Proposal for a European Media Freedom Act (EMFA)

EDRi amendments and recommendations

Table of content

Introduction.....3

Article 2 - Definitions.....5

Article 4 - Rights and protection of journalists.....8

This document was put together by Sebastian Becker and Chloé Berthélémy (EDRi) with the input of Jesper Lund (IT-Pol Denmark), Rand Hammoud, Eliska Pirkova, Estelle Massé and Natalia Krapiva (Access Now), and Rebecca White (Amnesty Tech).

Date of publication: 20 April 2023

Introduction

In the context of the "new push for EU Democracy",[1] the European Commission released on September of 2022 its legislative proposal for a European Media Freedom Act (EMFA), which seeks in part to protect journalists and media services providers through the introduction of safeguards against their targeting by Member States governments with spyware.

EDRi welcomes the Commission's attempt to regulate the surveillance powers of states against journalists and journalistic sources. The abuse of power by governments, intelligence services and law enforcement agencies in the EU, illustrated by the Pegasus[2] and Predator[3] spyware cases and well documented in the upcoming report of the European Parliament's Committee of inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA), highlights the importance to have strong, common European measures to protect journalists, journalistic sources and human rights defenders.

The mere risk of being targeted with spyware endangers the media function of "public watchdogs" in a democratic society due to the chilling effect this may have on their freedom of expression and their contribution to the public debate. Surveillance has therefore an acute impact on democracy and the rule of law.

In addition, its chilling effect disproportionately impacts women and gender-diverse journalists, who are exposed to online gender-based violence which manifests in different ways, such as sexist and misogynistic abuse; targeted harassment, cyber-stalking, defamation, blackmail, direct or indirect threats of physical or sexual violence; and violation of privacy in the form of doxing or the dissemination of sexual or private images without consent. There is also an intersectional dimension, where racialised women, women from ethnic or religious minorities, lesbian, bisexual, transgender women as well as gender diverse individuals, and women with disabilities are exposed to unique and compounded forms of online gender based violence.[4]

In light of this, EDRi supports the need to include in the scope of the EMFA strong protections for digital rights and digital security in order to guarantee journalists' right to privacy, the protection of their sources, their work and the confidentiality of their private communications.

We believe that the general rule is the prohibition of surveillance. Exceptions of this basic and

---

1 European Commission, "New push for Democracy", Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy_en

2 POLITICO, "Pegasus used by at least 5 EU countries, NSO Group tells lawmakers", June 21, 2022. Available at: https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/

3 Inside Story, "Who was tracking the mobile phone of journalist Thanasis Koukakis?", 11 April 2022,. Available at: https://insidestory.gr/article/who-was-tracking-mobile-phone-journalist-thanasis-koukakis

4 Marwa Fatafta, 'Unsafe anywhere: women human rights defenders speak out about Pegasus attacks' (17 January 2022) https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/

fundamental rule should be strictly limited to only the most serious cases. In order to align the proposal with fundamental rights standards based on the jurisprudence of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), EDRi suggests to introduce clear requirements of necessity and proportionality and other essential procedural safeguards.

In its current version, the proposal risks legalising routine deployment of spyware and other repressive measures involving or not surveillance technologies against journalists. This is due to the largely broad and undefined scope of safeguarding "national security", an area of exclusive competence of the Member States. Yet, it has been demonstrated how Member States have abused this notion of national security to impose mass surveillance or other exceptional repressive measures, not just in pursuit of fighting terrorism, but also for social and political control.[5] It is therefore not acceptable that EU law endorses the "ground of national security" to justify the use of spyware against journalists. This exception counteracts the desired effect to protect journalists given that Member States may hide behind this pretext to abuse their surveillance powers. The cases of Pegasus and Predator in the EU are crystal-clear examples of these abuses.

