****

**United Nations Special Rapporteur on Freedom of Opinion and Expression**

**Call for Comments on opportunities, challenges, and threats to media in the digital age to inform thematic report to the U.N. Human Rights Council**

26 January 2022

**Introduction**

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Special Rapporteur on the promotion and protection of freedom of opinion and expression to inform the Special Rapporteur’s thematic report on challenges, opportunities, and threats of media in the digital age to be presented to the U.N. Human Rights Council.[[1]](#footnote-1) As an ECOSOC accredited organisation, Access Now routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.[[2]](#footnote-2)

This submission addresses the key trends that threaten media freedom, as well as the viability and the safety of journalists online and offline. This submission specifically addresses (1) the trends, threats, and challenges of digital and social media platforms; (2) relevant insights from Access Now’s Digital Security Helpline; (3) persecution of journalists, online and offline, through the deployment of surveillance technologies and spyware, with a particular section dedicated to (4) surveillance as a form of violence against women followed by (5) best practices: technology company leadership in litigation against NSO Group. Drawing upon specific regional case studies, this submission then delves into (6) the weaponizing draconian extremism and Foreign Agent laws to stifle free expression and shut down independent media, with a particular focus on Russia’s Foreign Agent Laws, followed by (7) cybercrime and criminal laws used to persecute journalists in Africa and MENA and (8) the impact of internet shutdowns on the work of the media. We conclude with a series of recommendations for various stakeholders, including States, the private sector, and international organizations.

It is important to note that while this submission draws upon examples from various regions worldwide, including gender dimensions, these examples are non-exhaustive, and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly targeted.

***Practices of digital and social media platforms: trends, threats, and challenges***

1. Governments and companies are under increasing pressure to address illegal or undesirable content and expression online, but hasty or poorly crafted solutions can threaten human rights. Laws, policies, and content moderation practices that hurt free expression have a disparate impact on those most at risk of human rights violations, including journalists, and particularly journalists who are also members of oppressed or marginalized groups, such as women, religious or ethnic minority groups, people of colour, and the LGBTQ community. It is important to also note that all sorts of independent media workers engage in journalism and suffer the same threats as professional journalists, though often without the institutional resources and legal backing of their professionally-affiliated colleagues.
2. Companies make decisions about whether content is removed or amplified on their platforms, and follow their own rules, often in ways that are not transparent. Their actions — or lack of action — regarding content can cause or contribute to societal harm. Their role in spreading hate speech, disinformation, and illegal content, as well as facilitating discrimination, under a profit motive, is increasingly concerning.[[3]](#footnote-3)
3. Access to platforms is a lifeline in times of emergencies and social media is also a key tool for ensuring access to information for community organizing, peace-building and political participation. As the government of Kenya recently declared to the U.N. Security Council “...platforms have changed how most people find and interpret information.”[[4]](#footnote-4) Social media’s value in disseminating information must therefore be recognized in order for all stakeholders to call on social media companies’ to perform better.[[5]](#footnote-5)

***Insights from Access Now’s Digital Security Helpline***

1. Access Now’s Digital Security Helpline is a free-of-charge resource for civil society around the world. We offer real-time, direct technical assistance and advice to civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders.[[6]](#footnote-6) Our July 2021 report *Strengthening Civil Society’s Defenses: What Access Now’s Digital Security Helpline has Learned from its first 10,000 Cases,* reflected on Helpline cases from 2013 to 2021. Far from alone, Access Now’s Helpline joins a growing ecosystem of help desks, independent content providers, and digital support services for civil society, convened under the CiviCERT banner.[[7]](#footnote-7)
2. Women are often targets of harassment, doxxing, censorship, and other forms of gender based violence online. Organizations and groups working to defend women’s rights face additional challenges. Not only are they working to protect women, they are also working to protect themselves from the same kind of violence. Out of all cases the Helpline has handled related to women’s rights organizations, **63% came in response to adverse incidents, with the largest number of cases (23.6%) related to account compromise, followed by harassment (9.4%) and censorship (7.6%). Facebook was the platform where Helpline beneficiaries reported the most attacks (20.5% of cases), followed by Twitter (10.3%) and Instagram (8.9%).** These findings provide evidence to show that women’s rights organizations (and women in general) continue to be disproportionately targeted for attack on social media platforms.
3. Over the years, we have received and investigated reports of **more than 161 potential malware attacks**. Among our Helpline beneficiaries, **the people most likely to be targeted for malware attacks were journalists and independent media**, followed by NGOs working to defend human rights. The actors who target these groups often use off-the-shelf surveillance technology, and the Helpline team works with other parts of Access Now to hold the companies that make these products accountable for facilitating human rights violations.[[8]](#footnote-8) Many of the countries where victims are targeted — such as Mexico, Saudi Arabia, and Turkey — have been the site of surveillance and spyware campaigns linked to state actors.[[9]](#footnote-9)

***Persecution of journalists, online and offline: deploying surveillance technology and spyware***

1. The recent investigations into the surveillance industry exposes the digital security risks imposed on journalists voicing issues that often question authority. On 18 July 2021, Amnesty International and Forbidden Stories released a major investigation into the leak of 50,000 phone numbers of potential NSO Group surveillance targets that exposed potential NSO clients in 11 countries, including Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates.[[10]](#footnote-10) Amnesty’s Security Lab found traces of NSO’s surveillance software, Pegasus, on 37 out of 67 phones they were able to examine, belonging to journalists and human rights defenders, as well as their families and loved ones.[[11]](#footnote-11) French authorities later independently confirmed that Pegasus spyware has been found on the phones of three journalists, including a senior member of staff at the country’s international television station France 24.[[12]](#footnote-12) While the company claims its spyware is only used for legitimate criminal and terror investigations, it is evident that its technology facilitates systemic abuse. In response to the NSO case, the U.N. High Commissioner for Human Rights, stated that “governments should immediately cease their own use of surveillance technologies in ways that violate human rights, and should take concrete actions to protect against such invasions of privacy by regulating the distribution, use and export of surveillance technology created by others.”[[13]](#footnote-13)
2. On 12 January 2022, Access Now, in partnership with The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, and contribution from Amnesty International, Front Line Defenders, Fundación Acceso, and SocialTIC, uncovered the hacking of 37 devices belonging to 35 individuals with NSO Group’s Pegasus spyware.[[14]](#footnote-14) Twenty three of those devices belong to professionals affiliated with the regional media group El Faro, and four to the national media group, Gato Encerrado. El Faro and Gato Encerrado are independent investigative outlets that have often published reporting that is critical of the Salvadoran government’s actions. Other infected devices belong to the following media outlets: La Prensa Gráfica (one device), Revista Digital Disruptiva (one device), El Diario de Hoy (one device), El Diario El Mundo (one device), and one devices each belonging to two independent journalists. The rest of the infected devices belong to members of 4 NGOs. **Almost half of the victims identified in the El Salvador revelations are women.**

