“A DIGITAL PRISON”

SURVEILLANCE AND THE SUPPRESSION OF CIVIL SOCIETY IN SERBIA

EXECUTIVE SUMMARY

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

First published in 2024
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: EUR 70/8814/2024
Original language: English

amnesty.org

Cover photo: *Composite image created by Amnesty International using photos provided by SviĆe and Dragan Gmizic*

AMNESTY INTERNATIONAL

EXECUTIVE SUMMARY

In February 2024, Slaviša Milanov, an independent journalist from Dimitrovgrad in Serbia who covers local interest news stories, was brought into a police station after a seemingly routine traffic stop.

After Slaviša was released, he noticed that his phone, which he had left at the police station reception at the request of the officers, was acting strangely – the data and wi-fi settings were turned off. Aware that this can be a sign of hacking, and mindful of the surveillance threats facing journalists in Serbia, Slaviša contacted Amnesty International's Security Lab to request an analysis of his phone.

Amnesty International's analysis led to two remarkable discoveries. Firstly, forensic traces revealed that a Cellebrite product had been used to unlock his device. Cellebrite, whose forensic tool allows the extraction of all data on a device and which is used by police departments around the world, claim that they have strict policies to prevent misuse of their product; yet, this discovery provides clear evidence of a journalist's phone being targeted without any form of due process. Slaviša was neither asked for nor did he provide the passcode for his Android device. The authorities did not disclose to Slaviša that they wanted to search his device, nor did they declare any legal basis for such a search. Slaviša still does not know what data was taken from his phone.

The second finding of the analysis was even more extraordinary. Amnesty International found traces of a previously unknown form of spyware, which it has named 'NoviSpy'. NoviSpy allows for capturing sensitive personal data from a target's phone after infection and provides the ability to turn on the phone's microphone or camera remotely. Forensic evidence indicates that the spyware was installed while the Serbian police were in possession of Slaviša's device, and the infection was dependent on the use of Cellebrite to unlock the device. Two forms of highly invasive technologies were used in combination to target the device of an independent journalist, leaving almost his entire digital life open to the Serbian authorities.

The story does not end with Slaviša. Further research from Amnesty International has unveiled the breadth of digital surveillance in Serbia, including deployment of at least three different forms of spyware, as well as persistent misuse of Cellebrite's highly sophisticated digital forensics technology.

This report is a case study on how Serbian authorities have deployed surveillance technology and digital repression tactics as instruments of wider state control and repression directed against civil society. Serbia is a paradigmatic case of a system in which such tools can become core enablers of a digital crackdown, likely to be mirrored in other countries and contexts, which may well be happening already.

This report comes at a time of intensifying state repression and in an increasingly hostile environment for free expression and open debate in the country. Serbia has seen several major waves of anti-government protests since 2021, each triggering increasingly harsher response from the authorities – from sustained and vicious smear campaigns against critical non-governmental organisations (NGOs), media outlets and journalists to persistent judicial harassment of citizens organizing peacefully and engaging in political dissent.

In this report, Amnesty International combines extensive interviews with civil society representatives in Serbia, with highly technical digital forensic research to expose the concrete surveillance practices of the Serbian authorities. In revealing these tactics, the report aims to empower civil society efforts to ensure accountability for unlawful surveillance, while peeling back the layers of secrecy and reducing information asymmetry. The opacity of digital surveillance, and a perception of omnipotence and impunity, can drive and embolden a repressive state apparatus to engage in these practices, with a devastating effect on the health of a society as a whole.

The report findings reveal Serbia's pervasive and routine use of invasive spyware, including NSO Group's Pegasus spyware, alongside a novel domestically-produced Android NoviSpy spyware system, disclosed for the first time in this report. The Serbian Security Information Agency, known in Serbia as BIA (Bezbedonosno-informaciona Agencija) and the Serbian police have used the NoviSpy spyware alongside mobile forensic tools from Cellebrite to target independent think-tank activists, peaceful protesters and independent journalists.