We acknowledge the limited scope and regulatory reach of this legislative proposal. The EMFA is not the right instrument to introduce a general and EU-wide prohibition on the development, trade-in and use of spyware, as per our call to the PEGA Committee for an EU-wide ban on spyware.[6] Nevertheless, this Regulation should lay out the EU's clear stance against such invasive and excessively intrusive surveillance tools and their disproportionate impact on the essence of fundamental rights, as argued by the European Data Protection Supervisor (EDPS) in his preliminary remarks on modern spyware.[7]

Finally, it is crucial to include proactive measures to ensure meaningful protections for journalists in digital contexts. This regulation is a unique opportunity to promote anonymity, privacy-enhancing and digital security tools with the aim to ensure that journalists can work safely despite continuous threats of electronic surveillance. In light of this, we suggest the EMFA to include a specific obligation for Member States to ensure the protection and promotion of confidentiality of communications and end-to-end encrypted services.

To sum up, EDRi is proposing a series of amendments to strengthen the protection of journalists in digital contexts. The following provisions seek to follow strict human rights safeguards that will permit media services providers and journalists to embrace their vital "public watchdog" role

---

5 Laureline Lemoine, 'Data retention: "National security" is not a blank cheque' EDRi (29 January 2020) https://edri.org/our-work/data-retention-national-security-is-not-a-blank-cheque/

6 EDRi, 'PEGA Committee must call for an EU-wide ban on spyware' (21 February 2023) https://edri.org/our-work/pega-committee-must-call-for-an-eu-wide-ban-on-spyware/

7 EDPS, 'Preliminary Remarks on Modern Spyware' (15 February 2022) https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en

in EU democracies. EDRi stay at the disposal of the Members of the European Parliament and other stakeholders to work together towards improving this important legislation based on a truly human rights-centred and democratic approach.

Article 2 - Definitions

Commission's proposal	**EDRi amendment**
(new)	**Having regard to the preliminary remarks on modern spyware of the European Data Protection Supervisor,**
Article 2 (16)	
(16) 'spyware' means any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons by monitoring, extracting, collecting or analysing data from such products or from the natural or legal persons using such products, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices, without the natural or legal person concerned being made aware in a specific manner and having given their express specific consent in that regard;	**(16)** ~~'spyware' means any product with digital elements specially designed to exploit vulnerabilities in other products with digital elements that enables the covert surveillance of natural or legal persons~~ **'surveillance technologies' means any electronic, mechanical, or other surveillance device that enable the acquisition of information** by monitoring, extracting, collecting or analysing data ~~from such products or from the~~ **of any information and communication technology,** ~~natural or legal persons using such products, in particular by secretly recording calls or otherwise using the microphone of an end-user device, filming natural persons, machines or their surroundings, copying messages, photographing, tracking browsing activity, tracking geolocation, collecting other sensor data or tracking activities across multiple end-user devices,~~ without the natural or legal person concerned being made aware in a specific manner and having given their express specific**, free and informed** consent in that regard;
Recital 16a	
(new)	**(16a) Surveillance methods deployed against journalists are varied, such as interception of electronic communications and metadata, device or software hacking including denial of service attacks, wiretapping, bugging, videotaping, geolocation tracking via Radio-frequency identification (RFID), Global Positioning System (GPS) or cell-site data, data mining and social media monitoring. These techniques may gravely impact journalists' rights to privacy, data protection**

	and freedom of expression. The protections afforded by this Regulation therefore encompass current forms of digital surveillance but also future technologies that may appear along with technological innovation and they are without prejudice to the application of existing and future Union's law that restricts or prohibits the development, trade in, and use of specific surveillance technologies deemed too invasive. Considering the preliminary remarks of the European Data Protection Supervisor on modern spyware, spyware which grant full unlimited access to personal data, including sensitive data, on a device could affect the very essence of the right to privacy, and thus should under no circumstance be considered necessary and proportionate under Union law.

Comments

EDRi supports a comprehensive definition of surveillance in order to protect journalists and human rights defenders. This extended definition aims to specify the various forms of surveillance that journalists and media service providers may be facing by including not only the current, documented methods (e.g. wiretapping, phishing attacks, malware) but also new ones that may appear in the future via the emergence of new technologies. We propose the concept of "surveillance technologies" as used in the original recital (recital 16, Commission's proposal). Finally, we propose a new recital (16a) to illustrate and give examples of the different types of surveillance methods and tools that the definition encompasses in its scope.

