Spyware: An Unregulated and Escalating Threat to Independent Media

SAMUEL WOODHAMS
August 2021
Spyware: An Unregulated and Escalating Threat to Independent Media

AUGUST 2021

Contents

Introduction .............................................................................. 1
The Spyware Industry and the Privatization of Digital Repression .................................. 4
Spyware: The Direct and Indirect Threats to Independent Journalism .................................. 8
The Unequal Impact of Surveillance on Journalists ......................................................... 11
A New Battleground—Spyware’s Impact on Free and Independent Media ......................... 13
Reining in the Private Surveillance Industry .................................................................. 15
Protecting Independent Media from the Impact of Commercial Spyware........................... 18
Endnotes .................................................................................. 19

ABOUT THE AUTHOR

Samuel Woodhams is a digital rights researcher and freelance journalist based in London. He focuses on the intersection of surveillance technology, human rights, and democratic governance. He has written for Wired, Quartz, Al Jazeera, and CNN on issues of digital privacy, censorship, and surveillance. He also conducts research at Top10VPN, an internet research company. His research has been featured by the BBC, Reuters, The Washington Post, the Financial Times, and The Guardian. In 2020, Samuel published a peer-reviewed article in the Georgetown Journal of International Affairs on China’s role in the rise of digital authoritarianism in Africa. Samuel holds an MSc in empires, colonialism, and globalization from the London School of Economics.
Introduction

The digital surveillance industry is a broad and largely opaque network of companies that produce technology to monitor and track individuals. From tools that surveil citizens’ social media profiles to devices that indiscriminately monitor the activity of nearby mobile phones, the range and sophistication of technologies available has never been greater.

While their delivery methods and capabilities vary, all spyware products are designed to infect a user’s device and monitor their digital activity while remaining undetected. Typically, this means an infiltrator can covertly access a target’s phone calls, text messages, location, internet searches, and stored data. Even more troubling is the fact that most of the products are capable of evading antivirus tools that are specifically designed to detect malicious activity.

The rapid expansion of the digital surveillance industry has enabled governments around the world to acquire new technologies to monitor journalists, silence independent journalism, and control the flow of information. As of April 2021, the Committee to Protect Journalists (CPJ) had identified 38 cases of spyware targeting journalists, commentators, and their associates.¹ The University of Toronto’s Citizen Lab suggests the true figure could be over 50.² There are reports of spyware targeting journalists working with international media outlets, including Al Jazeera and the New York Times,³ as well as reporters and editors working for the US-based Ethiopian diaspora outlet Oromia Media Network, Colombia’s Semana magazine, and Mexico’s Proceso.⁴

In July 2021, French-based nonprofit Forbidden Stories, Amnesty International, and a consortium of 80 journalists from 17 outlets launched the Pegasus Project, a collaborative international investigative journalism initiative aimed at uncovering the extent to which Israeli spyware company NSO Group’s software is used by governments to target journalists, human rights activists, lawyers, and political dissidents.⁵ NSO Group’s signature product, Pegasus, named after the mythical winged horse, is one of the most powerful spyware tools ever deployed.⁶ Investigative journalists with the Pegasus Project revealed that at least 180 journalists were selected as potential targets of surveillance by government clients of NSO Group.⁷ The number of people who were attacked by the spyware infecting their phones remains unclear. NSO Group has repeatedly denied wrongdoing.
There is no question that spyware is being used by governments to identify, monitor, and ultimately silence journalists.

claiming it sells software to carefully vetted clients to ensure its technology is used only for law enforcement and anti-terrorism purposes.  

This is not the first time that NSO Group has been accused of abetting human rights violations. In 2019, WhatsApp filed a lawsuit against NSO Group, accusing the company of exploiting a vulnerability in the app and hacking into 1,400 accounts in 20 countries. More than 100 of these accounts are thought by WhatsApp to have belonged to journalists and human rights defenders, although the lawsuit did not disclose the identities of the victims. As a result of these allegations, the US Department of Justice reportedly renewed its investigation into the company in March 2021.

