the trade in, and use of spyware needs to be regulated strictly; recognising however, that the legislative process will take considerable time, calls for the immediate adoption of a conditional moratorium on the sale, acquisition, transfer and use of spyware, that must be lifted on a country-by-country basis if the following conditions have been met:	**27b. Recognising** however, that the legislative process will take considerable time, calls for the immediate adoption of a conditional moratorium on the **export**, sale, acquisition, transfer**, servicing** and use of spyware, that must be lifted on a country-by-country basis if the following conditions have been met:
(a) all cases of alleged abuse of spyware are fully investigated and resolved without delay by the appropriate law enforcement, prosecutorial and judicial authorities; and	(a) all cases of alleged abuse of spyware are fully investigated and resolved without delay by the appropriate law enforcement, prosecutorial and judicial authorities; and
(b) proof that the framework governing the use of spyware is in line with the standards laid down by the Venice Commission and relevant case-law by the CJEU and ECtHR; and	(b) proof that the framework governing the use of spyware is in line with the standards laid down by the Venice Commission and relevant case-law by the CJEU and ECtHR; and
(c) the explicit commitment to grant any request by Europol pursuant to Art 6(1a) of the Europol Regulation relating to investigations into allegations of illegitimate use of spyware; and	~~**(c) the explicit commitment to grant any request by Europol pursuant to Art 6(1a) of the Europol Regulation relating to investigations into allegations of illegitimate use of spyware; and**~~
(d) repealing all export licences that are not fully in line with both the letter and the spirit of the Dual-Use Regulation;	(d) repealing all export licences that are not fully in line with both the letter and the spirit of the Dual-Use Regulation **including a human rights due process assessment**;
28. Considers that the fulfilment of the conditions must be assessed by the Commission;	28. Considers that the fulfilment of the conditions must be assessed by the Commission; **requires the Commission to base its assessment on public and targeted consultations with relevant national and international stakeholders including but not**

	limited to civil society and human rights organisations and representative groups of victims of surveillance; requests that the Commission make publicly available its decision and the underlying assessment in order to ensure transparency and accountability of the process;

Comments

EDRi sees the value of the Rapporteur's proposal for an intermediary moratorium, given the urgency of the matter and the imperative to stop as soon as possible further rights and freedoms violations from occurring. It is however unclear how Member States should submit "proof" that their legal framework is in line with the relevant international standards regulating state surveillance activities and on which criteria the European Commission should assess this. This assessment is traditionally the role of courts (i.e. the ECtHR and the CJEU). We therefore suggest to at least specify some process requirements for the Commission when it decides whether or not to lift the moratorium – which is an important power.

We recall that the Commission refuses to launch infringement procedures since many years against Member States which refuse to align their telecommunications data retention regimes with the CJEU case law[7] and deliberately circumvent it[8] – showing a political bias. Therefore we caution the PEGA Committee to entrust the Commission with decisive powers on the surveillance activities of Member States and invite it to elaborate means to hold the Commission accountable for its decisions and actions.

We suggest to delete the condition in paragraph (c) for the reasons stated below under the section 'The role of Europol'.

Draft Recommendation	EDRi amendments
New	**AFa. whereas the concept of "serious crime" has not been defined by EU law; whereas attempts to circumscribe serious crimes in EU law often take as a basis the gravity of the sanction notably by setting the threshold at a minimum maximum custodial sentence; whereas this threshold tends to encompass a broad range of offences, including petty crimes, which puts into question its validity and legitimacy to define serious crimes;**

7 Chloé Berthélémy, 'Europe's Data Retention Saga and its Risks for Digital Rights' Digital Freedom Fund (26 July 2021) https://digitalfreedomfund.org/europes-data-retention-saga-and-its-risks-for-digital-rights/