Together, these tools provide the state with an enormous capability to gather data both covertly, as in the case of spyware, and overtly, through the unlawful and illegitimate use of Cellebrite mobile phone extraction technology. The authorities in Serbia have systematically deployed these tools against peaceful protesters who are already all too often subjected to unjustified criminalization for their activism. This unlawful digital surveillance and data collection directed against civil society violates people's right to privacy and personal data protection, and profoundly affects their other rights and freedoms, including the rights to freedom of expression, association and peaceful assembly.

The findings in this report are based on in-depth interviews with 13 people directly targeted by spyware or mobile data extraction products, or other forms of digital surveillance and 28 representatives of civil society from across Serbia who provided an invaluable insight into the increasingly challenging environment in which they operate. Their testimonies are corroborated by detailed forensic analysis on mobile devices of two dozen activists and journalists conducted by Amnesty International's Security Lab. The Security Lab used digital forensic tools developed by Amnesty International, including the open-source Mobile Verification Toolkit (MVT) and AndroidQF to gather and analyse forensic evidence for this report.

SPYWARE THREATS FACING SERBIAN CIVIL SOCIETY

The report details the history of use or procurement of highly invasive spyware, including systems from Finfisher, NSO Group, and Intellexa, by Serbian authorities over the past decade.

Critically, the research shows that at least three activists and an independent journalist had the NoviSpy spyware covertly installed on their devices during the time they attended informational interviews with the Serbian police or BIA. The infections occurred while the phones were temporarily taken away from their owners and apparently deposited in lockers in the police stations. This exceptionally deceptive tactic, i.e. installing spyware covertly on people's devices during informational interviews, appears to have been widely used. Technical evidence suggests that dozens, if not hundreds, of unique devices were targeted with the NoviSpy spyware over the last number of years. The full scope of targeting likely extends beyond the unlawful targeting of civil society.

In October 2024, an activist with Belgrade-based NGO Krokodil, was invited to BIA's office to provide information about an incident involving an attack on their organization. During the time they were attending the meeting, their phone was left unattended outside of the interview room. A subsequent forensic analysis by the Amnesty International Security Lab found evidence that the NoviSpy Android spyware was installed during that time. While less technically advanced than commercial spyware like Pegasus, the NoviSpy Android spyware still provides Serbian authorities with extensive surveillance capabilities once installed on the target's device.In addition to Slaviša and the Krokodil activist, Amnesty International found evidence of installation or attempted installation of NoviSpy spyware in at least two other cases involving Serbian civil society activists.

In response to these findings, NSO Group, which developed Pegasus, could not confirm whether Serbia was its customer but stated that the Group "takes seriously its responsibility to respect human rights, and is strongly committed to avoiding causing, contributing to, or being directly linked to negative human rights impacts, and thoroughly review all credible allegations of misuse of NSO Group products."

NOVISPY SPYWARE CONNECTS BACK TO BIA

An analysis of multiple NoviSpy spyware app samples recovered from infected devices, found that all communicated with servers hosted in Serbia, both to retrieve commands and surveil data. Notably, one of these spyware samples was configured to connect directly to an IP address range associated directly with Serbia's BIA. The research also found that configuration data embedded in the spyware sample ties back to a specific BIA employee, who was previously linked to Serbia's efforts to procure Android spyware from the now defunct spyware vendor, Hacking Team.

These significant operational security mistakes, and the fact the spyware was installed in multiple cases during interviews with BIA officers, allows Amnesty International to attribute with high confidence these spyware campaigns to BIA and the Serbian authorities.

MISUSE OF CELLEBRITE DIGITAL FORENSIC TOOLS

This report also reveals the extensive and illegitimate use of Cellebrite extraction technology to download personal data from the phones of protest organizers and journalists. The data obtained through use of such tools can allow authorities to map the social networks of protest movements, collect encrypted conversations from apps like Signal and Telegram, and mine cloud-stored data. The ability to download, in effect, an individual's entire digital life using Cellebrite UFED and similar mobile forensic tools, poses enormous human rights risks, if such tools are not subject to strict control and oversight. The legal controls in Serbia on the use of such tools are insufficient and Serbia's use of Cellebrite forensic products poses serious risks to human rights.