***Surveillance as a form of violence against women***

1. On 17 January 2022, Access Now, in partnership with the forensic investigation of Front Line Defenders, The Citizen Lab, and Amnesty International, revealed the hacking of **two women human rights defenders (WHRDs) from Bahrain and Jordan using NSO Group’s Pegasus spyware**.[[15]](#footnote-15) First, Front Line Defenders examined the mobile device of Bahraini human rights defender, **Ebtisam Al-Saegh**, and found that her iPhone had been hacked with NSO Group’s Pegasus spyware at least eight times between August and November 2019. These initial findings were confirmed by The Citizen Lab and Amnesty international. Bahraini authorities have previously harassed Al-Saegh:

* 1. On 20 March 2017, authorities detailed Al-Saegh for seven hours at Bahrain International Airport upon her return from the 34th session of the U.N. Human Rights Council. They thoroughly searched her, interrogated her for five hours, and confiscated her passport and mobile device. She was accused by the interrogator of delivering false statements about Bahraini human rights violations while in Geneva.
	2. On 26 May 2017, Bahrain’s National Security Agency summoned Al-Saegh to Muharraq police station. Interrogators subjected her to verbal abuse, physically beat and sexually assaulted her, and threatened her with rape if she did not halt her human rights activism. They released her at approximately 11:00 pm and she was immediately taken to a hospital.
	3. From August to November 2019, Al-Saegh’s phone was compromised multiple times; on August 8, 9, 12, 18, 28 and 31; September 19, and November 22, 2019.
	4. Traces of process names linked to Pegasus were identified on her phone, including “roleaccountd,” “stagingd,” “xpccfd,” “launchafd,” “logseld,” “eventstorpd,” “libtouchregd,” “frtipd,” “corecomnetd,” “bh,” and “boardframed.” Amnesty International’s Security Lab and The Citizen Lab attribute these process names to NSO Group’s Pegasus spyware.[[16]](#footnote-16)
1. Second, Front Line Defenders examined the phone of Jordanian human rights lawyer, **Hala Ahed Deeb,** discovering that her device had been infected with Pegasus spyware since March 2021. These findings were similarly validated by The Citizen Lab and Amnesty international. Hala defends prisoners of conscience in Jordan and is a member of the legal team defending the Jordan Teachers’ Syndicate, one of Jordan’s largest labour unions, which the Jordanian government dissolved in December 2020 in response to mass protests. Hala Deeb also headed the legal committee of the Jordanian Women’s Union and continues to defend women victims.
	1. On 16 March 2021, Hala Deeb’s phone was compromised by Pegagus. Traces of process names linked to Pegasus were identified on her phone, including “bluetoothfs,” “JarvisPluginMgr,” and “launchafd.” Amnesty International’s Security Lab and The Citizen Lab attribute these process names to NSO Group’s Pegasus spyware.[[17]](#footnote-17)
2. While the aforementioned cases focus on the experience of women HRDs, many other women, including journalists in the MENA region and beyond, have also been recently targeted with Pegasus spyware. This includes Emirati activist **Alaa Al-Siddiq**,[[18]](#footnote-18) Al Araby journalist **Rania Dridi**,[[19]](#footnote-19) and Al Jazeera broadcast journalist **Ghada Oueiss**,[[20]](#footnote-20) to name a few.
3. The impact of targeted surveillance on women can be particularly grievous,given that cultural, political, societal, economic, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing. This can include the publishing of private and intimate photos and conversations online. The **U.N. General Assembly has defined[[21]](#footnote-21)** **violence against women** as “any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.” This includes “physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs.” The spyware attacks have had a devastating impact on Ebtisam Al-Saegh and Hala Deeb. Since they discovered their phones were infected, they have each been living in a state of daily anxiety and fear. They are especially afraid of the possibility of exposing other women activists and victims they work with, and concerned that their families and friends are now at risk.
4. Overall, hacking stifles the exercise of a range of fundamental rights, including the right to freedom of expression and access to information, as well as the right to privacy, freedom of movement, and of peaceful assembly and association by creating a chilling effect on speech and democratic participation. Access Now continues to hear about journalists and independent media getting hacked in retaliation for reporting on government corruption and other abuses. Hacking also damages journalists' relationships with sources, impairing their ability to report on future stories.
5. For women targets, digital surveillance is a ticking bomb. They live in fear of how their personal information, including private photos, videos, and conversations, could be [used against them](https://www.nbcnews.com/tech/social-media/i-will-not-be-silenced-women-targeted-hack-leak-attacks-n1275540) at any given point, opening the door for harassment and abuse. This is especially worrying in regions, such as MENA, where governments [have routinely used doxxing](https://7amleh.org/2021/06/29/aetlaf-alhqwq-alrqmyh-ystnkr-anthakat-alhqwq-alrqmyh-ma-tsaad-alahdath-alakhyrh-ala-alardh.) of women and [LGBTQ+ activists](https://www.wired.co.uk/article/tunisia-police-facebook) in order to smear and intimidate them into silence.

***Best practice: Technology company leadership in litigation against NSO Group***

1. It is important that companies such as NSO Group are held responsible for facilitating egregious human rights abuses against journalists and activists around the world. The conduct of NSO Group and the clients who use its spyware have been subject of multiple lawsuits and criminal investigations in countries,[[22]](#footnote-22) including Cyprus,[[23]](#footnote-23) Israel,[[24]](#footnote-24) India,[[25]](#footnote-25) Mexico,[[26]](#footnote-26) the United Kingdom,[[27]](#footnote-27) France,[[28]](#footnote-28) and the United States. Often, NSO Group’s Pegasus spyware infiltrates a target’s device by exploiting vulnerabilities in third-party infrastructure and applications, such as messaging apps. Recently, the technology companies that provide the third-party applications and infrastructure NSO exploits to infect its victims have shown leadership in holding spyware companies accountable by taking NSO to court. In 2019, WhatsApp (owned by Meta) filed a lawsuit against NSO Group[[29]](#footnote-29) in a US federal court. Diverse stakeholders support this effort to hold NSO accountable: Access Now led a coalition of groups filing an amicus brief[[30]](#footnote-30) that spotlights those who survived Pegasus attacks from India, Morocco, Rwanda, and Togo, while Microsoft, Google, and other tech companies highlighted the dangers of cyber surveillance tools such as Pegasus for human rights and the overall security of the internet infrastructure.[[31]](#footnote-31) This year, Apple also filed a similar lawsuit against NSO Group, in addition to announcing a $10 million contribution to support cybersurveillance researchers and advocates[[32]](#footnote-32) and notifying their users of being targeted by Pegasus or other type of spyware.[[33]](#footnote-33) Another example of private companies working to address the problem of spyware is Google’s Project Zero, which released public analysis of how NSO’s Pegasus exploits vulnerabilities in Apple’s iMessage to infect users' devices.[[34]](#footnote-34) We encourage other companies to follow these practices and continue exposing and fighting the proliferation and use of spyware in violation of human rights, in collaboration with civil society.

***Weaponizing draconian extremism and Foreign Agent laws to stifle free expression and shut down independent media***

1. In recent years, we have witnessed a staggering increase in the number of repressive laws, such as extremism and terrorism laws and so-called “foreign agent” laws, often penalizing and criminalizing the rights to freedom of expression, around the world.