8 POLITICO, 'France seeks to bypass EU top court on data retention' (3 March 2021) https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/

	whereas the reviews of the EU Directive on Combating Terrorism by the EU Fundamental Rights Agency and civil society organisations have highlighted the issues arising from the overly broad definitions of terrorist offences that allow for application in ways that are discriminatory or violate human rights;
29. Considers that there is a clear need for common EU standards regulating the use of spyware by Member State bodies, drawing from standards laid down by the CJEU, ECtHR and the Venice Commission; considers that such EU standards should cover at least the following elements:	29. Considers that there is a clear need for common EU standards regulating the use of **the remaining** spyware **that are not subject to prohibition** by Member State bodies, drawing from standards laid down by the CJEU, ECtHR and the Venice Commission; considers that such EU standards should cover at least the following elements:
(a) the envisaged use of spyware must be subject to an effective and meaningful ex ante judicial authorisation by an impartial and independent judicial authority, having access to all relevant information, demonstrating the necessity and proportionality of the envisaged measure;	(a) the envisaged use of spyware must be subject to an effective and meaningful ex ante judicial authorisation by an impartial and independent judicial authority, having access to all relevant information, demonstrating the necessity and proportionality of the envisaged measure; **ex post judicial authorisation, even in emergency circumstances, should be explicitly ruled out;**
(b) the targeting with spyware should only last as long as is strictly necessary, the judicial authorisation beforehand should define the precise scope and duration and the hacking may only be extended when further judicial authorisation is granted for another specified duration, given the nature of spyware and the possibility of retroactive surveillance;	(b) the targeting with spyware should only last as long as is strictly necessary, the judicial authorisation beforehand should define the precise scope and duration and the hacking may only be extended when further judicial authorisation is granted for another specified duration, given the nature of spyware and the possibility of retroactive surveillance;
(c) the authorisation for the use of spyware may only be granted with respect to investigations into a limited and closed list of crimes, and spyware may only be used towards persons in relation to which there is sufficient indications that they have committed or are planning to commit such crimes;	(c) the authorisation for the use of spyware may only be granted with respect to investigations into a **narrow** and closed list of **clearly and precisely defined serious** crimes**; the list of serious crimes should be agreed based on specific criteria such as posing an immediate serious risk to health and safety of individuals; the list of serious crimes should be narrower than definitions in existing legislation such as the European Arrest Warrant Council Framework Decision and the Passenger Name Record Directive in light of the extremely serious interference with fundamental rights that deployment of spyware entails; the authorisation process for the use of spyware for crimes defined must include an assessment that the**
(d) there should be a non-exhaustive but binding list of privileged and sensitive professions, such as lawyers, journalists, politicians, and doctors that may not be targeted by spyware;	
(e) specific rules must be drawn up for surveillance with spyware technology given that it allows for unlimited retroactive access to messages, files and metadata;	

(f) Member States should publish, as a minimum, the number of requests for surveillance approved and rejected, and the type and purpose of the investigation and anonymously register each investigation in a national register with a unique identifier so that it can be investigated in case of suspicions of abuse;

(g) the right of notification for the targeted citizen: after the surveillance has ended, the authorities should notify the citizen of the fact that they were subject to the use of spyware by the authorities, including information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, data obtained, information on how that data has been used and by which actors as well as the date of deletion of the data; notes that such notification should be done without undue delay, unless an independent judicial authority grants delay of notification, in which case immediate notification would seriously jeopardise the purpose of the surveillance;

(h) an effective and independent ex post oversight over the use of spyware which must have all required means and powers to exercise a meaningful oversight and be coupled with a parliamentary oversight based on cross-party membership and full access to information;

(i) a meaningful legal remedy for direct and indirect targets and that individuals who claim to be adversely affected by surveillance should have access to redress through an independent body; calls, therefore, for the introduction of a duty of notification for state authorities, including appropriate timeframes for notification, whereby delivery occurs once the security threat has passed;

(j) legal remedies must be effective in both law and fact and that they must be known and accessible; stresses that such remedies require swift, thorough and impartial investigation by an independent oversight body and that this body should have access, expertise and technical capabilities to handle

proposed investigative measures should not breach the essence of the right to privacy or other fundamental rights such as the right to non-discrimination; Spyware may only be used towards persons in relation to which there is sufficient **objective** indications that they have committed or are planning to commit such crimes;

(ca) access to information obtained by spyware must be limited to the specific authorised authority for the sole original purpose of the operation and strictly limited for the duration authorised in the judicial process.