It is our opinion that the EU legislator should urgently adopt a ban on the deployment of so-called 'spyware'.[8] Given the grave interference these tools entail with fundamental rights, the EU should not create a two-tier system: everyone including journalists should not become the target of state surveillance through spyware. It is crucial for the EU to complement the protections afforded by the EMFA with a new regulation prohibiting Member States' use of surveillance methods and practices that are irreconcilable with fundamental rights standards and international legal instruments.

Commission's proposal	**EDRi amendment**
Article 2 (17)	
(17) 'serious crime' means any of the following criminal offences listed in Article 2(2) of	(17) 'serious crime' means any of the following criminal offences listed in Article 2(2) of

8 EDRi, 'PEGA Committee must call for an EU-wide ban on spyware' (21 February 2023) https://edri.org/our-work/pega-committee-must-call-for-an-eu-wide-ban-on-spyware/

the Council Framework Decision 2002/584/JHA58: (a) terrorism, (b) trafficking in human beings, (c) sexual exploitation of children and child pornography, (d) illicit trafficking in weapons, munitions and explosives, (e) murder, grievous bodily injury, (f) illicit trade in human organs and tissues, (g) kidnapping, illegal restraint and hostage-taking, (h) organised or armed robbery, (i) rape, (j) crimes within the jurisdiction of the International Criminal Court.	the Council Framework Decision 2002/584/JHA58: (a) terrorism **as defined in Directive (EU) 2017/541 of the European Parliament and of the Council,** (b) trafficking in human beings, (c) sexual exploitation of children and child pornography, (d) illicit trafficking in weapons, munitions and explosives, (e) murder, grievous bodily injury, (f) illicit trade in human organs and tissues, (g) kidnapping, illegal restraint and hostage-taking, **~~(h) organised or armed robbery,~~** (i) rape, (j) crimes within the jurisdiction of the International Criminal Court.

Comments

Unregulated surveillance can lead to severe violations of fundamental rights when the practices do not respect the principles of necessity and proportionality. Exceptions to the general rule of non-state interference should be strictly limited and regulated. According to the Court of Justice of the European Union case law, only severe forms of criminality can justify surveillance and other intrusive measures. Rules defining legal interferences with journalists' rights and freedoms should therefore be based on the aforementioned principles and provided for in law, which require them to be clear, precise and predictable as regards their effects. Only explicit and concrete exceptions are allowed under EU law.

We note the Commission's attempt to clearly define which circumstances could justify such exceptions, based on the list of criminal offences provided for by the European Arrest Warrant (EAW) Council Framework Decision (FD) 2002/584/JHA58. We welcome the proposal for a shorter, more restricted list of eligible criminal offences as in the EAW FD, showcasing the Commission's awareness of the very severe interferences entailed by the deployment of surveillance technologies against journalists and the wider implications they have for the quality of our democracy.

However, we believe the threshold should be reinforced to provide stronger protection for the exercise of media freedoms and to avoid a fragmented implementation by Member States due to diverging national interpretations. Based on the proportionality test, EDRi believes that "organised or armed robbery" is too broad and does not meet the quality-of-law requirements of specificity, accessibility and foreseeability. It may also encompass less serious crimes in certain Member States. Furthermore, it does not fulfil the threshold to justify the surveillance of media workers, media service providers or journalists in the context of their journalistic work. The severity of such infringement is not proportionate to the harm to fundamental rights and democratic society resulting from authorising access to the state.

Please note that we also add in Article 4 (below) a further requirement to limit circumstances under which interferences in journalists' rights and freedoms would be justified in a democratic society in order to pass the proportionality test.