***Extremism, terrorism, and related laws***

1. Extremism and terrorism laws are being weponized against journalists, independent media, and the broader civil society in many countries, including Belarus, Russia, Israel, Jordan and Turkey.[[35]](#footnote-35)
2. In Belarus, the government continues to actively resort to anti-extremism laws to censor and intimidate independent media and voices critical of the regime, online and offline. Such laws use excessively vague terminology, which allows overbroad interpretation and misuse. In determining if a given statement is a form of “extremist” expression or hate speech, no consideration is given to the speaker’s intent, the expression’s context, its audience, or the likelihood of harm to occur.
3. As of 20 January 2021, the total number of political prisoners in Belarus is 991, according to the Human Rights Center “Viasna.”[[36]](#footnote-36) In 2021 Belarusian Association of journalists reported 113 cases of detention, 146 cases of searches, and 29 cases of administrative arrests against media workers.[[37]](#footnote-37) 32 journalists are still behind bars, among them 17 women.[[38]](#footnote-38) Many of these individuals have been charged with extremism and related laws.
4. Popular Telegram channel NEXTA remains on the list of “extremist” materials. Anyone who reposts or shares NEXTA materials can be penalized. On May 23, NEXTA creator Raman Pratasevich, who was previously added to a “list of individuals involved in terrorist activities” and charged with “inciting hatred and bias,” was kidnapped and arrested by Belarusian authorities after his Athens to Vilnius Ryanair plane was forced to land in Minsk under the pretence of a false terrorist threat and accompanied by a pursuit plane.[[39]](#footnote-39) Pratasevich’s partner Sofia Sapega, was also arrested with him and forced to confess that she is the editor of Black Book of Belarus – a Telegram channel which has published the personal information of security officials. Belarus has classified the channel as an “extremist” group.[[40]](#footnote-40)
5. On 10 March 2021, it became known about the initiation of a criminal case against the popular opposition blogger Anton Motolko: he is accused of inciting social hostility, mass riots, organizing actions that grossly violate public order, calling for actions aimed at harming national security, as well as creating an extremist group.[[41]](#footnote-41) His Telegram channel was included in the list of extremist materials, and Anton himself was included in the “list of persons involved in terrorist activities,” having to leave Belarus as a result of persecution.[[42]](#footnote-42)
6. On 1 October 2021, Belarusian KGB detained Henadz Mazheika, the journalist of the Russian newspaper “Komsomolskaya Pravda v Belarusi.” He was accused of incitement of social enmity and insulting representatives of the authorities for writing about Andrei Zeltser who was killed in a shootout with Belarusian security officers.[[43]](#footnote-43)
7. Overall, 13 media outlets and 431 Telegram channels are recognized as “extremist” in Belarus.[[44]](#footnote-44) Sharing or saving information posted on them can lead to non-proportional administrative fines or arrests. For example, a young married couple, Anastasia Krupenich-Kodratyeva and Sergey Krupenich have spent 125 days in a detention centre for sending each other in their private communications posts from popular social media sources that were recognised as extremist by Belarusian authorities.[[45]](#footnote-45)
8. Russia has also started to aggressively use anti-extremism and anti-terrorism laws against independent media, bloggers and opposition voices online.[[46]](#footnote-46) Last year, a Moscow court banned political organisations, including Anti-Corruption Foundation (FBK), linked to the jailed anti-corruption activist, blogger, and opposition leader Alexey Navalny, classifying them as "extremist” for their work critical of the government, a move condemned by the UN High Commissioner for Human Rights.[[47]](#footnote-47) Since then, the former coordinator of Aleksey Navalny’s political headquarters in the Russian city of Ufa Lilia Chanysheva was charged with “establishing or leading an extremist association” for her activities that predated the designation of Navalny’s organizations as extremist.[[48]](#footnote-48) Last week, two of Navalny’s closest associates and popular bloggers, Ivan Zhdanov and Leonid Volkov, have been placed on the country's list of “extremists and terrorists.”[[49]](#footnote-49) In September 2021, Russian authorities also successfully pressured two tech companies, Apple and Google, to delete Navalny’s app that informed voters on latest political developments and provided recommendations on non-ruling party candidates. The authorities employed extra-legal measures, by threatening companies’ staff with baseless criminal charges.[[50]](#footnote-50)
9. Last month, Russia’s censorship body, Roskomnadzor, unexpectedly [blocked](https://www.reuters.com/world/russia-blocks-website-ovd-info-protest-monitoring-group-interfax-2021-12-25/) the website of a prominent human rights and independent media organization OVD-Info.[[51]](#footnote-51) The judicial [order](https://luhovitsy--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=337449901&delo_id=1540005&new=0&text_number=1) granting the blocking stated that by reporting on the political repressions and arrests during protests and by providing legal assistance to detained individuals, OVD-Info may create “impression” of justification of “extremist activities” to its online readers.[[52]](#footnote-52) Roskomnadzor also [sent notifications](https://www.change.org/p/call-for-social-media-don-t-be-a-censorship-tool) to social media companies - Telegram, Facebook, Instagram, Twitter, VKontakte, Yandex, and Google - asking them to block OVD-Info’s social media pages on this basis.[[53]](#footnote-53)

***Foreign agent laws (Russia)***

1. Since 2014 Russian authorities have been using a so-called “Foreign Agent” law as a tool to silence dissent, imposing heavy burdens upon media organizations, who receive foreign funding and engage in what the government deems “political activities,” and stigmatizing them by labelling “foreign agents.”[[54]](#footnote-54) The [legislation has since been amended](https://www.frontlinedefenders.org/en/statement-report/russias-amendment-foreign-agents-law-poses-major-new-restrictions-work-human) to target not only media outlets but also individual journalists and bloggers.[[55]](#footnote-55) The interpretation of criteria to be listed as ‘foreign agent’ are so broad that even being endorsed to attend international conferences can be regarded as one of the grounds for a journalist to be included on the list.[[56]](#footnote-56)
2. As of 18 January 2022, 113 media outlets, individuals and companies are registered as ‘media foreign agents’, among them 32 women.[[57]](#footnote-57) Some 96 media representatives received this status only in 2021, signifying that the Russian government only increases repressions aimed at independent journalists and plans to further exert its control over them. Some of the notable cases include:
3. Chief editor, Sergei Smirnov, and publisher, Pyotr Verzilov, of Mediazona outlet were listed as ‘foreign agents’ for gaining profits from Google ads.[[58]](#footnote-58)
4. Darya Apakhonchich, a feminist activist, is the first artist to be labelled a ‘foreign agent’ by Russian authorities. Following her recognition as a ‘foreign agent’ she has been subject to a search and confiscation of her family's electronic devices in an attempt to discover extremism materials.[[59]](#footnote-59)
5. The founder of LGBT Network was recognized as a media foreign agent on 12 November 2021 and was forced to leave the country to continue his activities abroad.[[60]](#footnote-60)
6. The status of ‘foreign agent’ obliges the media to mark all its materials, including their social media posts, with a special label and to provide excessive reports (approximately 44 pages every 3 months) to a controlling body, Roskomnadzor.[[61]](#footnote-61) Referring to a ‘media foreign agents’’ articles or posts imposes similar marking obligations to other journalists or bloggers. Non-compliance with these requirements can lead to the suspension of one's activities, administrative or even criminal charges.
7. For example, 840 administrative protocols were filed against media outlet [Radio Free Europe/Radio Liberty](https://www.rferl.org/) for not marking their materials with a ‘foreign agent’ label, subjecting the media to a fine of 227,8 million of rubles in total.[[62]](#footnote-62) Nobel prize laureate, Dmitry Muratov, and Novaya Gazeta media outlet were fined for not putting the ‘foreign agent’ label while referring to the articles of journalists with the corresponding status.[[63]](#footnote-63) Most strikingly, in December, Russian courts liquidated the two entities forming the most respected Russian human rights organizations, Memorial, for alleged failure to mark their online publications as “foreign agent” material as required by the Foreign Agent Law.[[64]](#footnote-64)
8. In a disturbing trend, more countries around the world are following Russia’s example. Kazakhstan, Belarus, Poland, Hungary, Egypt, Israel, Nicaragua, El Salvador, and Guatemala are among the countries around the world that have passed or are considering passing “Foreign Agent” laws similar to Russia’s.[[65]](#footnote-65)
9. U.N. High Commissioner Bachelet urged “the authorities to end the arbitrary practice of labelling ordinary individuals, journalists, and non-governmental organizations as 'extremists', 'foreign agents' or 'undesirable organizations.'"[[66]](#footnote-66)