(cb) under the ongoing supervision of an independent judicial authority, any data obtained by spyware that is not relevant for the specific investigation for which the use of spyware was authorised must be immediately deleted;

(d) there should be a non-exhaustive but binding list of privileged and sensitive professions, **including but not limited to** lawyers, journalists, politicians, **human rights defenders** and doctors, **and any other activities where the targeting individuals or communities would constitute a threat to democratic practices and values and would lead to the silencing of critical voices and a larger chilling-effect on civic space,** that may not be targeted **directly or indirectly** by spyware;

~~**(e) specific rules must be drawn up for surveillance with spyware technology given that it allows for unlimited retroactive access to messages, files and metadata;**~~

(f) Member States should publish, as a minimum, the number of requests for surveillance approved and rejected, and the type and purpose of the investigation and anonymously register each investigation in a national register with a unique identifier so that it can be investigated in case of suspicions of abuse;

(g) the right of notification for the targeted **person:** after the surveillance has ended, the

all relevant data to be able to determine whether the security assessment made by the authorities of an individual is reliable and proportionate;

(k) the need to improve victims' free of charge access to technological expertise at this stage, since increased availability and affordability of technological processes, such as forensic analysis, would allow victims to present stronger cases in court;

(l) during surveillance, authorities should delete all irrelevant data and after the surveillance and the investigation for which the authorisation was granted has ended, authorities should delete the data as well as any related documents, such as notes that were taken during that period, such deletion must be recorded, and be auditable;

(m) Member States must notify each other in case of surveillance of citizens or residents of another Member State or of a mobile number of a carrier in another Member State; 30. Emphasises that only spyware that is configured so that it enables and facilitates the functionality of spyware according to the legislative framework according to Article 82 TFEU and in particular supporting the different roles of the authorities involved may be placed on the internal market, developed or used in the Union;

authorities should notify the **person** of the fact that they were subject to the use of spyware by the authorities, including information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, data obtained, information on how that data has been used and by which actors as well as the date of deletion of the data; notes that such notification should be done without undue delay, unless an independent judicial authority grants delay of notification, in which case immediate notification would seriously jeopardise the purpose of the surveillance;

(ga) the right of notification for non-targeted persons whose data were accessed: after the surveillance has ended, the authorities should notify the persons whose right to privacy has been severely interfered with through the use of spyware but were not the target of the operation of the fact that their data was accessed by the authorities, including information regarding the date and duration of the surveillance, the warrant issued for the surveillance operation, data obtained, information on how that data has been used and by which actors as well as the date of deletion of the data; notes that such notification should be done without undue delay, unless an independent judicial authority grants delay of notification, in which case immediate notification would seriously jeopardise the purpose of the surveillance;

(h) an effective and independent ex post oversight over the use of spyware which must have all required means and powers to exercise a meaningful oversight and be coupled with a parliamentary oversight based on cross-party membership and full access to information;

(i) a meaningful legal remedy for direct and indirect targets and that individuals who claim to be adversely affected by surveillance should have access to redress through an independent body; calls, therefore, for the introduction of a duty of notification for state authorities, including appropriate timeframes for notification, whereby delivery occurs once

the security threat has passed;

(j) legal remedies must be effective in both law and fact and that they must be known and accessible; stresses that such remedies require swift, thorough and impartial investigation by an independent oversight body and that this body should have access, expertise and technical capabilities to handle all relevant data to be able to determine whether the security assessment made by the authorities of an individual is reliable and proportionate;

(k) the **improvement of** victims' free of charge access to technological expertise at this stage, since increased availability and affordability of technological processes, such as forensic analysis, would allow victims to present stronger cases in court;

(ka) the reinforcement of the rights of the defence and the right to a fair trial by ensuring that those accused of crimes are allowed and able to check the accuracy, authenticity, reliability and even the legality of the evidence used against them and therefore rejecting any blanket application of national defence secrecy rules;

(l) during surveillance, authorities should delete all ~~**irrelevant**~~ data **that is not relevant to the specific authorised investigation** and after the surveillance and the investigation for which the authorisation was granted has ended, authorities should delete the data as well as any related documents, such as notes that were taken during that period, such deletion must be recorded, and be auditable;

(m) Member States must **seek and obtain the validation of** each other **via applicable police and judicial cooperation legal channels** in case of surveillance of citizens or residents of another Member State or of a mobile number of a carrier in another Member State;

Comments

- Para (a): State hacking and the use of spyware should never occur prior to judicial authorisation given the risks of privacy violation and the interferences with fundamental rights.