There is no question that spyware is being used by governments to identify, monitor, and ultimately silence journalists. Ronald Deibert, director of Citizen Lab, a research organization using digital forensics to verify the use of spyware against journalists, summarizes the danger this way:
The reckless and abusive use of commercial spyware to target journalists, their associates, and their families adds to the numerous and growing risks that journalists worldwide now face. Media organizations and investigative journalists are valuable “soft” targets who control important information, including information on sources, that threaten powerful actors. Thanks to companies like NSO Group, unscrupulous dictators and autocrats now have a powerful tool to aid in their sinister aims to stifle dissent and quell controversial reporting.¹¹

When the devices and digital accounts of journalists and their sources are vulnerable to surveillance, the ability of journalists to carry out their newsgathering function is significantly diminished.¹² Journalists who fear they are a target of surveillance may self-censor. Credible sources may be less likely to talk to the press, and media outlets may struggle financially to keep pace with the increasingly sophisticated threats facing their staff.

The negative impact of commercial spyware on journalists’ safety is unmistakable, notably when the information spyware extracts promotes physical attacks or even murder of a journalist or source.¹³ However, spyware’s impact on journalists globally extends far beyond the journalists and sources directly targeted. As Forbidden Stories’ Laurent Richard and Sandrine Rigaud pointed out, spyware is an ideal weapon to “kill the story.”¹⁴ It’s a new tool that governments and other actors can use to harass and intimidate journalists and their sources to prevent the publication of information.

While companies and governments tout spyware products as essential to maintaining national security and combatting terrorism, evidence is mounting about how spyware is used to target journalists and others. According to David Kaye, former United Nations special rapporteur on freedom of expression, the largely opaque and unaccountable commercial spyware industry “is causing immediate and regular harm to individuals and organizations that are essential to democratic life.”¹⁵ In particular, he highlights its impact on independent journalists worldwide and how this violates internationally agreed human rights norms.

Spyware is likely to have a growing impact on journalists and news outlets due to its increasing sophistication and availability. A clearer understanding of how the technology threatens independent media can help encourage collaboration among media stakeholders and other human rights organizations to identify threats and combat them. Together, they can raise awareness of the issue, encourage regulation to prevent the spread of spyware, and strengthen litigation efforts when it is misused.
The Spyware Industry and the Privatization of Digital Repression

According to London-based advocacy organization Privacy International, more than 500 companies globally now sell “systems used to identify, track, and monitor individuals and their communications for spying and policing purposes.”

The commercial spyware industry was estimated to be worth $12 billion in 2020. Given the secrecy of the industry and the manufacturers’ complex corporate structures, the true figure could be far higher. For example, in 2019, the European private equity firm Novalpina Capital acquired the notorious Israeli cyberintelligence firm NSO Group in a deal that valued NSO Group at an estimated $1 billion.

The industry’s growth is driven primarily by lucrative government contracts. In the past, government intelligence agencies relied on their in-house capabilities to track and monitor citizens online. With the rise of the private surveillance industry, governments around the world are now able to acquire “off the shelf” tools from the private sector without having to invest in developing the technology themselves. Between 2011 and 2017, for example, the Mexican government is alleged to have spent $80 million on NSO Group’s technology. In 2019 alone, Colombia’s military reportedly spent $800,000 on spyware from Spanish firm Mollitiam Industries.

In countries with large defense budgets, such as the United States and Israel, close cooperation among intelligence agencies and private companies has created a “revolving door as employees with security clearances and sophisticated tradecraft move back and forth between them.”

In countries with large defense budgets, such as the United States and Israel, close cooperation among intelligence agencies and private companies has created a “revolving door as employees with security clearances and sophisticated tradecraft move back and forth between them.” As a result of this revolving door, private companies have acquired the expertise needed to create technologies that emulate the advanced, state-level espionage products developed and used by governments. Many of NSO Group’s staff, for example, are reportedly alumni of Israel’s Unit 8200, an intelligence unit of the country’s Defense Forces. Candiru, another Israeli spyware firm, is also reported to recruit from the unit.

As these companies emerged, governments around the world began to recognize the role digital technologies play both in circulating news and information and in organizing protests and mobilizing dissenting voices. This recognition created a surge in demand for technologies to monitor and control the online activity of citizens, particularly...
Spyware manufacturers insist their technology is designed to protect national security, which has shielded them and their customers from scrutiny. On NSO Group’s website, the company states it “creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.” Critics argue that few laws have been passed that effectively govern the use of spyware at the global level, claiming it is naïve to think that law enforcement agencies will always use these tools in justifiable ways that conform to international human rights standards.