***Cybercrime and criminal laws used to prosecute journalists in Africa and MENA***

1. States, particularly across Africa, continue to develop and update laws to stop “cybercrime.” Often, states develop this national legislation without adequate multi stakeholder input, or attention to human rights frameworks, and implement the laws as a means to shrink civic space and press freedoms. Such laws often purposefully contain vague and overbroad definitions to empower law enforcement and other government agencies with unfettered control. For instance, in Nigeria, the 2015 cybercrime act continues to be used against journalists in Nigeria. The Committee to Protect Journalists (CPJ) has repeatedly documented the use of Nigeria’s cybercrime act to prosecute journalists for their work.[[67]](#footnote-67)
2. In May - June 2020, Nigerian journalist **Saint Meinpamo Onitsha**, founder of the privately owned *Naija Live TV* news website, was charged and accused of violating section 21 (1) (b) of Nigeria’s cybercrime act for reporting on the alleged collapse of a COVID-19 isolation center in Nigeria’s northern Kogi State.[[68]](#footnote-68) That section of the cybercrime act criminalizes “sharing messages via a computer or network system which they know to be false for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another person.”[[69]](#footnote-69) CPJ’s sources said that on June 5 authorities granted bail to Onitsha, “but required a bond of 2 million naira ($5,163), a surety from a senior civil servant, and a surety from a land owner in Bayelsa state.”[[70]](#footnote-70) Onitsha was unable to meet such onerous bail requirements. CPJ therefore called on Nigerian authorities to immediately release Onitsha, drop all charges against him, and reform the country’s cybercrime act to ensure that it is not used to prosecute the press. Nigeria’s cybercrime act, which allows for journalists and independent media to be arrested for their critical reporting, violates freedom of expression and the press – a right guaranteed under section 39 of Nigeria’s Constitution.
3. States must not be encouraged to increase penalties for traditional crimes, such as trespass, simply for the use of a computer in their exercise, and any new offenses added to criminal codes must receive robust input and take care to adhere to human rights law and norms in their formulation, to avoid outlawing fundamental functions of journalism, such as newsgathering, source protection, and dissemination of materials and news in the public interest, in the digital age.
4. On 12 January 2022, a Criminal Procedure and Evidence (Controlled Investigation) Bill was introduced in Botswana’s Parliament.[[71]](#footnote-71) Media organisations based in Botswana have raised serious concerns about the Bill’s impact on free press. According to MISA, “the law jeopardizes freedom of expression and makes the media especially vulnerable.”[[72]](#footnote-72) Since Botswana does not have a Freedom of Information Law, the current Bill would make an already bad situation even worse. Without judicial oversight, Law Enforcement agencies would have unfettered power to intercept communications.[[73]](#footnote-73) Such power is ripe for abuse and would create an overall chilling effect in the country.
5. Likewise, Sierra Leone passed a cybercrime law in 2021 without adequate attention to impacts on press freedom and the freedoms of opinion and expression, and the right to privacy.[[74]](#footnote-74)
6. Access Now has tracked similar developments in the MENA region, reporting on cybercrime legislation that threatens freedom of expression in Libya[[75]](#footnote-75) and Egypt, Palestine, Lebanon, and Bahrain.[[76]](#footnote-76)

***Internet shutdowns and their influence on the work of the media***

1. Government-imposed internet shutdowns not only interfere with the media’s ability to report on the events and limit international journalists’ means to connect with sources and people on the ground, but the disruptions also provide a cover for state and non-state actors to get away with brutalities perpetrated against media workers. As reported by the Committee to Protect Journalists, “Internet shutdowns have serious consequences for press freedom and leave journalists struggling to do their job effectively… Turning off or limiting access to the internet means that media workers are unable to contact sources, fact check data, or file stories until after an event has happened.”[[77]](#footnote-77) Access Now and #KeepItOn,[[78]](#footnote-78) a global campaign and coalition fighting internet shutdowns, monitor internet shutdowns and often rely on journalistic reporting to verify the disruptions, their causes, and impacts, tasks made more difficult without internet connectivity.
2. Recent examples illustrate the multiple harms caused by internet shutdowns on media and journalistic work. According to several reliable reports, Kazakhstan has shut down and throttled mobile and fixed line internet on numerous occasions since 2 January 2022.[[79]](#footnote-79) The most widespread shutdown took place between January 5 and January 10, 2022, when the whole country was plunged into digital darkness amidst protests, and deadly violence. [[80]](#footnote-80) The brief restorations of the internet on each day lasted only for several hours, and were difficult to predict or react to, until the final restoration on January 11, 2022.
3. During protests and internet shutdown in Kazakhstan,[[81]](#footnote-81) at least 5 offices of media outlets were attacked, 5 journalists and bloggers were arrested, 2 journalists were injured, 1 media worker has been reported missing and one journalist has been killed amidst protests.[[82]](#footnote-82) The internet outages and blocking of independent outlets such as Orda.kz and kaztag.kz have significantly influenced the international community’s ability to prevent, document and investigate these cases of disruptions of the media's ability to work without obstruction or fear of retribution.[[83]](#footnote-83)
4. Telcos have a duty to respect human rights in their operations and to contribute to remedy for violations they cause or contribute to. The companies have a role to play in resisting and denouncing shutdowns, preserve evidence and reveal any demands from the government to disrupt access, publicly disclose details such as when the internet and related services have been disrupted, their status throughout the shutdown, and when they come back online; contest the legality of internet shutdown orders in court; and consult civil society and rally peer companies to jointly push back against government censorship demands, and issue regular transparency reports to ensure open and secure internet access and deter future shutdown orders.

**Concluding Recommendations**

The global network of journalists is in ever-increasing need of digital security assistance as they face more severe and more persistent threats. Keeping such actors safe, connected, and empowered to do their work is an essential foundation for the broader fight to protect human rights in the digital age. Calls for rapid digitalization should not come ahead of critical human rights protections — especially when implementation of more sophisticated technologies leads directly to a rise in digital authoritarianism. States must protect — not attack — their own populations; companies must commit to respecting human rights online; and civil society must recognize and respond to the inherent risks of online activities. Only then can we build a safer, more secure, free and open digital future for everyone.[[84]](#footnote-84) Journalists and the broad spectrum of independent and professional media workers play an essential role in informing stakeholders of threats to their rights, online and offline, and in ensuring democratic institutions can responsibly and effectively adapt for the digital age.