- Para (c): Only investigation and prosecution of extremely severe crimes, in narrowly defined and exceptional circumstances, could justify as legitimate aims in a democratic society the deployment of spyware (that are not prohibited by nature). To define which serious crimes should be eligible, we recommend to not take as a basis existing lists of categories of crimes in current EU legislation as they are too broadly defined and inadequate. This point is reinforced by the addition of a recital pointing out the problems identified[9] with current definitions of serious crimes and terrorism in EU law.

- Para (ca) and (cb): We suggest to add further limitations on the recipient of the data extracted with spyware, the duration of that access and rules for data deletion that reinforces proposals in the Draft Recommendation supporting data minimisation.

- Para (d): we recommend to enlarge the list of protected professions and activities to include those persons whose role and work are not officially recognised by States but that do contribute to the health of democratic society and the vitality of the civic space. We furthermore add cases where the operation targets these people indirectly (through the surveillance of their relatives).

- Para (e): we suggest to delete this paragraph as this type of spyware should fall into the prohibition scope introduced in para 27a.

- Para (g): we suggest to replace citizen by person as the legal status of the targeted individual should not prevent them to access effective remedies as this is a fundamental right guaranteed to all in the EU.

- Para (ga): we suggest to add another paragraph concerning the right to effective remedies of people not directly targeted but affected by the deployment of spyware. This can be merged with paragraph (g). However, we feel this obligation on authorities to notify third-persons is vitally important and needs to be clearly highlighted in the Parliament's position.

- Para (ka): we strongly recommend to strengthen the rights of the defence as the right to be notified is not sufficient to ensure access to a fair trial. Several recent operations of state hacking have shown how state authorities are applying very restrictive information and access rights on the grounds of 'defence secrecy'.[10]

9 By civil society: https://www.opensocietyfoundations.org/publications/joint-civil-society-report-on-the-fundamental-rights-impact-of-the-eu-directive-on-combatting-terrorism
By the EU Fundamental Rights Agency: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-directive-combating-terrorism_en.pdf

10 https://www.fairtrials.org/app/uploads/2022/02/EnroChat_LetterofConcern.pdf

- Para (m): In line with the EU existing judicial cooperation framework and the principles of mutual recognition, the deployment of spyware across borders should not happen without the review and *agreement* of the Member State having jurisdiction.

Development of and trade in spyware

Draft Recommendation	EDRi amendment
31. Stresses that spyware may only be placed on the market for sale to and use by a closed list of public authorities whose instructions include investigations of crimes for which the use of spyware may be authorised;	31. Stresses that spyware may only ~~**be placed on the market for sale to and used**~~ by a closed list of public authorities whose instructions include investigations of **serious crimes referred to in 27(c)** for which the use of spyware may be authorised.
32. Highlights the obligation to use a version of spyware that is programmed in such a way that it minimises the access to data, that the spyware should not have access to all data stored on a device, but should be programmed in such a way that it limits access to data to the minimum of what is strictly necessary;	32. **Highlights the obligation to always resort to the less intrusive surveillance measure available and only resort to the use of spyware when all alternatives have been proven to be insufficient in achieving similar results;** highlights the obligation to use a version of spyware that is ~~**programmed in such a way that it minimises the access to data, that the spyware should not have access to all data stored on a device, but should be**~~ programmed in such a way that it limits access to data to the minimum of what is strictly necessary; **if this limitation is not possible, then authorities should refrain from using the spyware tool at all; emphasises that automated data minimisation procedures cannot replace the need for manual review under independent judicial oversight that any information obtained by spyware not relevant to the specific authorised investigation is immediately deleted;**
33. Concludes that when a Member State has purchased spyware, the acquisition must be auditable to an independent, impartial audit body;	33. Concludes that when a Member State **develops** spyware, the **development** must be auditable to an independent, impartial audit body;
34. Stresses that all entities placing spyware on the internal market should comply with strict due diligence requirements, including vetting of potential clients and should report to the Commission on an annual basis on compliance;	34. **Delete**

Comments

It is EDRi's position that authorities– subject to transparency and accountability measures and human rights safeguards – that engage in any form of hacking must rely on their own internal

capacities and resources to carry out their operations while maintaining disclosure responsibility when discovering vulnerabilities. In particular, the search for vulnerabilities in software, devices, etc., as well as their exploitation and the execution of a hack, must not be outsourced to the private sector, domestic or foreign. The purpose here is to ensure public accountability. This restriction is primarily a limit on the use of spyware by raising the costs for each deployment operation. The issue of costs is considered in order to improve the proportionality of surveillance measures: it ensures that authorities only focus on the surveillance and investigations that are absolutely needed. We also strongly believe that the EU should stop directly or indirectly supporting an industry that sells information to cybercriminals as well as governments, or an industry that sells information to states that use it in an irresponsible way (like NSO did). Keeping the search for vulnerabilities "in house" for governments is the most straightforward way to ensure that the government procurement of vulnerability information which currently taking place does not contribute to information leakage to rogue states or cybercriminals.

We propose to reinforce the wording of para 33 by (1) restating the obligation to choose the least intrusive alternative possible as developed by the CJEU in relation to the principle of necessity, (2) highlighting the limits of automated solutions to minimise data access and stressing again the need for a manual review by an independent judicial authority. Lastly, the PEGA Committee should be aware that once spyware capabilities are permitted it is hard if not impossible and vain to minimise the tool's access to data.

Better enforcement of existing legislation

Draft Recommendation	EDRi amendment
46. Calls for changes to the Dual-use Regulation to ensure that transit is prohibited in cases where goods are or may be intended for internal repression and/or the commission of serious violations of human rights and international humanitarian law;	46. Call for changes to the Dual Use Regulation to ensure that transit is prohibited in cases where goods are or may be intended for internal repression and/or the commission of serious violations of human rights and international humanitarian law; **and to implement mandatory human rights due diligence in the licensing process, and further improvements such as remedy for victims of human rights abuses and transparent reporting of performed due diligence;**
47. Stresses that, in a future amendment of the Dual-use Regulation, designated national authorities responsible for the approval and denial of export licences for dual-use items should provide detailed reports including information on the dual-use item in question; the number of licences applied for, the name of the exporting country, a description of the export company and whether this company is a subsidiary; a description of the end user and	47. ~~**Stresses that, in a future amendment of the Dual-use Regulation,**~~ **Calls on** designated national authorities responsible for the approval and denial of export licences for dual-use items ~~**should**~~ **to** provide detailed reports **covering the last ten years** including information on the dual-use item in question; the number of licences applied for, the name of the exporting country, a description of the export company and whether this company is

destination; the value of the export licence; why the export licence was approved or denied; emphasises that these reports should be made public on a quarterly basis; calls for the set up of a dedicated standing parliamentary committee with access to classified information by the Commission, for the purpose of parliamentary oversight;	a subsidiary; a description of the end user and destination; **the nature** and value of the export licence; why the export licence was approved or denied; emphasises that these reports should be made public on a quarterly basis; calls for the set up of a dedicated standing parliamentary committee with access to classified information by the Commission, for the purpose of parliamentary oversight;

Comments

We propose to strengthen the wording calling for the reform of the Dual Use Regulation based on Access Now's and other civil society organisations' specific requests to meet the EU's human rights obligations and to prevent European-based surveillance companies from "licence shopping" among the states with weaker implementation of current export controls rules.[11]

The Dual Use Regulation following its recent re-cast already allows Member State authorities to publish this information. Other countries, such as Switzerland and the UK, have published such data on a quarterly basis for years, while EU Member States routinely publish such data pertaining to items on the military control list which are as sensitive as the surveillance items on the dual use control list. Transparency is core to and a preliminary requirement of any exercise and protection of human rights. Having access to this data would allow the public, national and European parliamentarians, and civil society to scrutinize decision making regarding the authorisation of license applications to ensure it is in line with national and EU legislation.

International cooperation to protect citizens

Draft Recommendation	EDRi amendment
New	**51a. Ensure all surveillance systems which pose a threat to human rights are subject to licensing requirements by ensuring there exists a transparent and consultative process for the addition of new items within the EU and Wassenaar Arrangement control lists, including systems specially designed to perform biometric identification of natural persons for security purposes;**
New	**52a. Calls for a white list and/or black list of spyware vendors (not) authorised to sell to public authorities, common criteria for vendors to be included in either list, arrangement reporting on the industry, scrutiny, common due diligence obligations for vendors and the criminalisation of the**

11 https://www.accessnow.org/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/

	sale of spyware to non-state actors;
New	**60a. Calls upon device manufacturers who place products with digital elements on the market to provide security software updates for the expected product lifetime or for a period of ten years from the placing of the product on the market, whichever is longer.**

Comments

At present, considerations for the addition of new technology within the EU control list are discussed by government representatives at the Wassenaar Arrangement with any decisions subsequently implemented within the EU control list. The decision to add a new item to the control list is not based on human rights concerns and there is no process at the Wassenaar Arrangement for consulting any civil society, parliamentary or other groups. This article would require the Commission to consult with stakeholders regarding the addition of additional items not currently subject to licensing requirements, such as a wide range of biometric surveillance technology including facial recognition systems.

Paragraph 52a would work in parallel with existing paragraph 51 but be used to include vendors who have a significant US presence which US authorities in the US may not want to blacklist but which nevertheless pose a risk.

Software is what keeps our devices secure, functional, compatible with the latest apps, and protected against known security vulnerabilities. Out-of-date software on an otherwise functioning device can render a device unusable, or worst still endanger safety and life even. Such a risk is enabled by software support periods that are shorter than the product's usable life cycle, and an industry focused only on selling its latest products rather than providing long-term software support for their older products. This is not a sporadic phenomenon; it is a practice deployed by most dominant actors in the digital markets for various categories of popular products.

Zero-day vulnerabilities

Draft Recommendation	EDRi amendment
57. Considers that researchers must be able to research vulnerabilities, and share their results without civil and criminal liability under inter alia the Cybercrime Directive and the Copyright Directive;	57. Considers that researchers must be able to research vulnerabilities, and share their results **with developers and maintainers of the software or systems and other security researchers** without civil and criminal liability under inter alia the Cybercrime Directive and the Copyright Directive;
New	**58a. Calls upon the Commission to ensure**

	adequate public funding for bugs bounty programmes for open and free software most commonly used in the Union in cases where the industry players do not provide sufficient incentives for security researchers to share vulnerability information with developers of the open and free software; calls upon the Commission to continue and expand the existing bugs bounty programmes under the Open source software strategy 2020-2023;
New	**60a. Notes that state actors have considerable funding available for buying zero-day vulnerability information; calls upon Member States and Union bodies to allocate this funding to security research for rapidly fixing software vulnerabilities to the benefit of all individuals and of the Union's cybersecurity overall capacities and resilience, rather than procuring and exploiting them for a limited time for the purpose of surveillance by spyware;**
61. calls for a ban for public authorities to purchase, keep open or stockpile vulnerabilities, except only in limited, specified cases with clear vulnerability equity processes, set in law, with necessity/proportionality test for the decision to disclose or exceptionally withhold a vulnerability, and strict rules on delaying notification, subject to strict oversight by an independent supervising body;	61. calls for a ban for public authorities to purchase, keep open or stockpile vulnerabilities, **without exception**, subject to strict oversight by an independent supervising body;

Comments

Since the Draft Recommendation proposes to regulate the discovery, sharing, patching and exploitation of vulnerabilities (paragraph 56) and ban the commercial trade in security vulnerabilities (paragraph 59), we suggest to clarify in paragraph 57 that security researchers should be free from criminal and civil liabilities when they do research and when they share vulnerability information with software vendors and other security researchers.

Industry actors should make sufficient incentives (bugs bounty programmes) available for security researchers to share vulnerability information with the relevant software vendors or developers. In some cases involving free and open software, there will not be sufficient funds for such programmes. Therefore, the private inventive programmes should be supplemented by public funding when this is necessary, The European Commission already has such a programme under the Open source software strategy 2020-23 which should be continued and expanded.[12]

12 https://commission.europa.eu/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-01-19_en

It is worth noting that considerable funding from states, presumably including EU Member States, is available for paying security researchers to find 0day vulnerabilities for exploit purposes and spyware deployment. The company Zerodium[13] acts as intermediary between security researchers and government institutions mainly in Europe and North America, keeping both sides of the transaction anonymous from each other. Zerodium currently offers payments up to 2.5 million dollars for vulnerability information, substantially above the bugs bounty programmes of the software industry. The state funding that supports these large payments from Zerodium and other intermediaries in the lucrative trade of vulnerability information for exploit purposes should, wherever possible, be redirected to fixing security vulnerabilities before they are exploited by bad actors, whether rogue states or criminals.

Regarding paragraph 61, the onerous consequences of vulnerabilities cannot be limited to specific instances, since their exploitation threatens the security of the Internet as a whole. What past cyberattacks have underlined is that hoarding system vulnerabilities might have onerous consequences for citizens across the whole Union. In addition, the introduction of such an exception, albeit well-intended, creates a serious risk of abuse by national authorities, as we have witnessed with other forms of surveillance for national security purposes.

Telecom networks

Draft Recommendation	EDRi amendment
63. Stresses that the current unlimited possibility for unknown individuals to buy any number for any country in the world available should be better regulated to make malicious activity more difficult to hide;	63. **Delete**

Comments

We propose deletion of paragraph 63 because SIM card registration and similar measures will disproportionately affect whistleblowers, journalists, activists, undocumented persons and other marginalised groups while providing little, if any, security benefit for telecom networks. Limiting access or anonymous access to telecom networks is not a suitable measure for protecting devices connected to these networks.

e-Privacy

Draft Recommendation	EDRi amendment
65. Calls for the rapid adoption of the e-Privacy Regulation in a way that fully reflects the case-law on the restrictions for national security and the need to prevent abuse of surveillance technologies, strengthens the fundamental right to privacy; points out that	65. Calls for the rapid adoption of the e-Privacy Regulation in a way that fully reflects the case-law on the restrictions for national security and the need to prevent abuse of surveillance technologies, strengthens the fundamental right to privacy **and to the**

13 Website: zerodium.com

the scope for surveillance should not go beyond the e-Privacy Directive;	**protection of terminal equipment by clarifying the scope of Article 8 in the legislative proposal to encompass state bodies**; points out that the scope for surveillance should not go beyond the e-Privacy Directive **and that derogations from the protections afforded by EU law should be strictly limited;**

The role of Europol

Draft Recommendation	EDRi amendment
14. (k) invite Europol to investigate all cases of alleged abuse of spyware;	14. (k) **Delete**
67. Calls on all Member States to commit to granting the proposals of Europol under the aforementioned article;	67. **Delete**
69. Calls for the revision of the Europol Regulation, so that in exceptional cases Europol can also start a criminal investigation without Member State consent, in cases where the national authorities fail or refuse to investigate and there are clear threats to the interests and security of the EU;	69. **Delete**

Comments

Europol does not have the powers under the EU treaties to start investigations against cases of abuse of spyware, either in Poland or in the EU. Revising the Europol Regulation in line with what paragraph 69 proposes would clearly go against Europol's legal basis (Article 88(2)). This would also contradict the spirit of the EU treaties, according to which the European Union may not carry out police operations on the territory of a member state unless the latter expressly invites it to do so. We therefore suggest to delete these paragraphs.

Furthermore, the way Europol fundamentally operates by receiving and sharing data obtained in majority from and to the Member States makes it an ill-suited actor to start a criminal investigation without Member State consent. Firstly, it would face many obstacles as it would remain dependent from Member States' good will to share information and would be most likely be prevented from collecting relevant evidence if the crime perpetrator is a national authority – undermining the efficiency of the investigation. Secondly, it would never be fully independent and free from political capture. Lastly, it would be difficult to see to which judicial authority/court Europol would eventually submit the evidence collected (case file): there is no entity with such mandate at EU level.

EDRi has been advocating against the reform of Europol's mandate[14] and opposed the expansion of its powers as we consider the agency already lacks accountability and transparency. We, as civil society, do not believe that bolstering policing infrastructures at European level will solve the political issues raised by the spyware scandals: the lack of red lines and safeguards in national laws against state hacking, the undermining of the rule of law, the weak oversight mechanisms, etc.

Union research programmes

Draft Recommendation	EDRi amendment
82. Calls for the implementation of more rigorous control mechanisms to ensure that Union research funds do not fund or facilitate tools that infringe on EU values; notes that assessments of compliance with Union law should contain specific control criteria to prevent such abuses;	82. Calls for the implementation of more rigorous control mechanisms to ensure that Union research funds do not fund or facilitate tools that infringe on EU values; notes that assessments of compliance with Union law should contain specific control criteria to prevent such abuses; **calls for any entities which have been credibly reported to be involved in provision of surveillance in violation of human rights standards to be blacklisted from access to research funds.**

Comments

Ensuring such entities are prohibited from accessing EU research funds will ensure such programmes do not facilitate the development of new technology and act as a deterrent to such entities.

14 https://edri.org/wp-content/uploads/2021/06/Recommendations-on-the-revision-of-Europols-mandate.pdf