In at least two cases Amnesty International documented, the Cellebrite UFED product and associated exploits were used to covertly bypass phone security features, enabling Serbian authorities to infect the devices with NoviSpy spyware. These covert infections, which also occurred during interviews with police or BIA, were only possible because of the capabilities provided by advanced technology like Cellebrite UFED to bypass device encryption. While activists have long expressed concerns about spyware infections occurring during police interviews, Amnesty International believes that this report describes the first forensically documented spyware infections enabled by the use of Cellebrite mobile forensic technology.

This research also uncovered a zero-day Android privilege escalation exploit used in Cellebrite UFED, patched in the course of this research, helping to protect millions of Android devices. In collaboration with security researchers at Google, Amnesty International identified the exploit from the careful analysis of forensic logs found on the phone of a protest organizer detained by Serbian authorities.

CRACKDOWN ON CIVIC SPACE IN SERBIA

Digital surveillance in Serbia is taking place amid rising state repression and a deteriorating climate for free expression. Since 2021, the country has seen numerous anti-government protests, each met with harsher crackdown by the authorities. Following country-wide mass protests in July and August 2024 against lithium mining and Serbia's agreement with the European Union (EU) on access to raw materials, the government assault on civil society dramatically escalated. In August, a widely watched pro-government outlet, TV Informer, featured extensive reports suggesting that some 40 "foreign-funded" NGOs were "waging special war against Serbia" at the behest of foreign donors, describing them as "foreign mercenaries." The defamatory statements about these organisations were further fuelled by senior officials, including the President, members of the Parliament, and the Governor of the National Bank.

Simultaneously, the activists taking part in or speaking about the anti-lithium protests, faced arrests and baseless, yet extremely serious, criminal charges, including "inciting the violent overthrow of the constitutional order," a criminal offense carrying a penalty of up to eight years of imprisonment. Activists and lawyers interviewed for the report recounted how the police frequently cited activists' posts on social media, their speeches or their mere participation in the protests as a basis for these charges. According to Civic Initiatives, at least 33 people were arrested or detained for informational interviews during the August protest, subjected to long questioning, search of their apartments, and seizure and search of their telephones and computers. Not one of them has been formally charged at the time of this report's publication.

Amnesty International spoke with nine activists who were detained or questioned between July and November 2024 and whose telephones and computers were temporarily seized by the police and subjected to in-depth searches, including the extraction of digital data in order to allow prosecutors to decide whether to formally charge them or not. However, the activists suspected that these intrusive investigative measures, which seem to be lawful under Serbian legislation, were a pretext for the police and security services to learn more about their social networks and their future plans, rather than pursue criminal charges.

SERBIA'S INADEQUATE LEGAL AND OVERSIGHT FRAMEWORK FOR DIGITAL SURVEILLANCE

Serbia's legislation provides for the use of exceptional measures, including secret communications surveillance, and sets specific circumstances in which such measures could be lawfully used. However, the deployment of advanced technologies, including spyware and other advanced digital forensic tools that collect vast amounts of personal data, is not fully recognised or sufficiently regulated by law, leaving too much space for potential abuse of such techniques, including for political purposes.

The generic provisions regulating the application of special measures across several different laws are not sufficiently clear, nor do they provide meaningful safeguards against misuse when it comes to digital surveillance technologies, which are far more intrusive and less targeted than the conventional means of covert communications surveillance, such as wiretapping. Even the mechanism of judicial ex-ante oversight, such as a judicial decision that specifies measures, strict timespan and the target of a surveillance, cannot provide effective protection against advanced digital surveillance tools, including spyware, that can gain complete and uncontrolled access to the data, messages, images, files and metadata on one's device.

Moreover, in the context of often-noted concerns about undue political influence of the government on courts and prosecutors and the degree of state capture in Serbia, the means of control and oversight over the use of special measures, which might appear sufficient on paper, are rendered meaningless or ineffective in practice.