1. **States**
	1. Undertake action to address persecution of journalists, online and offline, such as by issuing sanctions against the clients, owners, and affiliates of spyware companies and enhancing funding for circumvention tools and services.
	2. Adopt comprehensive regulations and legislation addressing the threat of invasive surveillance via spyware, ranging from export controls, sanctions, import restrictions, procurement and screening mandates, investor-facing and financial disclosure rules, and due diligence requirements that mandate transparency on the sale and use of surveillance technologies, and their outcomes and impacts on human rights. Ensure that any legislation that is adopted to regulate surveillance technology companies is developed in consultation with human rights defenders who have been impacted by the misuse of surveillance technologies.
	3. Stop using surveillance and censorship technologies against journalists, independent media, and other civil society actors, and impose an immediate moratorium on the sale, transfer, and use of surveillance technologies produced by private firms until adequate human rights safeguards and regulation is in place.
	4. End the arbitrary practice of labelling ordinary individuals, bloggers, journalists, independent media, and non-governmental organizations as 'extremists', 'foreign agents' or 'undesirable organizations', repeal such legislation, and release all political prisoners charged with crimes based on such legislation.
	5. Call on States to make a pledge to refrain from blocking or shutting down the internet.
2. **Private Sector**
	1. Stop providing technologies enabling shutdowns, censorship, surveillance, and other types of repression of journalists, independent media, and other civil society actors.
	2. Publicly denounce and resist internet shutdowns.
	3. Follow the best practices of other technology companies that continue to expose and fight the proliferation and use of spyware in violation of human rights, through litigation, and other forms of action, in collaboration with civil society.
3. **International Organizations**
	1. Appoint a U.N. Special Representative to the U.N. Secretary General for the safety of journalists and ensure that the mandate is tasked to address the persecution of journalists, online and offline, while advocating for the enhancement of circumvention tools and services.
	2. Investigate the harms of disinformation across the world and the unique harms to communities at risk of marginalization and in situations of vulnerability, which can include those of African descent, Indigenous, displaced, and migrant communities, persons with disabilities, and ethnic, racial, or religious minorities, among others. In consultation with expert organizations, the report should be accompanied by a set of recommended state policies for governments to consider adopting to stop the spread of disinformation. It should also suggest remedies for the harms people have already experienced.

##### **Access Now (**[**https://www.accessnow.org**](https://www.accessnow.org)**)** defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact:* ***un@accessnow.org***

1. U.N. Human Rights, Office of the High Commissioner for Human Rights, Call for comments on opportunities, challenges and threats to media in the digital age, available at <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Report-Media-Digital-Age.aspx>, 2022. [↑](#footnote-ref-1)
2. Access Now, About Us, 2021, available at <https://www.accessnow.org/>. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon. [↑](#footnote-ref-2)
3. Access Now, Guide: how to protect human rights in content governance, available at: [https://www.accessnow.org/guide-how-to-protect-human-rights-in-content-governance](https://www.accessnow.org/guide-how-to-protect-human-rights-in-content-governance/), 3 March 2020. [↑](#footnote-ref-3)
4. <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_854.pdf> [↑](#footnote-ref-4)
5. See regional e.g.’s where authorities tighten control over, blackout or surveil social media platforms: Access Now, **Laos** directs surveillance of social media platforms, further throttling expression online, available at: <https://www.accessnow.org/laos-directs-surveillance-of-social-media-platforms/>, 25 May 2021; Access Now, #ShutdownStories: how **Chad’s** fixation on social media blackouts hurts citizens, available at: <https://www.accessnow.org/shutdownstories-how-chad-fixation-on-social-media-blackouts-hurts-citizens/> , 22 September 2020; Access Now, **Indian** authorities tighten control over online content, available at: <https://www.accessnow.org/indian-authorities-tighten-control-over-online-content/> , 25 February 2021. [↑](#footnote-ref-5)
6. Access Now, *Digital Security Helpline,* available at: <https://www.accessnow.org/help/>, 2021. [↑](#footnote-ref-6)
7. See, CiviCERT, available at <https://www.civicert.org>. [↑](#footnote-ref-7)
8. ​​See, e.g., Access Now. Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts. December 23, 2020. <https://www.accessnow.org/nso-groupwhatsapp-lawsuit-civil-society-amicus-brief>; Natalia Krapiva and Peter Micek. Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus. September 3, 2020. <https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-andoppression-in-belarus/> [↑](#footnote-ref-8)
9. See Javier Pallero. International groups reject Mexican government surveillance of public health advocates. February 16, 2017. <https://www.accessnow.org/international-groups-rejectmexican-government-surveillance-public-health-advocates/> ; Access Now. Two years after Khashoggi’s slaying, no accountability for spyware firm or Saudi government. October 1, 2020. <https://www.accessnow.org/khashoggi-two-years-later/> ; Access Now. European-made FinSpy malware is being used to target critics in Turkey. May 14, 2018. https://www.accessnow.org/ european-made-finspy-malware-is-being-used-to-target-activists/. [↑](#footnote-ref-9)
10. Amnesty International, Scale of secretive cyber surveillance ‘an international human rights crisis’ in which NSO Group is complicit, available at: <https://www.amnesty.org/en/latest/press-release/2021/07/pegasus-project-spyware-digital-surveillance-nso/>, 23 July 2021. [↑](#footnote-ref-10)
11. Access Now, Enough is enough! States must intervene on NSO Group’s unchecked power*,* available at: <https://www.accessnow.org/enough-is-enough-nso-group/>, 27 July 2021. [↑](#footnote-ref-11)
12. The Guardian, Pegasus spyware found on journalists’ phones, French intelligence confirms, available at: <https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms>, 2 August 2021. [↑](#footnote-ref-12)
13. U.N. Human Rights, Office of the High Commissioner for Human Rights, Use of spyware to surveil journalists and human rights defenders, Statement by UN High Commissioner for Human Rights Michelle Bachelet, available at: <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=27326&LangID=E>, 19 July 2021. [↑](#footnote-ref-13)
14. Access Now, Exposed: civil society condemns use of Pegasus in El Salvador to spy on journalists and activists, available at: [https://www.accessnow.org/pegasus-el-salvador-spyware-targets-journalists-statement](https://www.accessnow.org/pegasus-el-salvador-spyware-targets-journalists-statement/), 12 January 2022; Citizenlab, Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, available at: [https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware /](https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/), 12 January 2022. [↑](#footnote-ref-14)
15. Access Now, Unsafe anywhere: women human rights defenders out about Pegasus attacks, available at: <https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>, 17 January 2022. [↑](#footnote-ref-15)
16. Amnesty International, Investigations, available at: <https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso>, 18 July 2021; The Citizen Lab, devices of Palestinian Human Rights Defenders Hacked with NSO Group’s Pegasus Spyware, available at: <https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/>, 8 November 2021. [↑](#footnote-ref-16)
17. Amnesty International, Investigations, available at: <https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso>, 18 July 2021; The Citizen Lab, devices of Palestinian Human Rights Defenders Hacked with NSO Group’s Pegasus Spyware, available at: <https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/>, 8 November 2021. [↑](#footnote-ref-17)
18. The Guardian, New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq, available at: <https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq>, 24 September 2021. [↑](#footnote-ref-18)
19. The Guardian, Dozens of Al Jazeera journalists allegedly hacked using Israeli firm’s spyware, available at: <https://www.theguardian.com/media/2020/dec/20/citizen-lab-nso-dozens-of-aljazeera-journalists-allegedly-hacked-using-israeli-firm-spyware>, 20 December 2020. [↑](#footnote-ref-19)
20. Committee to Protect Journalists (CPJ), Al-Jazeera’s Ghada Oueiss on hacking, harassment, and Jamal Khashoggi, available at: <https://cpj.org/2021/02/ghada-oueiss-hacking-harassment-jamal-khashoggi/>, 11 February 2021. [↑](#footnote-ref-20)
21. U.N. General Assembly, Declaration on the Elimination of violence against Women, U.N. Doc. A/RES/48/104, available at: <http://www.un-documents.net/a48r104.htm>, 20 December 1993. [↑](#footnote-ref-21)
22. Access Now, Two years after Khashoggi’s slaying, no accountability for spyware firm or Saudi government, available at <https://www.accessnow.org/khashoggi-two-years-later/>, 1 October 2020. [↑](#footnote-ref-22)
23. The New York Times, Hacking a Prince, an Emir and a Journalist to Impress a Client, available at: <https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html>, 31 August 2018. [↑](#footnote-ref-23)
24. The New York Times, Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says, available at: <https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html>, 2 December 2018. [↑](#footnote-ref-24)
25. The Guardian, Indian supreme court orders inquiry into state’s use of Pegasus spyware, available at: <https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware>, 27 October 2021. [↑](#footnote-ref-25)
26. Reuters, INSIGHT-Pegasus spyware scandal: years of questions, no answers for Mexico victims, available at: <https://www.reuters.com/article/mexico-tech-surveillance/insight-pegasus-spyware-scandal-years-of-questions-no-answers-for-mexico-victims-idUSL8N2PD6BQ>, 9 August 2021. [↑](#footnote-ref-26)
27. The Washington Post, Dubai ruler used Pegasus spyware to hack princess’s phone, U.K. court rules, available at: <https://www.washingtonpost.com/technology/2021/10/06/pegasus-dubai-princess-haya-court-ruling/>, 6 October 2021. [↑](#footnote-ref-27)
28. The Washington Post, France orders spyware investigation following Pegasus Project reports, available at: <https://www.washingtonpost.com/world/2021/07/20/france-investigation-pegasus-spyware/>, 22 July 2021. [↑](#footnote-ref-28)
29. The New York Times, WhatsApp Says Israeli Firm Used Its App in Spy Program, available at: <https://www.nytimes.com/2019/10/29/technology/whatsapp-nso-lawsuit.html>, 29 October 2019. [↑](#footnote-ref-29)
30. Access Now, Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts, 23 Dec. 2020,