The rapid growth of the private surveillance industry means that sophisticated surveillance capabilities are no longer confined to countries with vast defense and intelligence budgets. Instead, private industry has stepped in to fill the demand.

dissenting groups. This confluence created “a match made in heaven” between “the people who had the skills and the people who wanted to pay for them,” according to John Scott-Railton, senior researcher at Citizen Lab. In the last decade, “just about every state [has been] trying to build its own capabilities or if it can’t, going and buying them.” The rapid growth of the private surveillance industry means that sophisticated surveillance capabilities are no longer confined to countries with vast defense and intelligence budgets. Instead, private industry has stepped in to fill the demand.

Spyware: An Unregulated and Escalating Threat to Independent Media | mediadev
Most spyware manufacturers have not willingly published a comprehensive list of their customers. Governments also regularly refuse to disclose details of their surveillance arsenals. In response to the Pegasus Project revelations, not a single country confirmed it used NSO Group’s software. Even in the United Kingdom, which has strong transparency laws, authorities have not revealed whether they have access to what are considered relatively rudimentary interception tools. In countries with weak rule of law and a lack of transparency, barriers to acquiring this information are even more pronounced. The opacity of the industry—which is cultivated by private companies and intelligence agencies—has prevented meaningful oversight and increased opportunities for its misuse. This lack of transparency has also made it practically impossible for victims of unlawful surveillance to seek justice.

### Prominent Spyware Companies and Their Suspected Customers

<table>
<thead>
<tr>
<th>Company</th>
<th>Products</th>
<th>Suspected Government Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSO Group/Q Cyber Intelligence</td>
<td>Pegasus</td>
<td>Bahrain, Egypt, Kazakhstan, Togo, Mexico</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Morocco, Mozambique, Saudi Arabia, Zambia</td>
</tr>
<tr>
<td>DarkMatter</td>
<td>Project Raven</td>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>Hacking Team</td>
<td>Remote Control System (RCS) / Da Vinci / Galileo</td>
<td>Azerbaijan, Egypt, Ethiopia, Lebanon</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monaco, Saudi Arabia, South Korea, Sudan</td>
</tr>
<tr>
<td>Gamma Group/ FinFisher</td>
<td>FinFisher, FinSpy, FinFly, FinLi</td>
<td>Bahrain, Bangladesh, Belgium, Bosnia &amp; Herzegovina, Estonia, Hungary, Italy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mongolia, Nigeria, Pakistan, Qatar, Slovakia, Singapore, South Africa, Vietnam</td>
</tr>
<tr>
<td>Mollitiam Industries</td>
<td>Invisible Man, Night Crawler</td>
<td>Brazil, Colombia, Peru, Spain</td>
</tr>
<tr>
<td>Cyberbit</td>
<td>PC Surveillance System</td>
<td>Ethiopia</td>
</tr>
<tr>
<td>Candiru</td>
<td>Sherlock</td>
<td>Uzbekistan, Saudi Arabia, United Arab Emirates, Singapore</td>
</tr>
</tbody>
</table>
While established democracies have not misused the technology to the same degree as authoritarian regimes, they still play a vital role in the commercial spyware industry by facilitating the sale of the technology to governments where its malign use is more likely. Almost 90 percent of all spyware manufacturers are based in countries considered “full” or “flawed” democracies by the Economist Intelligence Unit, with the United States, Israel, and Europe home to the most companies. However, just 7 percent of their customers are considered full democracies and over half are considered “authoritarian” or “hybrid” regimes.

Democratic governments are not the only actors reluctant to purchase sophisticated spyware on the private market. Even in contexts where attacks on the free flow of information are common, some governments prefer to rely on in-house technology. In Russia, for example, the state security services suspect that spyware software developers cooperate with the intelligence agencies of their home countries, and that using their software could provide foreign intelligence services an opportunity to compromise Russia’s operations. For this reason, Russia has never been linked to NSO Group.