Article 4 - Rights and protection of journalists

Commission's proposal	**EDRi amendment**
Article 4 Rights of media service providers	
2. Member States shall respect effective editorial freedom of media service providers. Member States, including their national regulatory authorities and bodies, shall not:	2. Member States shall respect effective editorial freedom of media service providers. Member States, including their national regulatory authorities and bodies, shall not:
(b) detain, sanction, intercept, subject to surveillance or search and seizure, or inspect media service providers or, if applicable, their family members, their employees or their family members, or their corporate and private premises, on the ground that they refuse to disclose information on their sources, unless this is justified by an overriding requirement in the public interest, in accordance with Article 52(1) of the Charter and in compliance with other Union law;	(b) detain, sanction, intercept, subject to surveillance, or search and seizure, or inspect media service providers **and their employees** or, if applicable, their family members **and any other subject belonging to their professional and private network of relationships,** ~~**or their employees or their family members**~~ or **their sources,** or their corporate and private premises ~~**on the ground that they refuse to disclose information on their sources,**~~ unless ~~**this is justified by an overriding requirement in the public interest**~~ : • **there are valid reasons to believe that such measures, would prevent or enable the prosecution of a serious criminal offence listed under Article 2(17) of this Regulation and constituting an imminent concrete threat to a person's life or an attempt on the person's mental or physical safety;** • **a prior review is carried out on a case-by-case basis by a court delivering a duly reasoned decision based on a fair balance between the interests of enforcing criminal law and the fundamental rights affected by the measure, including in case of disclosure of journalistic sources ; and** • **the measure is provided for by law in accordance with Article 52(1) of the Charter, and in compliance with other Union law; and** • **defence rights and the right to access**

	to effective legal remedies are ensured in accordance with Article 47 of the Charter and in compliance with other Union law.
(c) deploy spyware in any device or machine used by media service providers or, if applicable, their family members, or their employees or their family members, unless the deployment is justified, on a case-by-case basis, on grounds of national security and is in compliance with Article 52(1) of the Charter and other Union law or the deployment occurs in serious crimes investigations of one of the aforementioned persons, it is provided for under national law and is in compliance with Article 52(1) of the Charter and other Union law, and measures adopted pursuant to sub-paragraph (b) would be inadequate and insufficient to obtain the information sought.	**(c) force access to ~~deploy spyware in any device or machine used by~~** any device **~~or machine~~** used by or **deploy surveillance technologies against** media service providers **and their employees** or, if applicable, their family members **and any other subject belonging to their professional and private network of relationships**, **or their sources, where it might lead to access to information protected by professional secrecy, without exception. ~~unless the deployment is justified, on a case-by-case basis, on grounds of national security and is in compliance with Article 52(1) of the Charter and other Union law or the deployment occurs in serious crimes investigations of one of the aforementioned persons, it is provided for under national law and is in compliance with Article 52(1) of the Charter and other Union law, and measures adopted pursuant to sub-paragraph (b) would be inadequate and insufficient to obtain the information sought.~~**
(new)	**2b. Member States shall ensure the promotion and protection of confidentiality of communications and of end-to-end encrypted services in particular in media service providers communications.** **The use of encrypted and anonymisation tools by media service providers and their employees shall be encouraged and shall not be considered a valid reason for suspicion for the adoption of measures pursuant to subparagraph (b).**
Recital 16	
(16) Journalist and editors are the main actors in the production and provision of trustworthy media content, in particular by reporting on news or current affairs. It is essential therefore to protect journalists' capability to collect, fact-check and analyse information, including information imparted confidentially. In particular, media service providers and journalists (including those operating in non-standard forms of employment, such as	(16) Journalists, **~~and~~** editors **and media workers** are the main actors in the production and provision of trustworthy media content, in particular by reporting on news or current affairs. It is essential therefore to protect journalists' capability to collect, fact-check and analyse information, including information imparted confidentially. In particular, media service providers, **media workers and** journalists (including those

freelancers) should be able to rely on a robust protection of journalistic sources and communications, including against deployment of surveillance technologies, since without such protection sources may be deterred from assisting the media in informing the public on matters of public interest. As a result, journalists' freedom to exercise their economic activity and fulfil their vital 'public watchdog' role may be undermined, thus affecting negatively access to quality media services. The protection of journalistic sources contributes to the protection of the fundamental right enshrined in Article 11 of the Charter.	operating in non-standard forms of employment, such as freelancers) should be able to rely on a robust protection of journalistic sources and communications, including against **arbitrary interferences and** deployment of surveillance technologies, since without such protection sources may be deterred from assisting the media in informing the public on matters of public interest. **This chilling effect is more pronounced for women and gender-diverse journalists, particularly women from marginalised groups such as racialised women, women from ethnic or religious minorities, LGTBI+ individuals and women with disabilities.** As a result, **media workers and** journalists' **freedom of expression** ~~to exercise their economic activity~~ and **capacity to** fulfil their vital 'public watchdog' role may be undermined, thus affecting negatively access to quality media services. The protection of journalistic sources **is a fundamental condition for** the protection of the fundamental right enshrined in Article 11 of the Charter. **The added value of the protection of journalistic sources and whistleblowers against criminalisation, retaliation and undue surveillance has already been acknowledged by the Union legislator in the Directive (EU) 2019/1937. In addition, the role of non-governmental organisations in informing the public and in exposing and preventing serious threats or harms to the public interest, which often relies on information provided by academics, whistleblowers and other sources, should also be acknowledged and therefore, they should receive an equal level of protection under this Regulation.**
	Recital 16b
(new)	**(16b) The use of surveillance technologies or coercion to access journalists' data protected by professional privilege and linked to secrecy obligations should never be considered necessary and proportionate in a democratic society given the gravity of the interference they entail with media freedoms. They undermine the role of public watchdog of journalists and the fundamental role of journalistic sources to the protection of freedom of expression enshrined in Article**

	11 of the Charter in an unacceptable way.
Recital 17	
(17) The protection of journalistic sources is currently regulated heterogeneously in the Member States. Some Member States provide an absolute protection against coercing journalists to disclose information that identify their source in criminal and administrative proceedings. Other Member States provide a qualified protection confined to judicial proceedings based on certain criminal charges, while others provide protection in the form of a general principle. This leads to fragmentation in the internal media market. As a result, journalists, which work increasingly on cross-border projects and provide their services to cross-border audiences, and by extension providers of media services, are likely to face barriers, legal uncertainty and uneven conditions of competition. Therefore, the protection of journalistic sources and communications needs harmonisation and further strengthening at Union level.	(17) The protection of journalistic sources is currently regulated heterogeneously in the Member States. Some Member States provide an absolute protection against coercing journalists to disclose information that identify their source in criminal and administrative proceedings. Other Member States provide a qualified protection confined to judicial proceedings based on certain criminal charges, while others provide protection in the form of a general principle. This leads to fragmentation in the internal media market. As a result, journalists, which work increasingly on cross-border projects and provide their services to cross-border audiences, and by extension providers of media services, are likely to face barriers, legal uncertainty and uneven conditions of competition. Therefore, the protection of journalistic sources and communications needs harmonisation and further strengthening at Union level, **without weakening the current protection in any Member State. Journalists working on cross-border projects should benefit from the highest protection standards of the Member States involved.**
	Recital 17b
(new)	**(17b) Digital safety and the confidentiality of electronic communications have become a major concern for journalists. In light of this, the promotion and protection of anonymisation tools and end-to-end encrypted services used by media service providers and their employees needs to be encouraged at European level to ensure an equal level of access to such equipment across all Member States. These tools have become vital for many journalists to freely exercise their work and their rights to privacy, data protection and freedom of expression including by securing their communications and protecting the confidentiality of their sources.**

Comments

In its current form, Article 4.2 risks legalising the arbitrary deployment of surveillance technologies against journalists and giving a blank cheque to Member States in terms of defining the circumstances under which it should be considered lawful and what safeguards should be applied.

The interference with the fundamental rights of journalists, media workers and journalistic sources should fulfil the principles of legality, proportionality and necessity. In light of this, we suggest to strengthen the provision of Article 4 to guarantee the same level of protection in EU law and across the EU. We propose the following standards to protect journalists from arbitrary repressive measures: an ex-ante review by an independent court which should deliver a reasoned decision for granting authorisation to the deployment of any state interference measures; an explicit mention to the principle of necessity and proportionality; and a definition of the strictly defined legitimate aims that would pass the proportionality test (the prosecution of serious crimes and the existence of an imminent concrete threat to someone's life or mental or physical safety).

Given the important risks for fundamental rights, including the right to life, that any measure leading to the disclosure of journalistic sources entails (retaliation, political prosecution, etc.), we add these specific requirements in order to make those measures the last resort in narrowly-defined, exceptional cases and incentivise the use of less intrusive alternatives that could equally achieve the same objectives. In particular the interest in disclosure (the prevention and prosecution of very serious cases of criminality) should always be balanced against the harm to freedom of expression and other fundamental rights at issue. For example, courts should never order disclosure of a source's identity in the context of a defamation case.

The requirement of the existence of a threat to life is an important addition given that the "serious crime" definition in Article 2(17) already covers criminal activities that affect "national security" such as "terrorism" or "illicit trafficking in weapons, munitions and explosives". Member States often abuse the "national security" card to justify very intrusive policies – yet, the CJEU established in its case law on general and indiscriminate data retention that the mere fact that a national measure has the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.[9]

In addition, we recall that EDRi and other civil society have also repeatedly expressed concerns with regards to the vague and broad definitions of terrorist acts in EU law.[10] The interpretation of the definition of terrorism remains very disparate among European States, despite legal attempts to clarify and harmonise it. These vague definitions permit states to criminalise, as terrorism, public protests or other peaceful acts that they deem 'seriously destabilise the fundamental political, constitutional, economic or social structures of a country or an international organisation.'

---

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

10 https://www.icj.org/wp-content/uploads/2016/11/EU-Press-Release-Flawed-Counterterrorism-Directive-2016-ENG.docx.pdf

https://edri.org/our-work/eu-terrorist-content-online-regulation-could-curtail-freedom-of-expression-across-europe/

With regards to the protection of sources, on the one hand, media workers and journalists play a crucial role as public watch-dogs, on the other hand, the protection of journalistic sources is a fundamental condition for the protection of the fundamental right enshrined in Article 11 of the Charter. In light of this, both subjects should be protected with the same guarantees of protection. The EMFA should also not restrict the protections it affords only in cases where media service providers or their employees have refused to disclose information on their sources but they should apply in all circumstances.

The current methods of digital surveillance that lead to the access of virtually all personal data on a device (communications, photos, online behaviour and preferences, etc.), including malware such as spyware[11], entail such a disproportionate level of interference with the right to privacy that "in fact deprive of it"[12]. Other methods can lead to the disclosure of sources' identity (such as geolocation tracking where journalists meet their sources in person) or access to material protected by professional privilege under national law (such as installing a keylogger or using a Universal Forensics Extraction Device (UFED)). These surveillance practices lead to an unacceptable level of interference with media freedoms in a democratic society and severely undermine the vital public-watchdog role of the press by adversely affecting its ability to provide accurate and reliable information.[13] We therefore strongly believe that forcing access to a device by the use of coercion or deceit or deploying any form of targeted digital surveillance against journalists or anybody in contact with them in order to access their communications or protected material do not pass the proportionality test and should therefore be prohibited in the EMFA.

Finally, in order to fulfil obligations under EU law, the regulation should be put in place sufficiently robust safeguards to prevent violations of Article 7 and Article 10 of the Charter of Fundamental Rights. Following from this, the Regulation should ensure and promote the use of encrypted, privacy-enhancing and anonymisation tools by journalists. Notably the use of end-to-end encryption is to be encouraged and protected by Member States – abandoning any attempt to weaken these systems. A general provision to protect confidentiality of communications and specifically protecting end-to-end encryption (E2EE) is thus essential.

---

11 EDRi calls a general, EU-wide ban on the development, trade in and use of spyware: https://edri.org/our-work/pega-committee-must-call-for-an-eu-wide-ban-on-spyware/

12 European Data Protection Supervisor, "Preliminary Remarks on Modern Spyware", 15 February 2022, Available at: https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

13 See the case law of the ECtHR since 1996 in the case of Goodwin v. the United Kingdom.