Serbian government did not comment on the report findings, the details of which were shared with them ahead of the publication.

CHILLING EFFECT

Digital surveillance does not only have a devastating impact on people's right to privacy but also profoundly affects the rights to freedom of expression, association and peaceful assembly. Activists in Serbia told Amnesty International how learning that they were targeted made them feel violated, vulnerable and alone, and forced them to reconsider or change their behaviour. Some became more reluctant to speak out about controversial issues, while others decided to lower their profile or completely disengage from activism.

After learning that he was targeted, Slaviša was very concerned that some of his sources could have been compromised and had to change the way in which he researched his articles and engaged with sources:

"I can no longer use phone or email and have to find other ways to speak with people, including in person. I tend to do this only when we are in public places and in larger groups, which is obviously not ideal."

"Goran" was one of the other activists targeted with Pegasus and interviewed by Amnesty International. For him, the attack caused a great deal of soul-searching about future work.

"It led me to question my engagement in the organization. I asked myself if I should carry on working, and how this affects the organization and considered stepping down. An attack like this truly digs deep into one's personal integrity, and one's attitude towards work, and makes you question if you are prepared to continue doing what you're doing, despite this. I had hundreds of questions."

"Goran" stayed at the organization but had to introduce numerous security measures both in his personal life and his organization.

"If the government can do what they did to me, they can target someone else next. I realized that the activities of all civil society organizations are under constant scrutiny by the authorities and that we must stay vigilant."

For the organizations already facing numerous pressures, having to deal with digital security issues was yet one more distraction from doing the core work, a Krokodil activist told Amnesty International

"Having to deal with so many different attacks at the same time is keeping us very busy and will weaken us so fundamentally, to the point that we will not be able to operate at all...This is probably the aim."

HUMAN RIGHTS RESPONSIBILITIES OF COMPANIES AND OTHER PARTIES

While states have the primary duty to uphold human rights law, companies and other parties have a responsibility to respect human rights wherever they operate in the world and across all their business activities. A key part in fulfilling this responsibility is the adequate implementation of human rights due diligence to identify, prevent and mitigate for the potential risks to human rights to which the companies could contribute. Amnesty International found a number of companies have failed to fulfil their human rights responsibilities in Serbia.

Additionally, the Norwegian Ministry of Foreign Affairs, which donated the Cellebrite UFED technology, and the United Nations Office for Project Services (UNOPS), which managed procurement for the Norwegian government's grant to Serbia's Ministry of Interior, failed to conduct an adequate due diligence process to assess and mitigate for the potential risks of this technology to human rights or provide safeguards against its abuse. Given the weak regulatory environment for digital surveillance in Serbia, concerns about the independence of the judiciary, and persistent reports of threats to civil society and independent journalists, the Norwegian government and UNOPS had a responsibility to exercise oversight and due diligence when procuring highly invasive technology and handing it over to Serbian institutions. By failing to do so, they enabled and contributed to Serbia's violations of people's rights to privacy, freedom of expression, association and peaceful assembly through unlawful digital surveillance.

In a response to the details of the findings, the Norwegian Ministry of Foreign Affairs said that the Ministry finds it "alarming that digital forensic tools, purchased through a project funded by Norway, may have been misused top target members of civil society in Serbia," and added that, "if correct, [this] would be in clear violation of core principles of Norwegian development assistance, and the agreed purpose of the support to Serbian authorities at the time." The Ministry added that UNOPS, which was responsible for all project activities, is expected to conduct a thorough investigation of the alleged misuse.

Just as crucially, Cellebrite had a responsibility to conduct human rights due diligence to ensure that its product did not cause or contribute to adverse human rights impacts. On its website, Cellebrite states that the company will "take any actions necessary to prohibit bad actors from using or accessing" their solutions when Cellebrite technology is "used in a manner that is not in accordance with international law, does not comply with Cellebrite's terms of use or is not aligned with Cellebrite's corporate values." Yet, all information available to date indicates that Cellebrite has not taken sufficient and effective measures to use its leverage to address the human rights risks in Serbia. As Amnesty International's research in Serbia demonstrates, the use of Cellebrite's product has had an adverse impact on the human rights of Serbian activists and journalists. At the very least, Cellebrite is directly linked to these human rights violations.