While other digital practices that disrupt independent journalism, such as internet shutdowns, are relatively easy to identify, it is often not immediately clear who is responsible for the use of spyware or even whether it is being used at all. This is particularly true when spyware technology is deployed transnationally and involves a patchwork of furtive companies and government agencies. Definitively attributing use of spyware is often exceedingly difficult, adding another barrier to combatting its use and abuse.
Spyware: The Direct and Indirect Threats to Independent Journalism

The harmful impacts of sophisticated spyware are most obvious when the technology is used to support the extrajudicial killing and imprisonment of prominent journalists or their sources. While these cases may be relatively infrequent, they provide important insights that show how repressive regimes use these tools. However, they are just one aspect of how spyware negatively impacts broader independent news systems.

In 2018, Omar Abdulaziz, a Saudi dissident video blogger living in Canada, filed a lawsuit suggesting that information extracted by NSO Group’s Pegasus software may have played a role in the plot to detain and murder his friend, the journalist Jamal Khashoggi, at the Saudi consulate in Istanbul. The lawsuit alleges that the spyware was delivered via a fake DHL postal delivery text message that included a hyperlink. The malicious code covertly infected his device as soon as he clicked the link. This particular spyware can reportedly access all the stored data on a device and log all the keystrokes made by a victim. As a result, the attackers were able to monitor Abdulaziz’s communication with Khashoggi even though they were using an encrypted messaging app to communicate.

In Mexico, NSO Group’s technology was also allegedly used to target colleagues of the journalist Javier Valdez Cárdenas just days after his murder. Citizen Lab indicates that the operator of the spyware was linked to the government, although details around its use prior to the murder of Valdez remain unclear. At the time of Citizen Lab’s report, 28 targets of spyware had been identified in Mexico, and many of those were working in the news media.

In Morocco, Amnesty International accused the government of using NSO Group’s products to monitor journalist Omar Radi, who was reportedly the target of a network injection attack. Instead of requiring a target to click on an exploit link concealed in a carefully designed text message, this type of attack does not require any interaction by the targeted individual. Instead, a user’s browser or app is automatically rerouted to a malicious website where the spyware is delivered before the target is sent to the originally requested web page. The entire process takes milliseconds, making it very difficult to detect.
Radi was later charged for espionage, which, according to Human Rights Watch, was not supported by evidence. In response to his imprisonment, a group of 15 human rights organizations made a joint call demanding his release. In July 2021, Radi was sentenced to six years in prison. While the Moroccan government and NSO Group denied using spyware, it is conceivable that information acquired through its use helped facilitate Radi’s detention.

In addition to the increasing use of spyware to monitor journalists and ultimately assist in their arrest or murder, the use of commercial spyware also has a “terrorizing” effect, even when they are not directly targeted. The mere presence of this type of invasive surveillance technology may cause journalists to avoid publishing particular stories and to self-censor. It can also make it difficult for them to find sources who are willing to speak to them.
For journalists operating in less than free media environments, the presence of sophisticated spyware tools may stifle criticism of those in power and hamper investigative work that aims to unearth information withheld from public view. For Maati Monjib, a Moroccan historian and journalist who was allegedly targeted with NSO Group’s spyware, heightened surveillance forced him to “moderate [his] discourse.” According to Tasneem Khalil of Netra News, a Bangladeshi news outlet, the threat of invasive surveillance technologies is “scaring journalists into inaction.”

The proliferation of these technologies also undermines journalists’ ability to build trusted relationships with whistle-blowers and other sources. “When you have a regime or government that is so brazenly engaging in surveillance of its population, journalists’ sources are also very fearful.” Similarly, Vladimir Cortés of ARTICLE 19 says, “It is not just that they are spying on journalists, but this also has an effect on the relationships and confidence that they [can] establish with their sources.”

Media observers around the world have similar concerns. In Pakistan, the rise in covert digital monitoring is “pushing journalists to practice self-censorship.” A similar trend is unfolding in countries throughout the Middle East where surveillance technologies are exacerbating the “tendency of many in the media sector to exercise self-censorship.”

A high-quality and independent media system can be maintained only when journalists are free to engage with and report on a wider civil society that enjoys certain safeguards from repression and censorship. From creating an atmosphere of fear that promotes self-censorship to putting sources and whistle-blowers at risk, surveillance technologies dramatically undermine the ability of independent media outlets to operate independently and in the public interest.
The Unequal Impact of Surveillance on Journalists

The impact of the proliferation of targeted spyware is not uniformly experienced among journalists. Frequently, it is those most at risk that have the least access to resources to help protect them.

This is particularly true for freelance reporters, who cannot necessarily rely on the support of a media organization for assistance. News outlets in the Global South may be unable to afford the tools and resources required to keep their staff safe.

Some journalists have greater capacity to protect themselves than others. For example, in January 2020, Tom Gardner, The Economist’s correspondent in Addis Ababa, discovered that his WhatsApp account had been hacked. Although he is not certain whether he was targeted due to his role as a journalist or even if targeted spyware was used, his employment at a well-resourced international news organization likely helped him remedy the situation more quickly than many of his peers would have been able to.

“Unfortunately, I don’t think local journalists in Ethiopia are in as safe a position as somebody like myself—my Economist email is well-secured and when I lost access to my WhatsApp two weeks ago, I was able to leverage my connections to get Access Now to deal with WhatsApp very quickly to resolve the situation. I don’t think that’s something a local journalist not working for an international media outlet would be able to access.”

Gardner’s situation differs greatly from that of Venezuelan freelance journalist Margaret López, who does her reporting without the institutional support of a large, well-resourced media outlet. And working at a news outlet is itself not a guarantee that journalists will have the training and tools that could potentially help them. López notes that “Not all Venezuelan journalists have participated in training workshops on digital security. In some cases, this is because the Venezuelan media do not have the money to pay for the private training required for the entire workforce.”

Independent media supporters and civil society organizations must continue to address this disparity in access to digital security experts and technologies to bolster the safety and security of journalists.
and security of journalists. This may involve civil society organizations supporting the creation and dissemination of digital security training, as well as extending and strengthening relationships between news outlets and digital security organizations.

In response to the increased threat of spyware and other forms of digital surveillance, many journalists have adapted their methods to protect their safety and digital privacy. Both Gardner and López stress that digital privacy tools, including virtual private networks (VPNs), encrypted messaging platforms such as Signal, and encrypted email addresses, are now essential tools for journalists due to security concerns. While these tools cannot prevent the most sophisticated spyware attacks, robust digital security practices would prevent many of the most basic attacks and may even mitigate the damage of a complex attack.

## Five Useful Digital Security Training Resources for Media Professionals

<table>
<thead>
<tr>
<th>Resource</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safer Journo: Digital Security Resources for Media Trainers</td>
<td>Internnews</td>
</tr>
<tr>
<td>Surveillance Self-Defence</td>
<td>Electronic Freedom Foundation</td>
</tr>
<tr>
<td>Digital Security Helpline</td>
<td>AccessNow</td>
</tr>
<tr>
<td>Digital Security Guides</td>
<td>Reporters Without Borders</td>
</tr>
<tr>
<td>Security Planner</td>
<td>Citizen Lab/Consumer Reports</td>
</tr>
</tbody>
</table>
A New Battleground—Spyware’s Impact on Free and Independent Media

The use of spyware against journalists and news organizations creates a new battlefront in the struggle to support independent media worldwide. Globally, the news media are in a more precarious financial position than ever before, and now news outlets and civil society organizations must compete with an ever more sophisticated surveillance industry that continues to flourish.

This means that not only are journalists in danger, but entire media organizations may be at risk and unable to sustain themselves due to the financial stresses that the surveillance industry puts them under. As Courtney Radsch, former advocacy director of the Committee to Protect Journalists (CPJ), explains, “We are a group of underfunded organizations and reporters trying to counteract these incredibly well-resourced companies and governments. It is definitely not a fair fight.”

While the financial impact of increased surveillance on media outlets is unclear and not comprehensively documented, independent media may need to increase investments in privacy and security tools to keep pace with these new threats. For cash-strapped news outlets, this requires difficult trade-offs. News organizations must decide whether “to put more money towards digital security and training, or reporting, or social media optimization. There are all these choices that means it can be difficult to decide where digital security fits.”

Beyond the potential financial implications, the proliferation of surveillance can strain the relationship between journalists and the media support organizations seeking to protect them. Given the likelihood that a journalist might be surveilled, civil society organizations that support media must weigh the risk of being exposed to surveillance when they communicate with journalists. This is a concern of the Samir Kassir Foundation in Lebanon. Ayman Mhanna, executive director of the foundation, states, “The impact of surveillance technologies and the risk of spyware have forced us to be more vigilant in communicating with journalists who face threats where they live and operate.”

Given the likelihood that a journalist might be surveilled, civil society organizations that support media must weigh the risk of being exposed to surveillance when they communicate with journalists.
While the proliferation of surveillance technologies undoubtedly places additional demands on publishers and advocacy organizations, it has also opened new areas for collaboration. Mhanna, for example, said that the proliferation of surveillance has “increased the demand for assistance and training on digital safety and digital hygiene, thus opening new cooperation opportunities with universities, media outlets, and international media development organizations.”

Not only do these relationships have the potential to promote more widespread digital security awareness, they also provide the opportunity for more effective information sharing on topics of surveillance, digital rights, and internet freedoms. This, in turn, may spur more critical reporting on the topics, advancing public awareness and ultimately helping bolster efforts to rein in the industry.
Reining in the Private Surveillance Industry

The variety of actors involved in the commercial spyware industry—spyware manufacturers, governments that approve their exports, and the government end users—presents both opportunities and challenges for those working to address the use of targeted spyware technology.

On the one hand, the industry’s size provides multiple leverage points at which advocates can apply pressure to bring about change. On the other hand, its diffuse and opaque structure makes targeting each actor simultaneously a challenge to the operational capacities of civil society organizations.

One tactic opponents of spyware have employed is to demand that governments of countries where companies are based deny export licenses for this type of software, especially when they have strong indications that it will be used to violate human rights. By doing so, advocates aim to rob repressive governments of the tools used to target journalists and other members of civil society. In Israel, Amnesty International mounted a legal petition to have NSO Group’s export license revoked. In the United Kingdom and Germany, Privacy International and other human rights groups filed legal complaints against Gamma International for its role in exporting spyware to Bahrain. Since the manufacturers of spyware are overwhelmingly based in democracies, lobbying these governments for export controls may be quicker and more effective than trying to influence less accountable authorities. That said, both of the legal challenges mentioned previously were unsuccessful. As Privacy International wrote, there is an “inherent difficulty in holding an industry to account that by its nature operates under a cloak of secrecy.”

Other civil society organizations are pressuring governments that purchase and misuse spyware to protect and uphold press freedoms and human rights. In Mexico, journalists and human rights defenders filed a criminal complaint with the office of the attorney general of Mexico following a New York Times article that documented the use of spyware in the country. Then President Enrique Peña Nieto denied involvement in the attacks against journalists. Similarly, after pro-independence Catalan politicians in Spain were allegedly targeted with NSO Group’s spyware, then Spanish Deputy Prime Minister Pablo Iglesias called for an investigation into how digital surveillance technologies were being used by the government.

These advocacy strategies often overlap and, when working in tandem, aim to disrupt both the demand for and supply of the technology.
This combined approach is reflected in CPJ’s recommendation that governments introduce legislation prohibiting the use of spyware to target journalists and preventing governments from approving exports of spyware to countries with poor press freedom records.65

There are also high-level efforts to regulate the industry. David Kaye has called for a moratorium on the sale, transfer, and use of spyware.66 While this recommendation has yet to be adopted, some progress is being made. In 2020, the European Union (EU) introduced new export regulations “to prevent human rights violations and security threats linked to the potential misuse of cyber-surveillance technology.”67 Access Now and other human rights organizations praised the “positive elements” of the regulation, but also critiqued it as a missed opportunity for a more ambitious vision that includes stronger protections to safeguard human rights and security.68 Similarly, The Guardian reported in July 2021 that an Israeli commission “will examine whether rules on Israel’s export of cyberweapons such as Pegasus should be tightened” following the Pegasus Project revelations.69

While enhancing the regulation of invasive technologies is an important step in increasing transparency, it does little to prevent authoritarian regimes that already have access to these tools from using them to target journalists and stifle dissent. Advocates suggest that systemic change is required, where democratic countries responsible for exporting surveillance technologies address “fundamental questions” over “the right balance between being normative leaders and employing realpolitik.”70 Doing so may involve democratic countries preventing the export of spyware and banning its use domestically to set a global precedent that promotes the protection of human rights.

Demanding that human rights be placed at the center of foreign policy considerations may provide new opportunities for greater collaboration among advocacy groups that have traditionally worked separately. For example, those seeking to reduce the influence of the commercial spyware industry may find common cause with those working to restrict the sale of military arms to undemocratic regimes. The Campaign Against Arms Trade, for example, has access to detailed information about the United Kingdom’s exports of telecommunication interception equipment and expertise of the arms trade that could be used to help support efforts to prevent spyware attacks against journalists.71 Additionally, organizations that work to promote ethical business practices through a human rights lens may have expertise on how to pressure private companies to abide by the United Nations Guiding Principles on Business and Human Rights.72
Civil society organizations are starting to collaborate to minimize the deleterious impact of spyware. For instance, civil society groups joined forces to develop a response to the EU’s export regulation, and a coalition of human rights organizations filed an amicus brief in support of Facebook’s legal proceedings against NSO Group. In June 2021, a new Middle East and North Africa Coalition to Combat Digital Surveillance was formed. It includes press freedom organizations, like Reporters Without Borders and the CPJ, as well as regional human rights organizations, such as the Gulf Centre for Human Rights. Their aim is “to end the sales of digital surveillance tools to repressive governments in the region, fight for a safe and open internet, defend human rights, and protect human rights defenders, journalists, and internet users from governments’ prying eyes.” This broad collaborative approach helps enable knowledge transfer, educate and mobilize supporters, manage potential resource limitations, and improve litigation efforts.

Greater transparency is required from each of the actors involved in the industry. This includes spyware companies disclosing information about their clients, governments divulging details of the exports they have approved, and purchasing governments revealing how they use the technology. As journalists are one of the most affected groups, it is vital that organizations working to protect press freedoms and journalistic independence continue to push for such transparency.

Journalists themselves also play a vital role in uncovering information about the commercial spyware industry. Reporters are credited for uncovering the use of spyware in Saudi Arabia and Mexico, and for amplifying the work of research institutions such as Citizen Lab. To counter the opaqueness of the spyware industry and provide civil society organizations with up-to-date data on the malign use of such technologies, it is important that funding and opportunities remain available for investigative reporters to collaborate and continue this work. As Laurent Richard and Sandrine Rigaud argue, “the collaboration of journalists from around the world is without a doubt one of the best defenses against these violent attacks on global democracy.”
Protecting Independent Media from the Impact of Commercial Spyware

Targeted spyware has become an important way for authorities to crack down on independent media and attempt to control the free flow of information.

In an environment where journalists are routinely targeted by these invasive technologies, the critical role of a free and objective media to bolster democratic society by informing the citizenry and providing a check on power is seriously compromised.

To fully comprehend the true impact of the industry on media sectors around the world, a holistic perspective that looks at the intersection of spyware with broader threats to independent journalism and press freedom is required.

It is not just the direct threat spyware poses to journalists that should be taken into account. The potential of its use to induce self-censorship among journalists, as well as the chilling effect it creates more broadly, should also be considered in terms of how it impacts the free flow of information. While not all journalists are impacted the same way by this new technology, recent reporting suggests that its prevalence and use is more widespread than previously thought. Moreover, the growing and sustained threat spyware poses to journalists and news outlets is likely adding one more strain to an already beleaguered and under-resourced sector. Expanding common conceptions about why this technology and its use is harmful may improve advocacy efforts by broadening the arguments about its potential impacts and increasing the number of stakeholders demanding action.

Sustained collaboration among press freedom organizations, human rights nonprofits, digital security experts, journalists, and news outlets is needed to address the proliferation of targeted spyware and push for greater transparency and accountability. Without it, the commercial spyware industry will undoubtedly continue to grow unabated.
Endnotes


41 Tasneem Khalil, Netra News, personal communication, March 4, 2021
44 Khalil, personal communication.
45 Khalil, personal communication.
49 Courtney Radsch, former advocacy director, Committee to Protect Journalists, personal communication, September 2, 2020.
51 Margaret Lopez, Venezuelan freelance journalist, personal communication, February 9, 2021.
53 Radsch, personal communication.
54 Radsch, personal communication.
55 Mhanna, personal communication.
56 Mhanna, personal communication.
59 Ibid.
68 Mhanna, personal communication.
75 Richard and Rigaud, “Spyware Can Make Your Phone Your Enemy.”