 available at: <https://www.accessnow.org/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/> [↑](#footnote-ref-30)
31. Reuters, Microsoft, Google, Cisco, Dell join legal battle against hacking company NSOm available at: <https://www.reuters.com/article/us-facebook-nso-cyber/microsoft-google-cisco-dell-join-legal-battle-against-hacking-company-nso-idUSKBN28V2WX>, 21 December 2020. [↑](#footnote-ref-31)
32. Apple, Apple sues NSO Group to curb the abuse of state-sponsored spyware, available at: <https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/>, 23 November 2021. [↑](#footnote-ref-32)
33. Apple, About Apple threat notifications and protecting against state-sponsored attacks, available at: <https://support.apple.com/en-us/HT212960>, 23 November 2021. [↑](#footnote-ref-33)
34. Google Project Zero, A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution, available at: <https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html>, 15 December 2021. [↑](#footnote-ref-34)
35. Euronews, Belarus toughens laws against protesters and 'extremism', available at: <https://www.euronews.com/2021/06/08/belarus-toughens-laws-against-protesters-and-extremism> , 8 June 2021; RadioFreeEurope/RadioLiberty, 'Extremism' As A Blunt Tool: Behind The Russian Law Being Used To Shut Navalny Up, available at: <https://www.rferl.org/a/russia-anti-extremism-law-blunt-instrument-navalnu-jehovahs-witnesses/31230149.html> , 29 April 2021; Npr, Israel designates 6 Palestinian human right groups as terrorist organizations, available at: <https://www.npr.org/2021/10/23/1048690050/israel-palestinian-human-right-groups> , 23 October 2021; Access Now, Jordan is arresting people for criticizing the government on social media, available at: <https://www.accessnow.org/jordan-arresting-people-criticizing-government-social-media/> , 26 January 2017; Amnesty International, Turkey: Measures to prevent terrorism financing abusively target civil society and set dangerous international precedent, available at: <https://www.amnesty.org/en/latest/news/2021/06/turkey-measures-to-prevent-terrorism-financing-abusively-target-civil-society-and-set-dangerous-international-precedent> , 17 June 2021. [↑](#footnote-ref-35)
36. Human Rights Center “Viasna,” List of Political Prisoners, available at: <https://prisoners.spring96.org/en> , 20 January 2021. [↑](#footnote-ref-36)
37. Belarusian Association of Journalists, Рэпрэсіі супраць журналістаў у 2021 годзе (табліца, спіс зняволеных), available at: <https://baj.by/be/analytics/represii-suprac-zhurnalistau-u-2021-godze-tablica-spis-znyavolenyh>, 23 December 2021. [↑](#footnote-ref-37)
38. Belarusian Association of Journalists, Рэпрэсіі супраць журналістаў у 2021 годзе (табліца, спіс зняволеных), available at: <https://baj.by/be/analytics/represii-suprac-zhurnalistau-u-2021-godze-tablica-spis-znyavolenyh>, 23 December 2021. [↑](#footnote-ref-38)
39. The Financial Times, Lukashenko claims ‘planned provocation’ forced interception of Ryanair flight, available at: <https://www.ft.com/content/ac60d3bb-af7d-4441-9c43-4ec6d3dc89be>, 26 May 2021; Politico, Alexander Lukashenko, international terrorist, available at: [https://www.politico.eu/article/alexander-lukashenko-terrorist-belarus-ryanair-plane-roman-protasevich](https://www.politico.eu/article/alexander-lukashenko-terrorist-belarus-ryanair-plane-roman-protasevich/)/, 24 May 2021. [↑](#footnote-ref-39)
40. Naviny.by, Телеграм-канал «Черная книга Беларуси» признан экстремистским, available at: <https://naviny.online/new/20210429/1619704373-telegram-kanal-chernaya-kniga-belarusi-priznan-ekstremistskim>, 29 April 2021. [↑](#footnote-ref-40)
41. Investigative Committee of the Republic of Belarus, УСК по городу Минску возбуждено уголовное дело в отношении Антона Мотолько, available at: <https://sk.gov.by/ru/news-usk-gminsk-ru/view/usk-po-gorodu-minsku-vozbuzhdeno-ugolovnoe-delo-v-otnoshenii-antona-motolko-9757/>, 10 March 2021. [↑](#footnote-ref-41)
42. Belsat, Matolka’s Telegram channel labeled extremist media, available at: <https://belsat.eu/en/news/30-03-2021-blogger-anton-matolka-s-telegram-channel-labeled-extremist-media/>, 30 March 2021. [↑](#footnote-ref-42)
43. Voice of Belarus, [Journalist of the Russian newspaper detained for an article about KGB officer’s murder](https://www.voiceofbelarus.org/belarus-news/journalist-of-the-russian-newspaper-detained-for-an-article-about-kgb-officers-murder/), available at: <https://www.voiceofbelarus.org/belarus-news/journalist-of-the-russian-newspaper-detained-for-an-article-about-kgb-officers-murder/>, 2 October 2021. [↑](#footnote-ref-43)
44. Belarusian Association of Journalists, Рэпрэсіі супраць журналістаў у 2021 годзе (табліца, спіс зняволеных), available at: <https://baj.by/be/analytics/represii-suprac-zhurnalistau-u-2021-godze-tablica-spis-znyavolenyh>, 23 December 2021; Ministry of Information of the Republic of Belarus, The list of extremist materials, available at: <http://mininform.gov.by/documents/respublikanskiy-spisok-ekstremistskikh-materialov/>, 18 January 2021. [↑](#footnote-ref-44)
45. Reform.by, Семейную пару в девятый раз осудили за репост с «экстремистских» каналов в личной переписке, available at: <https://reform.by/274659-semejnuju-paru-v-devjatyj-raz-osudili-za-repost-s-jekstremistkih-kanalov-v-lichnoj-perepiske>, 5 November 2021. [↑](#footnote-ref-45)
46. From 2009 to December 2021, human rights center Memorial included 992 people on its list of political prisoners. 349 of them are accused of religious extremism. See, e.g., <https://memohrc.org/ru/content/programma-podderzhka-politzaklyuchyonnyh-i-drugih-zhertv-politicheskih-repressiy>, 20 January 2022. [↑](#footnote-ref-46)
47. BBC News, Alexei Navalny: Moscow court outlaws 'extremist' organisations, available at:<https://www.bbc.com/news/world-europe-57422346>, 10 June 2021; Reuters, U.N. decries Russia moves against Navalny, calls for upholding rights, available at: <https://www.reuters.com/world/un-decries-russia-moves-against-navalny-calls-upholding-rights-2021-06-21/>, 21 June 2021. [↑](#footnote-ref-47)
48. Amnesty International, Russia: Detention of Navalny associate on “extremism” charges a forewarning of mass reprisals, available at: <https://www.amnesty.org/en/latest/news/2021/11/russia-detention-of-navalny-associate-on-extremism-charges-a-forewarning-of-mass-reprisals/>, 11 November 2021. [↑](#footnote-ref-48)
49. RadioFreeEurope/RadioLiberty, Navalny Associates Volkov, Zhdanov Placed On Russia's 'Terrorist' List, available at: <https://www.rferl.org/a/russia-volkov-zhdanov-extremists-navalny/31654095.html>, 14 January 2022. [↑](#footnote-ref-49)
50. Access Now, Not good enough: Apple, Google bow to government pressure, censor content during Russian elections, available at: <https://www.accessnow.org/apple-google-censor-russian-elections/>, 21 September 2021; Aljazeera, Why are Google and Apple still silent on Russian censorship?, available at: <https://www.aljazeera.com/opinions/2021/11/1/why-are-google-and-apple-still-silent-on-russia-censorship>, 1 November 2021. [↑](#footnote-ref-50)
51. Reuters, Russia blocks website of OVD-Info protest-monitoring group, available at: <https://www.reuters.com/world/russia-blocks-website-ovd-info-protest-monitoring-group-interfax-2021-12-25/>, 28 December 2021. [↑](#footnote-ref-51)
52. Lukhovitsy district court of Moscow region, Decision available at: <https://luhovitsy--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=337449901&delo_id=1540005&new=0&text_number=1>, 20 January 2022. [↑](#footnote-ref-52)
53. Change.org, Call for social media. Don't be a censorship tool!, available at: <https://www.change.org/p/call-for-social-media-don-t-be-a-censorship-tool>, 20 January 2022. [↑](#footnote-ref-53)
54. Human Rights Watch, Russia: Government vs. Rights Groups.The Battle Chronicle, available at: <https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle>, 18 June 2018. [↑](#footnote-ref-54)
55. Npr, Russia's 'Foreign Agent' Law Targets Journalists, Activists, Even Ordinary Citizens, available at: <https://www.npr.org/2021/07/31/1021804569/russias-foreign-agent-law-targets-journalists-activists-even-ordinary-citizens> , 13 July 2021. [↑](#footnote-ref-55)
56. Golos Ameriki, Репрессии против журналистов и правозащитников в России в 2021 году, available at: <https://www.golosameriki.com/a/repressions-against-journalists-and-human-rights-lawyers-in-russia/6375927.html> , 30 December 2021. [↑](#footnote-ref-56)
57. The Ministry of Justice of Russian Federation, The Register of foreign mass media performing the functions of a foreign agent, available at: <https://minjust.gov.ru/ru/documents/7755/> , 14 January 2022. [↑](#footnote-ref-57)
58. Центр защиты прав СМИ, «Медиазону» признали «иностранным агентом» из‑за дохода от Google‑рекламы и ссылок на «Медузу», available at: [https://mmdc.ru/news-div/digest/mediazonu-priznali-inostrannym-agentom-iz%e2%80%91za-dohoda-ot-google%e2%80%91reklamy-i-ssylok-na-meduzu/](https://mmdc.ru/news-div/digest/mediazonu-priznali-inostrannym-agentom-iz%E2%80%91za-dohoda-ot-google%E2%80%91reklamy-i-ssylok-na-meduzu/) , 30 December 2021. [↑](#footnote-ref-58)
59. Npr, Russia's 'Foreign Agent' Law Targets Journalists, Activists, Even Ordinary Citizens, available at: <https://www.npr.org/2021/07/31/1021804569/russias-foreign-agent-law-targets-journalists-activists-even-ordinary-citizens> , 13 July 2021. [↑](#footnote-ref-59)
60. Ovd-Info, Сооснователь Российской ЛГБТ-сети Игорь Кочетков уехал из России, available at: <https://ovdinfo.org/express-news/2021/12/31/soosnovatel-rossiyskoy-lgbt-seti-igor-kochetkov-uehal-iz-rossii>, 31 December 2021. [↑](#footnote-ref-60)
61. Meduza, 2021 год в России — год «иноагентов» Как государство преследует независимых журналистов, СМИ и НКО. Самые впечатляющие числа, available at: <https://meduza.io/feature/2021/12/31/2021-god-v-rossii-god-inoagentov>, 31 December 2021. [↑](#footnote-ref-61)
62. Meduza, 2021 год в России — год «иноагентов» Как государство преследует независимых журналистов, СМИ и НКО. Самые впечатляющие числа, available at: <https://meduza.io/feature/2021/12/31/2021-god-v-rossii-god-inoagentov>, 31 December 2021. [↑](#footnote-ref-62)
63. Ovd-Info, «Новой газете» и Дмитрию Муратову назначили шесть штрафов из-за упоминания иноагентов без маркировки, available at: <https://ovdinfo.org/express-news/2021/11/17/novoy-gazete-i-dmitriyu-muratovu-naznachili-shest-shtrafov-iz-za-upominaniya>, 17 November 2021. [↑](#footnote-ref-63)
64. The New York Times, Russian Court Orders Prominent Human Rights Group to Shut, available at: <https://www.nytimes.com/2021/12/28/world/europe/russia-memorial-human-rights.html> [↑](#footnote-ref-64)
65. Coda Story,Putin’s playbook: Strongmen around the world are using Russian tactics to quell dissent, available at: <https://www.codastory.com/disinformation/russias-foreign-agents-law-reverberates-around-the-world/>, 27 July 2021; Eurasianet, Russia’s foreign agent law ricochets around Kazakhstan. Kazakhstan is aping Russia’s attacks on civil society, available at: <https://eurasianet.org/russias-foreign-agent-law-ricochets-around-kazakhstan>, 5 January 2022; The Guardian, Israel passes law to force NGOs to reveal foreign funding, available at: <https://www.theguardian.com/world/2016/jul/12/israel-passes-law-to-force-ngos-to-reveal-foreign-funding>, 12 July 2016; Committee to Protect Journalists, Proposed Salvadoran ‘foreign agent’ law could impact media organizations, available at: <https://cpj.org/2021/11/proposed-salvadoran-foreign-agent-law-could-impact-media-organizations>, 16 November 2021; Reuters, Guatemala's top court backs controversial NGO law, overturns past ruling, available at: <https://www.reuters.com/world/americas/guatemalas-top-court-backs-controversial-ngo-law-overturns-past-ruling-2021-05-13/>, 13 May 2021. [↑](#footnote-ref-65)
66. Reuters, U.N. decries Russia moves against Navalny, calls for upholding rights, available at: <https://www.reuters.com/world/un-decries-russia-moves-against-navalny-calls-upholding-rights-2021-06-21/>, 21 June 2021. [↑](#footnote-ref-66)
67. See e.g.’s Committee to Protect Journalists (CPJ), Nigerian journalist held under cybercrime act for COVID-19 coverage, available at: <https://cpj.org/2020/06/nigerian-journalist-held-under-cybercrime-act-for-covid-19-coverage/>, 10 June 2020; CPJ, Nigerian journalist Fejiro Oliver charged with cybercrime for corruption report, available at: <https://cpj.org/2020/02/nigerian-journalist-fejiro-oliver-charged-with-cyb/>, 13 February 2020; CPJ, How Nigeria’s cybercrime law is being used to try to muzzle the press, available at: <https://cpj.org/2016/09/how-nigerias-cybercrime-law-is-being-used-to-try-t/>, 21 September 2016. [↑](#footnote-ref-67)
68. Committee to Protect Journalists (CPJ), Nigerian journalist held under cybercrime act for COVID-19 coverage, available at: <https://cpj.org/2020/06/nigerian-journalist-held-under-cybercrime-act-for-covid-19-coverage/>, 10 June 2020. [↑](#footnote-ref-68)
69. Committee to Protect Journalists (CPJ), Nigerian journalist held under cybercrime act for COVID-19 coverage, available at: <https://cpj.org/2020/06/nigerian-journalist-held-under-cybercrime-act-for-covid-19-coverage/>, 10 June 2020. [↑](#footnote-ref-69)
70. Committee to Protect Journalists (CPJ), Nigerian journalist held under cybercrime act for COVID-19 coverage, available at: <https://cpj.org/2020/06/nigerian-journalist-held-under-cybercrime-act-for-covid-19-coverage/>, 10 June 2020. [↑](#footnote-ref-70)
71. MISA, Botswana media group fret over new snooping bill, available at: <https://misa.org/blog/botswana-media-groups-fret-over-new-snooping-bill/>, 26 January 2022. [↑](#footnote-ref-71)
72. MISA, Botswana media group fret over new snooping bill, available at: <https://misa.org/blog/botswana-media-groups-fret-over-new-snooping-bill/>, 26 January 2022. [↑](#footnote-ref-72)
73. MISA, Botswana media group fret over new snooping bill, available at: <https://misa.org/blog/botswana-media-groups-fret-over-new-snooping-bill/>, 26 January 2022. [↑](#footnote-ref-73)
74. See, e.g., The Sierra Leone Telegraph, Access Now and CHRDI express concern over Cybercrime Bill, available at: <https://www.thesierraleonetelegraph.com/access-now-and-chrdi-express-concern-over-cybercrime-bill>, 26 january 2022, and Global Voices, Sierra Leone’s new cybercrime bill could turn a phone into a crime scene, available at: <https://globalvoices.org/2021/03/21/sierra-leones-new-cybercrime-bill-could-turn-a-phone-into-a-crime-scene> 26 January 2022. [↑](#footnote-ref-74)
75. Access Now, Libya’s cybercrime law: A threat to freedom of expression and legalization of censorship, available at <https://www.accessnow.org/libya-cybercrime-law-threat-to-freedom-of-expression> 26 January 2022. [↑](#footnote-ref-75)
76. Access Now, When “cybercrime” laws gag free expression: stopping the dangerous trend across MENA, available at: <https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena> 26 January 2022. [↑](#footnote-ref-76)
77. See Committee to Protect Journalists, Digital Safety: Internet shutdowns, 13 April 2021, available at [https://cpj.org/2021/04/digital-safety-internet-shutdowns](https://cpj.org/2021/04/digital-safety-internet-shutdowns/) and https://cpj.org/tags/internetshutdown [↑](#footnote-ref-77)
78. Access Now, #KeepItOn, available at: <https://www.accessnow.org/keepiton/>, 2022. [↑](#footnote-ref-78)
79. Access Now, Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence, available at: <https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening/> , 12 January 2022. [↑](#footnote-ref-79)
80. Cloudflare, Internet shut down in Kazakhstan amid unrest, available at: <https://blog.cloudflare.com/internet-shut-down-in-kazakhstan-amid-unrest/>, 5 [January](https://blog.cloudflare.com/internet-shut-down-in-kazakhstan-amid-unrest/) 2022; Aljazeera, Kazakh authorities say 225 people killed in violent unrest, available at: <https://www.aljazeera.com/news/2022/1/15/kazakh-prosecutors-say-225-people-have-died-in-unres>, 15 January 2022. [↑](#footnote-ref-80)
81. Access Now, Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence, available at: <https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening/>, 12 January 2022. [↑](#footnote-ref-81)
82. Legal media center, Хроника нарушений прав в отношении сотрудников СМИ в период "газовых" протестов, available at: <https://lmc.kz/ru/news/hronika-narusheniy-prav-v-otnoshenii-sotrudnikov-smi-v-period-gazovyh-protestov>, 14 January 2022. [↑](#footnote-ref-82)
83. CPJ, Journalists detained, news crew attacked, as Kazakhstan state of emergency continues, available at: <https://cpj.org/2022/01/journalists-detained-news-crew-attacked-as-kazakhstan-state-of-emergency-continues/>, 10 January 2022. [↑](#footnote-ref-83)
84. <https://www.accessnow.org/cms/assets/uploads/2021/06/Helpline-10000-cases-report.pdf> [↑](#footnote-ref-84)