Cellebrite has fallen short of its corporate responsibility under the UN Guiding Principles on Business and Human Rights to mitigate and prevent potential and actual harms to human rights defenders and therefore more effective human rights due diligence policies and procedures are needed. In situations where a company has contributed to actual impacts, the company should also provide remedy to affected individuals.

In response to Amnesty International's queries sent to Cellebrite during the research process, as further explained in the full report, Cellebrite sent a short response stating that it was not a surveillance company and did not provide cyber surveillance technology or spyware. It noted that the company's product was a "digital investigative platform [that] equips law enforcement agencies with technology needed to protect and save lives, accelerate justice and preserve data privacy," and that their products "are licensed strictly for lawful use, require a warrant or consent to help law enforcement agencies with legally sanctioned investigations after a crime has taken place."

Prior to publication, Amnesty International shared this report's findings with Cellebrite. In response, Cellebrite said, "Our digital investigative software solutions do not install malware nor do they perform real-time surveillance consistent with spyware or any other type of offensive cyber activity.

"We appreciate Amnesty International highlighting the alleged misuse of our technology. We take all allegations seriously of a customer's potential misuse of our technology in ways that would run counter to both explicit and implied conditions outlined in our end-user agreement.

"We are investigating the claims made in this report. Should they be validated, we are prepared to impose appropriate sanctions, including termination of Cellebrite's relationship with any relevant agencies."

A full analysis of the company's human rights responsibilities can be found in the full report and both of the company's responses can be found in the appendix of the report.

CONCLUSION AND RECOMMENDATIONS

The findings of this report are emblematic of how a repressive state apparatus can combine disparate surveillance practices to achieve their objectives. The report also highlights emerging surveillance tactics including the widespread use of invasive digital forensic tools to collect data from peaceful protestors not charged with any crime. As security improvements make zero-click and other remote spyware attacks prohibitively expensive or unfeasible, authorities may increasingly turn to infecting devices with spyware through physical access to a device. Indeed, some States have proposed specific legislation to allow secret break-ins to homes in order to infect devices with targeted spyware.

Serbia must commit to immediately stop using-highly invasive spyware and carry out prompt, independent and impartial investigations into all documented and reported cased of unlawful digital surveillance. It also must take concrete steps to ensure that digital technologies are not misused to violate human rights, including by putting in place and robustly enforcing a legal framework that provides meaningful procedural safeguards, effective systems of control and oversight through judicial review, and effective mechanisms for redress for victims.

Cellebrite and other digital forensic companies designing and providing law enforcement and security agencies with highly intrusive technologies must conduct meaningful and thorough due diligence to ensure that their products are not used in a way which contributes to human rights violations. In particular, Cellebrite should investigate how its technology has been used in Serbia to assess possible adverse human rights impact and act on its commitment to "take any actions necessary", including not renewing Cellebrite licences, to prohibit bad actors from using or accessing their solutions in a manner that is inconsistent with international law.

See full list of recommendations at the end of the report.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

“A DIGITAL PRISON”

SURVEILLANCE AND THE SUPPRESSION OF CIVIL SOCIETY IN SERBIA

EXECUTIVE SUMMARY

This report documents how Serbian authorities have deployed surveillance technology and digital repression tactics as instruments of wider state control and repression directed against civil society. The report findings reveal Serbia’s pervasive and routine use of invasive spyware, including NSO Group’s Pegasus spyware, alongside a novel domestically-produced Android NoviSpy spyware system, disclosed for the first time in this report. The report highlights widespread misuse of Cellebrite’s UFED mobile forensics tools against Serbian environmental activists and protest leaders.

INDEX: EUR 70/8814/2024
DECEMBER 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL