“A DIGITAL PRISON”

SURVEILLANCE AND THE SUPPRESSION OF CIVIL SOCIETY IN SERBIA

PROTECT THE PROTEST

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 70/8813/2024
Original language: English

amnesty.org

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

AMNESTY INTERNATIONAL

1. EXECUTIVE SUMMARY **7**

2. METHODOLOGY **13**

3. INTRODUCTION **16**

3.1 CIVIC SPACE IN SERBIA 17

3.2 PROTESTS IN SERBIA 2021-2024 18

3.3 STIGMATIZATION AND SMEAR CAMPAIGNS THROUGH MEDIA 19

3.4 PERSISTANT HARASSMENT AND INTIMIDATION OF CIVIL SOCIETY AND JOURNALISTS 21

4. SPYWARE TARGETING HRDS AND JOURNALISTS IN SERBIA **24**

4.1 PREVIOUS REPORTS OF SERBIAN SPYWARE PROCUREMENT 25

4.2 PREDATOR SPYWARE DEPLOYED IN SERBIA 25

4.3 PEGASUS SPYWARE TARGETING CIVIL SOCIETY IN SERBIA 26

4.3.1 TWO SERBIAN THINK-TANK ACTIVISTS TARGETED BY PEGASUS (CASE 1) 27

4.3.2 PROTEST ORGANIZER TARGETED BY PEGASUS (CASE 2) 28

4.4 NOVEL "NOVISPY" ANDROID SPYWARE DEPLOYED BY SERBIAN AUTHORITIES 28

4.4.1 SPYWARE INSTALLED COVERTLY DURING INTERVIEW WITH BIA (CASE 3) 29

4.4.2 SPYWARE INSTALLED ON PHONE OF JOURNALIST FOLLOWING TRAFFIC STOP (CASE 4) 32

4.4.3 NOVISPY SPYWARE INSTALLED ON DEVICE OF YOUTH ACTIVIST (CASE 5) 33

4.4.4 ATTEMPTS TO INSTALL SPYWARE ON DEVICE OF ENVIRONMENTAL ACTIVIST (CASE 6) 34

4.5 ATTRIBUTION OF THE MALICIOUS APPLICATIONS TO BIA 36

4.6 WIDER TARGETING USING SERBIAN ANDROID SPYWARE 37

4.6.1 GOOGLE CONFIRMS MALICIOUS NATURE OF NOVISPY SPYWARE 38

5. MISUSE OF CELLEBRITE DATA EXTRACTION TOOLS IN SERBIA **39**

5.1 HOW CELLEBRITE CAN BREAK INTO PHONES 41

5.1.1 ZERO-DAY EXPLOIT DISCOVERED FROM PHONE OF SERBIAN ACTIVIST 41

5.2 PHONES UNLOCKED WITH CELLEBRITE UFED AND INFECTED WITH SPYWARE 42

5.2.1 JOURNALIST'S PHONE UNLOCKED WITH CELLEBRITE BEFORE INFECTION WITH NOVISPY SPYWARE (CASE 4A) 42

5.2.2 CELLEBRITE USED TO UNLOCK PHONE OF YOUTH ACTIVIST INFECTED WITH SPYWARE (CASE 5A) 44

5.2.3 IMPLICATIONS OF CELLEBRITE USE TO ENABLE SPYWARE INFECTIONS 44

5.3 CELLEBRITE USED ON ENVIRONMENTAL ACTIVISTS AND PROTESTORS 45

5.3.1 CELLEBRITE ZERO-DAY EXPLOIT USED TO EXTRACT PHONE OF ENVIRONMENTAL ACTIVIST (CASE 7) 45

5.3.2 SUSPECTED USE OF CELLEBRITE PRODUCTS TO INSPECT AND SEARCH PHONES OF ENVIRONMENTAL PROTESTORS 46

5.4 NORWEGIAN DONATION OF CELLEBRITE TO SERBIA'S MINISTRY OF INTERIOR 46

6. SURVEILLANCE IS SILENCING CIVIL SOCIETY IN SERBIA **49**

6.1 THE CHILLING EFFECT 49

6.2 SELF-CENSORSHIP 50

6.3 DISENGAGEMENT 50

7. NATIONAL LEGAL FRAMEWORK ON DIGITAL SURVEILLANCE IN SERBIA 52
7.1 SPECIAL EVIDENTIARY MEASURES 53
7.2 TARGETED SEARCH MEASURES 53
7.3 SURVEILLANCE FOR THE PURPOSE OF NATIONAL SECURITY 54
7.4 INSPECTION AND SEARCHES OF DIGITAL DATA 54
7.5 DATA RETENTION 55
7.6 OVERSIGHT OVER SPECIAL MEASURES 56
7.7 LACK OF NECESSARY SAFEGUARDS 57
7.7.1 WEAK JUDICIAL OVERSIGHT 57
7.7.2 INEFFECTIVE OVERSIGHT AND LACK OF REMEDY FOR VIOLATIONS 58
7.7.3 BLURRY LINES BETWEEN POLICE AND SECURITY SERVICES 58
8. HUMAN RIGHTS ANALYSIS 60
8.1 HUMAN RIGHTS COMPATIBILITY OF THE USE OF SPYWARE 62
8.1.1 HIGHLY INVASIVE SPYWARE 62
8.1.2 SERBIAN NOVISPY SPYWARE 62
8.2 HUMAN RIGHTS IMPACT OF THE USE OF CELLEBRITE AGAINST JOURNALISTS AND HRDS IN SERBIA 63
8.3 HUMAN RIGHTS RESPONSIBILITIES 63
8.3.1 HUMAN RIGHTS DUE DILIGENCE ACROSS THE VALUE CHAIN 64
8.3.2 CELLEBRITE'S HUMAN RIGHTS DUE DILIGENCE ACROSS THE VALUE CHAIN 65
8.3.3 CELLEBRITE'S HUMAN RIGHTS RESPONSIBILITIES 67
8.4 HUMAN RIGHTS RESPONSIBILITIES OF NSO GROUP AND INTELLEXA 68
9. RECOMMENDATIONS 69
9.1 TO SERBIAN AUTHORITIES 69
9.2 TO THE NORWEGIAN GOVERNMENT 70
9.3 TO THE EUROPEAN UNION 70
9.4 TO HUMAN RIGHTS DEFENDERS 71
9.5 TO MOBILE DEVICE VENDORS 71
9.6 TO NSO GROUP, INTELLEXA AND OTHER SURVEILLANCE TECHNOLOGY VENDORS 73
10. ANNEXES 75
10.1 ANNEX 1: HOW CELLEBRITE UFED AND EXTRACTION TOOLS FUNCTION 75
10.2 ANNEX 2: FORENSIC ANALYSIS OF USE OF CELLEBRITE ON THE PHONE OF "IVAN" 78
10.3 ANNEX 3: TRACES OF POSSIBLE ZERO-CLICK SPYWARE TARGETING OF "IVAN" 80
10.4 ANNEX 4: FORENSIC ANALYSIS OF CELLEBRITE USE AGAINST "SLAVIŠA" 82
10.5 ANNEX 5: INTELLEXA CUSTOMER RELATED INFRASTRUCTURE 83
10.6 ANNEX 6: NOVISPY SPYWARE SAMPLES AND INFRASTRUCTURE 84
10.7 ANNEX 7: CELLEBRITE RESPONSE TO AMNESTY INTERNATIONAL 85

GLOSSARY

WORD	DESCRIPTION
SPYWARE	*Spyware* is software which enables an operator to gain covert access to information from a target computer system or device.
COMMERCIAL SPYWARE	*Commercial or mercenary spyware* are surveillance products developed and sold by corporate actors to governments to conduct surveillance operations. So called "end-to-end" commercial spyware systems provide a full system for device infection and data collection. Components of these systems include the exploits used to install the spyware, a spyware agent which runs on the target device after infection and backend systems to gather and analyse the collected surveillance data.
SPYWARE AGENT	A *spyware agent* (or implant) is the final software code installed on a computer or phone after it has been successfully infected. The agent is responsible for collecting data from the device, activating sensors such as microphones and cameras, and uploading this data to the spyware operator.
HIGHLY-INVASIVE SPYWARE	*Highly-invasive spyware* is spyware which can gain complete access to all data on a targeted device and whose functionality is not limited to accommodate the need for proportionality, or spyware who's use cannot be independently audited or verified in case of abuse.
SOFTWARE VULNERABILITY	A *software vulnerability* is a technical flaw or weakness in a software component or piece of code which can be exploited by an attacker to bypass security defences.
EXPLOIT	An *exploit* is a piece of software or code which takes advantage of (or exploits) one or more software vulnerabilities to gain access to a device. On modern mobile devices exploits must bypass numerous layered security defences and can be highly complex. A full exploit chain targeting latest device versions can sell for millions of euros.
ZERO-DAY	A *zero-day vulnerability* is a software flaw which is not known to the original software developer and for which a software fix is not available. A zero-day exploit taking advantage of this flaw can successfully target even fully patched and updated devices.
VECTOR	*Vector* is a surveillance industry term for the different pathways or techniques which can be used to deliver an exploit to a target device. These include so called *1-click* and *zero-click* vectors.
1-CLICK	A *1-click* attack requires action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles. If clicked on, the

WORD	DESCRIPTION
	attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device.
ZERO-CLICK	A *zero-click* attack is a surveillance industry marketing term for any vector which can infect a device without requiring a user action, such as clicking on a link. *Fully remote* zero-click attacks allow infection over the internet, often by exploiting flaws in popular messaging apps such as iMessage or WhatsApp. Non-remote or *tactical* zero-click attacks can silently infect devices where the attacker has privileged network access or is in physical proximity to the target.
DIGITAL SURVEILLANCE	*Digital surveillance* refers to the use of digital technologies to collect information about targeted individuals or groups. This includes both covert surveillance tactics, such as the use of spyware; and the use of invasive digital forensic products to collect sensitive information from mobile phones and computers of targeted individuals.
BINARY	A compiled version of a software program in machine-readable code, typically consisting of 0s and 1s, that can be directly executed by a computer's hardware without further processing.
SLAPP	A *SLAPP* (Strategic Lawsuit Against Public Participation") lawsuit is filed with the primary intent to intimidate or silence critics by burdening them with the cost of legal defense, rather than addressing actual legal grievances.
BRUTE-FORCE	A *brute-force attack* is used to gain unauthorized access to systems, networks, or encrypted data by systematically testing all possible combinations of credentials or keys until the correct one is found through trial and trial-and-error.
SPECIAL EVIDENTIARY MEASURES	*Special Evidentiary Measures* refer to any covert data collection, including secret communication surveillance measures, that are carried out by police or BIA for criminal investigative purposes and regulated by Serbia's Criminal Procedure Code.
TARGETED SEARCH MEASURES	*Targeted Search Measures* refer to special measures, including secret communications surveillance, by police, carried out for the limited purpose of arresting a suspect, and regulated by the Serbian Law on Police.
NOVISPY	A newly discovered Serbian Android spyware system with capabilities to collect extensive information from a targeted Android phone.
IOCS	*IOCs* ("Indicators of Compromise") are digital forensic artifacts, such as IP addresses, domain names, or file hashes, that indicate a potential security breach or malicious activity within a system or network.
MVT	MVT ("Mobile Verification Toolkit) is an open-source consensual forensic tool, originally published by Amnesty International used to detect traces of spyware or other malicious software on mobile devices.
ARTIFACT	A piece of data or evidence retrieved from a digital device, such as log files, binaries, or metadata, used in forensic analysis to understand activity or reconstruct events.
MOBILE FORENSICS TECHNOLOGIES	Mobile forensic tools or mobile data extraction products, are specialised systems used by law enforcement or intelligence services to recover, analyze, and interpret data from mobile devices for legal or investigative purposes. There tools can be used non-consensually to unlock devices or bypass device security mechanisms.

1. 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-informativna 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, stated that it could not comment on specific existing or past customers and therefore whether Serbia was its customer, but stated "that we are talking about a significantly democratic and free country" when referring to Serbia. The response also 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 organizations 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 recognized 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.

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 and to 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 have 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 to 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 has a responsibility to conduct human rights due diligence to ensure that its product does not cause or contribute to adverse human rights impacts, or that it is directly linked to any 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 and impacts 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.

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.

2. METHODOLOGY

This report investigates Serbia's recent use of unlawful digital surveillance to target human rights defenders, activists and journalists critical of the authorities and its impact on people's right to freedom of assembly, expression and association. Digital surveillance, including the use of spyware and invasive digital forensic technologies, are among the plethora of repressive measures used by Serbian authorities in the context of recurring anti-government protests and the broader crackdown against civil society.

In the context of this report, digital surveillance refers to the use by authorities of digital technologies to collect information about targeted individuals or groups. This includes both covert surveillance tactics, such as the use of spyware; and the use of invasive digital forensic products, at times also covertly, to collect large amounts of sensitive information from mobile phones and computers of targeted individuals.

This research contributes to Amnesty International's global flagship campaign, "Protect the Protest", which challenges the increasing repression of peaceful protests, acts in solidarity with those targeted and supports the causes of social movements advocating for human rights change.[1] It is also a part of Amnesty International's ongoing research to monitor the development and deployment of surveillance technologies, including targeted mobile spyware, which threaten human rights defenders and civil society globally.[2] Finally, it builds on the ongoing work of documenting the increasingly more repressive measures used by the Serbian authorities against civil society, activists and independent journalists, especially in the context of recurring anti-government protests.[3]

The report is primarily based on research conducted between December 2023 and November 2024, including online interviews and two field trips to Serbia – in October and November 2024.

During the course of the research, Amnesty International interviewed 28 representatives of civil society from Belgrade and other towns across Serbia, including 13 people directly targeted by unlawful spyware or invasive and often covert digital forensic searches, including 10 men and 3 women. The purpose of these interviews was to (i) gain insight into the scale of and the impact of the persistent pressure and attacks against NGOs, activists and journalists in Serbia and (ii) get a better understanding of the mechanics used by the authorities to target civil society members with digital surveillance, and (iii) understand the impact of the use of highly intrusive surveillance on the people affected and on their ability to stay engaged in the issues of public interest.

---

[1] Amnesty International, *Under Protected and Over Restricted: The state of the right to protest in 21 European countries* (Index: EUR 01/8199/2024), 8 July 2024, https://www.amnesty.org/en/documents/eur01/8199/2024/en/

[2] Amnesty International's research on surveillance is published at https://securitylab.amnesty.org/. For examples of recent reports, see Amnesty International, "Thailand: State-backed digital violence used to silence women and LGBTI activists", 16 May 2024, https://www.amnesty.org/en/latest/news/2024/05/thailand-state-backed-digital-violence-silence-women-lgbti-activists/ and Amnesty International, "Global: 'Predator Files' spyware scandal reveals brazen targeting of civil society, politicians and officials", 9 October 2024, https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/

[3] Amnesty International, *Serbia: Submission for the EU Enlargement Package/Opinion 2024*, 23 May 2024, https://www.amnesty.eu/news/serbia-amnesty-international-submission-for-the-eu-enlargement-package-opinion-2024/#:~:text=23rd%20May%202024-,Serbia%3A%20Amnesty%20International%20submission%20for%20the%20EU%20Enlargement%20Package%20%2F%20Opinion,membership%20in%20the%20European%20Union; See Amnesty International, *Serbia: Submission for the EU Enlargement Package/Opinion 2023* (Index: EUR 70/6688/2023), 17 April 2023, https://www.amnesty.org/en/documents/eur70/6688/2023/en/ and Amnesty International, *Europe: Under Protected and Over Restricted: The state of the right to protest in 21 European countries that relate to Serbia* (Index: EUR 01/8199/2024), 8 July 2024, https://www.amnesty.org/en/documents/eur01/8199/2024/en/

The accounts of recipients are corroborated by a review of official documents, including search warrants, court and police orders, relating to nine people who were either brought in for questioning by the police, had their homes searched and/or had their devices (smartphones or computers) temporarily seized by the police.

It is further corroborated by detailed forensic analyses performed by Amnesty International's Security Lab on mobile devices of two dozen members of Serbian civil society who suspected they were targeted using spyware, mobile data extraction products, or other forms of digital surveillance. 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.[4] The Security Lab also relied on internet scanning data and previous technical investigations carried out by Amnesty International to document the history of spyware usage in Serbia.

Etienne Maynier of Human Rights Watch's digital security team was asked to independently review an earlier draft of this report. His review affirmed that the report's forensic methodology was sound, and that the forensic findings on the use of spyware and Cellebrite products presented in the report are credible. Mr Maynier did not have access to original forensic data, and as such, his analysis is based on the forensic evidence documented in the report.

Amnesty International also conducted extensive desk research, including a review of legal and policy frameworks governing the use of digital surveillance in Serbia as well as international human rights law and standards; research from partner organizations, media outputs, academic articles, official statistics and documents.

In addition, the research focused on the tender documentation related to the procurement of the licences for the Cellebrite UFED technology, grant documentation and other exchanges between the Serbian authorities, namely the Ministry of Interior, and the Norwegian Embassy in Belgrade, which donated the digital forensic equipment to Serbia in 2019. In addition to publicly available documents, Amnesty International obtained considerable project documents relating to the Norwegian Government's donation through a freedom of information access request to the Norwegian Ministry of Foreign Affairs.

Interviews with representatives of civil society organizations and persons who were targeted with digital surveillance were conducted in Serbian. All interviewees were informed about the nature and purpose of our research and how the information provided would be used and gave their written consent. As is standard in Amnesty International's objective and impartial research practices, no incentives were given to interviewees in exchange for their accounts.

Unless explicitly stated, the names of activists, and in some instances identifying details such as the names of organizations and similar have been excluded and/or changed to protect people's security, privacy and confidentiality. Personal names that have been changed are marked by quotation marks (").

In September 2024, Amnesty International wrote to the Serbian government, including to the Ministry of Interior and Security Information Agency, the Norwegian Ministry of Foreign Affairs, and Cellebrite to notify them of the ongoing research and request specific information relating to the use of digital surveillance. Only Cellebrite responded at the time.[5]

In November 2024, in line with the organization's Right of Reply policy, Amnesty International shared the detailed findings of the research with the Serbian Ministry of Interior, Serbian Security Information Agency, Norwegian Ministry of Foreign Affairs, United Nations Office for Project Services (UNOPS), Cellebrite, NSO Group, and Intellexa and sought their written responses to specific allegations ahead of the publication of this report. Amnesty received responses from NSO Group and the Norwegian Ministry of Foreign Affairs, which are included throughout the report. The responses from Cellebrite are discussed in Chapter 5 and can be found in Annex 7.

Amnesty International would like to express gratitude to the activists, journalists and human rights defenders who agreed to share their stories and to civil society organizations in Serbia who generously provided support for this research. In particular, Amnesty International is grateful to the partners in SHARE Foundation, Reporters Without Borders, and Access Now for assisting this research and providing key information about the national context. Amnesty International is deeply appreciative to Etienne Maynier of Human Rights Watch for his independent review of this research report.

[4] For Mobile Verification Toolkit (MVT) and AndroidQF, see Amnesty International Security Lab, Tools and Guides, https://securitylab.amnesty.org/tools-and-guides/

[5] Email from Cellebrite Senior Director for Corporate Communications to Amnesty International in response to Amnesty International's research letter of 20 September 2024, 5 October 2024. On file with Amnesty International.

Amnesty International extends special thanks to Benoît Sevens of Google's Threat Analysis Group, and Seth Jenkins and Jann Horn from Google Project Zero for their invaluable assistance in this investigation, particularly in efforts leading to the successful identification of an Android zero-day security vulnerability used to target Serbian civil society.

Amnesty International is very grateful to SviĆe organization for giving permission to use their photos as part of the cover image on this report.

3. INTRODUCTION

Authorities across the world are increasingly using highly invasive spyware, mobile phone forensic products, and other intrusive surveillance technologies to control and monitor civil society and journalists, silence dissent and discourage civil engagement. Over the past several years, there has been a growing number of reports of governments, including in Europe, directly targeting human rights defenders, journalists and opposition groups with advanced and extremely invasive technologies, including spyware and other digital surveillance tools.

Such tools often exploit non-public vulnerabilities in the operating system of the devices they target and enable covert surveillance by monitoring, extracting, collecting or analysing data. However, unlike conventional wiretapping and communications surveillance, which only allow real-time monitoring of specific communications, more advanced techniques, like spyware, provide access to the full range of one's data – even retrieving historic and deleted communication, messages and files on the person's device. Spyware can even subvert the camera and microphone on an infected device to use them to spy on the owner or their surroundings.

A recent European Parliament study of the use of spyware in the European Union showed that the use of spyware had been fully embedded into the legal systems of some countries and, at least on paper, has been accompanied by the required safeguards, mechanisms of oversight and redress.[6] Yet, as the study indicated, these legal systems were often too permissive, legal safeguards too weak, and access to justice and redress virtually non-existent. In some cases, indeed, the entire system was "designed purposefully to serve as a tool of power and control," and was used as a part of a deliberate strategy.[7]

Governments tend to justify the use of advanced digital surveillance, including spyware, as necessary to protect national security or public order. But governments have often used spyware as a means of domestic espionage rather than for legitimate public security concerns, posing a serious threat to civil society and civic engagement.[8] This gross misuse of surveillance for political purposes has been, at least in part, enabled by the weak domestic legal frameworks regulating the use of covert surveillance that have not kept up with the lightning-fast development of new surveillance technologies. However, even the systems with more robust mechanisms of scrutiny and oversight can be rendered meaningless in the face of powerful hacking tools that have complete and unfettered access to someone's private life.

While well-regulated digital technologies have their rightful place in law-enforcement, highly invasive spyware, such as Pegasus and Predator, poses significant threats to the rights to privacy, freedom of expression, peaceful assembly and association and can never be justified. The use of highly invasive spyware has a devastating impact on the individuals affected, others in their network and the broader environment of free expression. As the Council of Europe's Human Rights Commissioner noted, spyware

[6] European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of the Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22 May 2023, 2022/2077(INI), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

[7] European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of the Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22 May 2023, 2022/2077(INI), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

[8] See for example, European Parliament, Report of the Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2022/2077(INI)), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

"creates a climate of self-censorship and fear where all individuals can be treated as suspects and where human rights defenders and active members of political life are particularly threatened."[9] It especially affects journalists because it endangers the confidentiality of sources and undermines the right to access to information. Other means of digital surveillance can also be used to silence dissent and punish independent reporting, and must be regulated through a clear and robust legal framework that provides strict conditions for its use, independent and effective monitoring and oversight mechanisms, and strong means of accountability and redress.

As this research shows in the case of Serbia, digital surveillance has become an integral tool of state repression, with human rights defenders and journalists suffering its devastating consequences. This report documents how the authorities in Serbia have deployed or used at least three different spyware systems, as well as other invasive digital forensics tools to covertly spy on protest organizers, journalists and civil society leaders. Widespread digital surveillance is a part of an increasingly repressive campaign by the government of Serbia designed to punish criticism and discourage civic participation.

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, as this research demonstrates, the deployment of advanced technologies, including spyware and other digital forensic tools that collect vast amounts of personal data, is not fully recognised or regulated by law, leaving too much space for potential abuse of such technologies for political purposes.

3.1 CIVIC SPACE IN SERBIA

Although vibrant, civil society in Serbia is facing an existential threat. For years, non-governmental organizations, think tanks and independent journalists have been operating in an environment which is increasingly hostile to any expression of dissent. As illustrated below, the use of invasive digital surveillance comes amid an intensifying smear campaign against activists and journalists, a growing number of arrests on spurious and baseless criminal charges, and persistent judicial harassment of citizens organizing peacefully and engaging in political dissent. In Serbia, any criticism of mainstream government policies or a challenge to the government's authority has been perceived as a threat that needs to be decisively countered and eliminated. The growing state-level oppression has made the operating environment for NGOs and independent journalists extremely challenging and had a chilling effect on the freedom of expression, association and peaceful assembly.[10]

Civil liberties and the civic space in Serbia have steadily declined since 2012, when the Serbian Progressive Party (Srpska Napredna Stranka or SNS) came to power.[11] Over the next few years, Civicus downgraded Serbia's civil space from "narrowed" to "obstructed", making Serbia one of the two lowest-ranking countries in the region.[12] Serbia's Freedom House ranking has also steadily declined over the years, with the country rated as "partly free" in 2024.[13] Freedom House cited the "pattern of retribution" and "openly retaliatory measures" against government critics as key contributing factors to an increasingly hostile environment for free expression and open debate.

Since 2017, the government has expanded its influence over both state-owned media and private outlets dependent on government subsidies. With pro-government outlets holding four out of five public broadcast frequencies, the government exercises tight control of and has a ubiquitous presence in the media space, enabling it to fully control the public narrative.[14] The lack of media pluralism has undermined the ability of civil society to effectively communicate and to counter disinformation or reach citizens through mainstream media. The credibility of civil society is further weakened by the persistent negative reporting about NGOs in

[9] Council of Europe's Human Rights Commissioner, "Highly intrusive spyware threatens the essence of human rights", 27 January 2023, https://www.coe.int/sr-RS/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights
[10] Freedom House, Freedom in the world 2024: Serbia, https://freedomhouse.org/country/serbia/freedom-world/2024 (accessed on 7 November 2024).
[11] Freedom House, Freedom in the world 2023: Serbia, https://freedomhouse.org/country/serbia/freedom-world/2023 (accessed on 7 November 2024).
[12] CIVICUS, Serbia, https://monitor.civicus.org/country/serbia/ (accessed on 7 November 2024).
[13] Freedom House, Freedom in the world 2024: Serbia, https://freedomhouse.org/country/serbia/freedom-world/2024 (accessed on 7 November 2024).
[14] Osservatorio Balcani Caucaso Transeuropa (OBCT) and Independent Journalists' Association of Serbia (IJAS), The rule of law and media freedom in Serbia: shadow report 2024, July 2024, https://en.nuns.rs/media/2024/07/Shadow-Report_-Rule-of-Law-and-Media-Freedom-in-Serbia-1.pdf

government-controlled media outlets, which is usually triggered by openly hostile and slanderous comments by senior public officials.[15]

The assault on civil society has significantly intensified during times of political crises and especially in the context of mass protests challenging the authority of the government. Each time the protests gain momentum, state repression against civil society – including intense smear campaigns in the media – dramatically escalate.

3.2 PROTESTS IN SERBIA 2021-2024

Protests in Serbia have become a frequent occurrence. As the persecution and harassment of activists, human rights defenders and journalists has intensified, the authorities have also gradually reduced space and opportunities for genuine consultation and dialogue with civil society on issues of public interest. In such a challenging context, citizens and NGOs have found that the only way to engage on important issues and have their voices heard is by taking to the streets.

Serbia has seen several major waves of protests over the past four years, many of which focused on the government's development policies and strategic infrastructure projects that were perceived by the protesters, and sometimes by the wider community, as exploitative and harmful for the local environment in the long-term.[16]

From September 2021 to February 2022, in a series of demonstrations across Serbia, protesters demanded the rejection of a lithium extraction mine investment by the Australian and British mining company Rio Tinto and the withdrawal of proposed changes to the Expropriation and Referendum Laws, which – the activists claimed – were connected with the deal.[17] The protests ended only after the proposed legal reforms were withdrawn and the government annulled contracts with Rio Tinto.[18]

In May 2023, a series of mass protests began in Belgrade and other locations in Serbia following two unrelated mass shootings that took place on two consecutive days – a school shooting in Belgrade and a separate shooting near Mladenovac and Smedrevo, in which 19 people in total, many of them children, lost their lives.[19] For months, the protests, named Serbia Against Violence, brought tens of thousands of people out to the streets demanding the resignations of senior officials, more effective oversight over media content and closure of media outlets blamed for promoting violence.

A new series of mass protests rocked Belgrade in December 2023, following the parliamentary and Belgrade City Assembly elections, the results of which were reported to be fraught with irregularities.[20] The organizers of the demonstrations which lasted two weeks asked for the annulment of the results and an independent inquiry into the elections process.[21]

In July and August 2024, tens of thousands of people gathered in towns across Serbia to protest against Serbia's agreement with the European Union and Germany on access to critical raw materials.[22] Within days after Serbia's constitutional court overturned the original cancellation of the project in 2022, the government reinstated the license for the Rio Tinto mining project to create Europe's largest lithium mine in Jadar

[15] Council of Europe Human Rights Commissioner, Report following her visit to Serbia from 13-17 March 2023, 6 September 2023, CommHR (2023)25, https://rm.coe.int/report-on-serbia-by-dunja-mijatovic-commissioner-for-human-rights-of-t/1680ac88cc
[16] Business & Human Rights Resource Centre, "Serbia: Activists block roads to protest possible lithium mine over concerns it will damage environment" , 3 January 2022, https://www.business-humanrights.org/en/latest-news/serbia-activists-block-roads-to-protest-possible-lithium-mine-that-might-damage-environment-environment-groups-warn/; BBC, "Thousands protest against lithium mining in Serbia", 11 August 2024, https://www.bbc.co.uk/news/articles/cged9qgwrvyo
[17] Guardian, "Rio Tinto lithium mine: thousands of protesters block roads across Serbia", 5 December 2021, https://www.theguardian.com/world/2021/dec/05/rio-tinto-lithium-mine-thousands-of-protesters-block-roads-across-serbia
[18] Reuters, "Serbia revokes Rio Tinto lithium project license amid protests", 20 January 2022, https://www.reuters.com/business/retail-consumer/serbian-government-revokes-rio-tintos-licences-lithium-project-2022-01-20/
[19] Guardian, "Thousands rally in Belgrade against government and culture of violence", 3 June 2023, https://www.theguardian.com/world/2023/jun/03/thousands-rally-in-belgrade-against-government-and-culture-of-violence
[20] Al Jazeera, "Thousands protest in Serbia alleging election fraud by governing party", 30 December 2023, https://www.aljazeera.com/news/2023/12/30/thousands-protest-in-serbia-alleging-election-fraud-by-ruling-party
[21] European Parliament, Situation in Serbia following the 2023 elections, 5 February 2024, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)757638
[22] Guardian, "Thousands take to the streets in Serbia to protest against proposed lithium mine", 22 August 2024, https://www.theguardian.com/world/video/2024/aug/22/thousands-take-to-streets-in-serbia-to-protest-against-proposed-lithium-mine-video-report; Reuters, "Serbian protestors rally to oppose Rio Tinto's lithium mine project", 16 October 2024, https://www.reuters.com/world/europe/serbian-protestors-rally-oppose-rio-tintos-lithium-mine-project-2024-10-16/

valley.[23] This triggered a new wave of mass protests across the country with communities arguing that the excavation would cause irreversible environmental damage.[24]

More recently, in November 2024, thousands of people took to the streets in Novi Sad and Belgrade in anger over the roof collapse at a Novi Sad railway station that killed 15 people earlier in the month. The protesters claimed that the alleged corruption and nepotism led to the sloppy renovations causing the deadly collapse and demanded official accountability for the tragedy.[25]

3.3 STIGMATIZATION AND SMEAR CAMPAIGNS THROUGH MEDIA

Senior public officials in Serbia frequently stigmatise civil society and independent journalists, demonizing critical NGOs labelling them as "traitors", "foreign agents" and "enemies of Serbia" and accusing them of attempting to violently overthrow the government.[26]

In August 2024, a widely watched pro-government outlet, Informer TV, featured an extensive report on the alleged "special war against Serbia" waged by some 40 "foreign-funded NGOs." The show, which aired on several subsequent days, named individual organizations, their employees, and activists along with their salaries and activity budgets, describing them as foreign mercenaries working against the state and alleging their involvement in money laundering.[27] According to a local NGO, Civic Initiatives, the data presented by Informer TV included financial and other information that is not publicly available and could not have been obtained lawfully.[28] Most senior public officials, including the President, hinted about the forthcoming Informer TV "revelations" days before the broadcast lending further credence to the apparent links between the media and authorities.[29] The defamatory statements about the NGOs using foreign donations to fund protests were further fuelled by the Governor of the National Bank as well as numerous members of parliament.[30]

This was not the first time that the details of financial activities of individual NGOs were disclosed and debated in public. In 2020, Serbia's Administration for the Prevention of Money Laundering asked commercial banks to provide data on financial transactions of close to 60 media outlets, journalists, civil society organizations and activists on the grounds of alleged involvement in money laundering and financing of terrorism.[31] The organizations and individuals included: those investigating and reporting on human rights, rule of law, and war crimes; think tanks dealing with security and foreign policy; and media associations conducting investigative journalism. At the time, the Financial Action Task Force (FATF) determined that

[23] Intellinews, "Backlash after Serbia's constitutional court overturns ban on Rio Tinto lithium mine", 15 July 2024, https://www.intellinews.com/backlash-after-serbia-s-constitutional-court-overturns-ban-on-rio-tinto-lithium-mine-333889/

[24] Rio Tinto maintained that it would operate the mine safely and comply with the highest environmental standards. See Radio Free Europe/Radio Liberty, "Rio Tinto CEO Says 'Well-Organized' Disinformation Targeting Serbian Lithium Project", 15 September 2024, https://www.rferl.org/a/serbia-lithium-tinto-stausholm-mine/33120768.html; Balkan Insight, "European Union agrees controversial lithium mine project with Serbia", 19 July 2024, https://balkaninsight.com/2024/07/19/european-union-agrees-controversial-lithium-mining-project-with-serbia/

[25] Al Jazeera, "Police fire tear gas at Serbians protesting deadly station roof collapse", 6 November 2024, https://www.aljazeera.com/news/2024/11/6/police-fire-tear-gas-at-serbians-protesting-deadly-station-roof-collapse; Time, "Serbian Protesters Blame Government for Deadly Train Station Roof Collapse", 12 November 2024, https://time.com/7175231/serbia-protests-anti-government-corruption-train-station-roof-collapse-deaths/

[26] Al Jazeera, "Protesti i blokade u Srbiji: Masovna tuča u Novom Sadu" ["Protests and blockades in Serbia: Mass brawl in Novi Sad"], 4 December 2021, https://balkans.aljazeera.net/news/balkan/2021/12/4/srbiju-danas-ocekuju-masovni-ekoloski-protesti-i-blokade-puteva (in Serbian).

[27] Informer, "Specijalni program - ko i kako finasira uništavanje srbije! Haos u studiju informera! Uključio se Gavrilović i priznao: Ja sam strani plaćenik, vaša televizija da se ukine" ["Special programme – who finances the destruction of Serbia and how! Chaos in the informer's studio! Gavrilović admitted: I am a foreign mercenary, your television programme should be canceled"], 21 August 2024, https://informer.rs/vesti/politika/936361/finansiranje-rusenja-srbije (in Serbian).

[28] Civic Initatives report, https://www.gradjanske.org/zaustaviti-represiju-nad-gradjanima-i-govor-mrznje-protiv-aktivista/

[29] NIN, "Vučić optužio NVO da su dobile "desetine i stotine miliona evra" da ga ruše" ["Vučić accused NGOs of receiving "tens and hundreds of millions of euros" to destroy him"], 17 August 2024, https://www.nin.rs/politika/vesti/55262/vucic-optuzio-nvo-da-su-dobile-desetine-i-stotine-miliona-evra-da-ga-ruse (in Serbian).

[30] NIN, "Vučić optužio NVO da su dobile 'desetine i stotine miliona evra' da ga ruše" ["Vučić accused NGOs of receiving "tens and hundreds of millions of euros" to destroy him"] (previously cited); Informer, "Strane agenture finansirale proteste! Guvernerka: Milioni evra se pumpaju u Srbijusa ciljem nasilnog rušenja vlasti" ["The U.S. government has funded the protests. Governor: Millions of euros are being pumped into Serbia with the aim of violently overthrowing the government!"], 19 August 2024, https://informer.rs/vesti/politika/935677/ekonomija-protesti-opozicija-litijum-jadar (in Serbian).

[31] Radio Free Europe/Radio Liberty, "EU, SAD i Amnesty traže detalje o proveri finansija novinara i NVO u Srbiji" [https://www.slobodnaevropa.org/a/uprava-finansije-nvo-mediji/30755081.html EU, SAD i Amnesty traže detalje o proveri finansija novinara i NVO u Srbiji" ["The EU, the USA and Amnesty are asking for details on checking the finances of journalists and NGOs in Serbia"], 29 July 2020, https://www.slobodnaevropa.org/a/uprava-finansije-nvo-mediji/30755081.html (in Serbian).

such control would be baseless and said that FATF measures should not be "exploited and used to oppress human rights under the pretext of counter-terrorism."[32] Three UN Special Rapporteurs issued a joint statement criticising Serbia for misusing the anti-money laundering and anti-terrorist financing mechanism to "intimidate civil society actors and human rights defenders, restricting their work and muffling any criticism of the government."[33]

The anti-NGO rhetoric and the misrepresentation of seemingly authoritative and credible data about their purported treasonous activities undermine citizens' confidence in civil society and profoundly endanger individual organizations and their staff. Together with media campaigns focusing on the alleged Western-funded plot to overthrow the government, they seemed intended to create an environment to legitimize the adoption of a Russian-style "Foreign Agents Law". Senior government officials, including the current Deputy Prime Minister and former Security Information Agency (BIA) Director Aleksandar Vulin, and his political party called for such a law in April/May 2024,[34] and formally submitted it into parliamentary procedure in November 2024.[35]

It is not only the non-governmental organizations that face huge pressure and targeted smear campaigns. By November 2024, the Independent Association of Journalists of Serbia (NUNS) reported 151 incidents, including 65 verbal threats, 15 physical assaults, and 66 cases of undue pressure on journalists.[36] A recent poll indicated that nearly 30% of journalists have been the target of a smear campaign, and every third journalist experienced threats over their reporting in 2023, with journalists reporting on organized crime and corruption being at greater risk.[37]

Journalists reporting critically about these events are also routinely labelled as traitors leading a "hybrid war against Serbia",[38] foreign mercenaries, and enemies of the state by senior government officials and pro-government media outlets, often leading to harassment, online abuse and even physical attacks against journalists by non-state actors.[39] Independent journalists and outlets face other forms of pressure, including being prevented from accessing media events and denied information or responses by public institutions.[40] Over the past several years, there has also been a notable increase in strategic lawsuits against public participation (SLAPPs) against journalists, the vast majority of which were filed by public officials and private companies associated with the government.[41] As of November 2024, Crime and Corruption Reporting Network, KRIK, alone faced 16 separate cases of vexatious lawsuits over their investigative reporting.[42] The Independent Journalists Association of Serbia labelled this as a "lawfare campaign by which government

---

[32] Dr. Marcus Pleyer, FATF President, letter to Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; Special Rapporteur on the rights to freedom of peaceful assembly and of association and Special Rapporteur on the situation of human rights defenders, pursuant to Human Rights Council resolutions 40/16, 41/12 and 43/16, 18 December 2020, https://fatfplatform.org/assets/2020-12-18-FATF-re-UN-APML-Serb.pdf. See also Raskrikavanje, "FATF: Neosnovano češljanje računa organizacija i novinara" ["FATF: Unfounded combing of the accounts of organisations and journalists"], 26 January 2021, https://www.raskrikavanje.rs/page.php?id=FATF-Neosnovano-cesljanje-racuna-organizacija-i-novinara-771 (in Serbian).

[33] Office of the UN High Commissioner for Human Rights (OHCHR), "Serbia's anti-terrorism laws being misused to target and curb work of NGOs, UN human rights experts warn", 11 November 2020, https://www.ohchr.org/en/press-releases/2020/11/serbias-anti-terrorism-laws-being-misused-target-and-curb-work-ngos-un-human?LangID=E&NewsID=26492

[34] Istinomer, "Dobro jutro uz ruski zakon: Ko u Srbiji smatra NVO „stranim agentima" ["Good morning with the Russian law: Who in Serbia considers NGOs "foreign agents"?"], 12 May 2024, https://www.istinomer.rs/analize/dobro-jutro-uz-ruski-zakon-ko-u-srbiji-smatra-nvo-stranim-agentima/ (in Serbian).

[35] Radio Free Europe/Radio Liberty, "Vulinova stranka u Skupštini Srbije predložila zakon o stranim agentima" ["Vulin's party proposed a law on foreign agents in the Serbian Parliament"], 4 September 2024, https://www.slobodnaevropa.org/a/srbija-vulin-strani-agenti/33220976.html (in Serbian).

[36] Figures provided by the Independent Association of Journalists of Serbia, email correspondence with Amnesty International, 13 December 2024

[37] Council of Europe, Journalists' Association of Serbia, the Independent Journalists' Association of Serbia, "Safety of Journalists, Behind the headlines: Threats, attacks and pressure on journalists in Serbia", March 2024, https://rm.coe.int/hf42-research-threats-attacks-onjournalists/1680aee322

[38] N1, "Vučić nacrtao napade na sebe – državu: Optužio strane službe, medije i NVO" ["Vučić drew attacks on himself – state: accused foreign agencies, media and civil society"], 5 February 2024, https://n1info.rs/vesti/vucic-nacrtao-napade-na-njega-drzavu-optuzio-strane-sluzbe-medije-i-nvo/ (in Serbian).

[39] See OHCHR, "Serbia: UN expert alarmed by rise in hateful rhetoric after mass shootings", 5 June 2023, https://www.ohchr.org/en/press-releases/2023/06/serbia-un-expert-alarmed-rise-hateful-rhetoric-after-mass-shootings

[40] N1, "Predsednica SO Knić iz SNS, zamenica iz SPS – ekipi N1 bilo zabranjeno prisustvo na sednici" ["President of SO Knić from SNS, deputy from SPS – N1 team prevented from attending the session"], 2 February 2024, https://n1info.rs/vesti/ekipi-n1-zabranjeno-prisustvo-na-prekinutoj-konstitutivnoj-sednici-so-knic/ (in Serbian); N1, "Šapić odbija da odgovara na pitanja N1: Prekinuo sam svaku komunikaciju s vama, prosto niste dorasli" ["Šapić refuses to respond to N1 questions: I quit all communication with you; You are not up to standards"], 27 January 2024, https://n1info.rs/vesti/sapic-odbija-da-odgovara-na-pitanja-n1-prekinuo-sam-svaku-komunikaciju-s-vama-i-nemam-nameru-da-je-nastavljam/ (in Serbian).

[41] European Commission, Serbia 2023 Report, 8 November 2023, https://neighbourhood-enlargement.ec.europa.eu/document/download/9198cd1a-c8c9-4973-90ac-b6ba6bd72b53_en?filename=SWD_2023_695_Serbia.pdf

[42] SafeJournalists Network, "Coalition for Media Freedom: KRIK's Verdict is Unfair, Urgent Adoption of Anti-SLAPP Recommendations is Necessary", 10 June 2024, https://safejournalists.net/coalition-for-media-freedom-kriks-verdict-is-unfair-urgent-adoption-of-anti-slapp-recommendations-is-necessary/. Also see: https://javniservis.net/wp-content/uploads/2024/11/KRIK-SLAPP-cases-update-November-2024.pdf

officials, organized crime, and others are weaponizing legislation to silence investigative and critical voices."[43]

The recurring pattern of publicly naming, smearing, and discrediting investigative or independent journalists by public officials, including members of the government, makes the journalists direct targets for online hate speech and harassment and foments distrust in and hostility towards independent media. The Council of Europe Commissioner for Human Rights warned that the "repeated smear campaigns have encouraged and legitimized intimidation of journalists."[44] In its resolution on the situation in Serbia, the European Parliament also condemned "the attacks instigated by media outlets close to the government against critical journalists," and expressed concern about cases of abusive language and harassment against journalists, human rights defenders, and civil society organizations coming from government officials.[45] In March 2024, the UN Human Rights Committee noted concern about "the continued prevalence of hate speech in public discourse, both online and traditional media, including by politicians and high-level officials, in particular towards journalists."[46]

3.4 PERSISTANT HARASSMENT AND INTIMIDATION OF CIVIL SOCIETY AND JOURNALISTS

UNLAWFUL OR EXCESSIVE FORCE AGAINST PROTESTERS

Over the years, Serbian authorities have faced significant criticism for heavily policing protests, including by subjecting participants to often unlawful or excessive use of force, fines, intimidation, and judicial harassment.[47] On numerous occasions in 2022 and 2023, Serbian police used riot gear to disperse largely peaceful environmental assemblies and break local community sit-ins organized across Serbia.[48] In December 2023, police used excessive and indiscriminate force, including tear gas and pepper spray, against the people demonstrating in criticism of the reported irregularities associated with the elections.[49] Several media workers covering the demonstrations were attacked and beaten, including by police officers.[50] The authorities have also routinely contracted private security companies, sometimes in plain clothes and without visible insignia, to "police" protests, often using unlawful force with impunity.[51]

BASELESS CHARGES AND FINES

Between 2020 and 2023, hundreds of activists and protesters received misdemeanour and criminal charges for alleged involvement in violent behaviour, and public peace and order disturbances.[52] There were also numerous cases of police issuing heavy fines to citizens who simply shared invitations to protests or publicised their views on their social media. Many of these were spontaneous protests; yet the police designated these individuals as "organizers" and prosecuted them for failure to comply with the obligation to

---

[43] Independent Journalists' Association of Serbia (IJAS) and OBC Transeuropa (OBCT), *The rule of law and media freedom in Serbia: Shadow report* 2024, July 2024, https://en.nuns.rs/media/2024/07/Shadow-Report_-Rule-of-Law-and-Media-Freedom-in-Serbia-1.pdf
[44] Council of Europe Human Rights Commissioner, *Report following her visit to Serbia from 13-17 March 2023*, 6 September 2023, CommHR (2023)25, https://rm.coe.int/report-on-serbia-by-dunja-mijatovic-commissioner-for-human-rights-of-t/1680ac88cc
[45] European Parliament resolution of 8 February 2024 on the situation in Serbia following the elections (2024/2521(RSP)), paras. 19 and 20, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0075_EN.html
[46] Human Rights Committee, Concluding observations on the fourth periodic report of Serbia, 28 March 2024, CCPR/C/SRB/CO/4, para. 14.
[47] Amnesty International, *Serbia: Submission for European Union Enlargement Package/Opinion, 2023* (Index: EUR 70/6688/2023), 17 April 2023, https://www.amnesty.org/en/documents/eur70/6688/2023/en/
[48] Amnesty International, *Serbia: Submission for European Union Enlargement Package/Opinion, 2023* (previously cited).
[49] Nova, "Potresne scene ispred gradske skupštine: Policajci vuku mladića, njegova majka pokušava da ga spase" ["Disturbing scenes in front of the Assembly: Policemen drags the young man, while his mother is trying to save him"], 25 December 2023, https://nova.rs/vesti/politika/potresne-scene-ispred-gradske-skupstine-policajci-vuku-mladica-njegova-majka-pokusava-da-ga-spasi/ (in Serbian). See also European Western Balkans, "EP adopted resolution on Serbia, calling for an investigation into December elections", 8 February 2024, https://europeanwesternbalkans.com/2024/02/08/ep-adopted-resolution-on-serbia-calling-for-an-investigation-into-december-elections/
[50] Gradjanske inicijative, Platform Three Freedoms, *Zaustaviti policijsku brutalnost nad građanima/kama [Stop Police brutality against citizens],* 25 December 2023, https://www.gradjanske.org/zaustaviti-policijsku-brutalnost-nad-gradjanima-kama/ (in Serbian).
[51] Amnesty International, *Serbia: Submission for European Union Enlargement Package/Opinion, 2023* (previously cited).
[52] Significant number of misdemeanour offenses and fines were issued between 2020-2023 for the violations of the Article 21, Paragraph 1, Item 1, which envisages a fine for the failure to notify an upcoming public assembly to competent authorities. According to statistics collected by the Belgrade Centre for Human Rights, the vast majority (131 out of 183) of minor offence cases before courts in 2022 pertained to charges under Article 22 and many specifically to the failure to notify the responsible authority. See Beogradski centar za ljudska prava, *Stanje ljudskih prava u Srbiji 2022 [Human rights in Serbia 2022]*, 2023, https://www.bgcentar.org.rs/wp-content/uploads/2023/03/Ljudska-prava-u-Srbiji-2022-web-2.pdf, p. 157 (in Serbian) and Yucom, *Report on the attacks on human rights defenders in Serbia for 2022*, https://en.yucom.org.rs/wp-content/uploads/2022/12/Izvestaj-o-napadima-ENG-2022-V2.pdf

notify the assembly.[53] Local organizations have partnered with lawyers to provide legal aid or representation to more than 340 people in such situations over the past several years.[54]

More recently, however, during the protests following the elections in December 2023 and the anti-lithium demonstrations in August 2024, activists who were arrested or called for questioning faced more serious charges of "inciting the violent overthrow of the constitutional order," a criminal offence carrying a penalty of up to eight years of imprisonment.[55]

According to the activists and lawyers who spoke with Amnesty International and based on the court orders for home searches shared with and reviewed by the organization, the police frequently cited activists' posts on social media, their speeches or even their mere participation in the protests as elements for such serious criminal charges.[56] 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.[57] Amnesty International interviewed nine activists who were questioned in relation to the criminal charge of "inciting the violent overthrow of the constitutional order" and whose telephones and other electronic devices were temporarily seized by the police. Not one of them has been formally charged at the time of this report's publication.

ARBITRARY DETENTION AND SEARCHES AT BORDER CROSSINGS

Some civil society representatives faced repeated visits from the police at their homes and were held at border crossings as they attempted to travel. Sofija Todorović, the director of the Youth Initiative for Human Rights, was held at the airport in Belgrade, both upon departure and arrival, ten times between July and September 2024 without an explanation or any formal documents.[58] An activist of the New Social Initiative from northern Kosovo, Jovana Radosavljević, was held several times at the administrative boundary between Serbia and Kosovo,[59] and Milica Randjelović, an opposition politician and an activist, missed her summer holidays after border police stopped her at Belgrade airport over suspicion of involvement in the "violent overthrow of the constitutional order."[60]

In most of these cases, the activists were not told why and at whose orders they were held at border crossings, nor were they shown any official documents. They were denied access to a lawyer and, following extensive questioning, being searched and several hours in custody, released without charge.

Throughout the summer of 2024, several foreign nationals, including artists, singers and film directors popular in the region who are often critical of the Serbian government, or its role in the wars in former Yugoslavia, were held and questioned on Serbia's borders and eventually denied entry. In August, after a very high-profile case involving Croatian singer Severina Vučković who faced intrusive questioning when attempting to enter Serbia, Serbia's Vice President and former BIA Director Aleksandar Vulin told the media

---

[53] Yucom, *Report on the Attacks on Human Rights Defenders in Serbia for 2022* (previously cited).

[54] In one case, a decision issued by the Misdemeanor Appellate Court on 17 May 2022 concluded that announcing or promoting a protest via social media networks is insufficient for someone to be considered an organizer and that, instead, three conditions must be fulfilled cumulatively: inviting, preparing and organising the assembly. Other acquittals followed, especially in cases where the police filed requests to initiate misdemeanour proceedings against citizens simply because they had shared social media posts calling for a protest; an act which is not listed as a misdemeanour. See N1, "NVO: Prva pravosnažna presuda kojom je oslobođen učesnik protesta" ["NGO: The first final judgement acquitting a protest participant"], 20 June 2022, https://n1info.rs/vesti/nvo-pozdravile-oslobadjajucu-presudu-organizatoru-proslogodisnjih-protesta/ (in Serbian) and Yucom, "Pozdravljamo prvu pravnosnažnu presudu kojom je oslobođen Srđan Vukša, aktivista optužen za kršenje Zakona o javnom okupljanju, povodom organizovanja prošlogodišnjih protesta u Srbiji" ["We welcome the first legally binding verdict acquitting Srđan Vukša, an activist accused of violating the Law on Public Assembly, in connection with the organization of last year's protests in Serbia"], 20 June 2022, https://yucom.org.rs/pobeda-solidarnosti-i-prava-na-slobodu-okupljanja-nad-institucionalnom-odmazdom/ (in Serbian).

[55] In December 2023, when at least 38 people were arrested, several students, who were among them, were charged with this serious offence. Some remained under house arrest for several months, while others continued to fight the charges through the courts. The specific charge involved the offense of "endangering the constitutional order or security of Serbia, calling or inciting change of its constitutional order by force, overthrowing the highest state authorities or representatives of those authorities" [Article 309 of the Criminal Code and Article 320 preparation of an act against the constitutional order and security of Serbia.]

[56] Amnesty International conversation with activists and lawyers representing the arrested individuals conducted via telephone between August and November 2024.

[57] Civic Initiatives, *Weaponizing Influence: How Russia's and China's Soft Power Clashes Serbia's Civil Society using Lithium Controversies*, August 2024, https://www.gradjanske.org/wp-content/uploads/2024/08/Weaponizing-Influence-Report-Civic-Initiatives.pdf

[58] Danas, "Ko je Sofija Todorović, aktivistkinja koja je od jula zadržana na graničnim prelazima čak devet puta?" ["Who is Sofija Todorović, the activist who has been detained at border crossings nine times since July?"], 6 September 2024, https://www.danas.rs/vesti/drustvo/ko-je-sofija-todorovic/ (in Serbian).

[59] Novosti, "Kome je Srbija zabranjena" ["To whom Serbia is forbidden"], 5 September 2024, https://www.portalnovosti.com/kome-je-srbija-zabranjena (in Croatian); Insajder, "Zvaničnici saopštavaju da su spiskovi nepoželjnih ukinuti, pitanje odgovornosti za samovoljno postupanje institucije i dalje ne pokreću" ["Officials announce that the lists of undesirables have been abolished, they still do not raise the issue of accountability for the institution's arbitrary actions"], 9 September 2024, https://insajder.net/teme/zvanicnici-saopstavaju-da-su-spiskovi-nepozeljnih-ukinuti-pitanje-odgovornosti-za-samovoljno-postupanje-institucije-i-dalje-ne-pokrecu (in Serbian).

[60] Radio Free Europe/Radio Liberty, "'Tuga i bes' aktivista zbog policijskog saslušavanja nakon protesta zbog litijuma u Srbiji" ["'Sadness and anger' of activists over police questioning after lithium protests in Serbia"], 19 August 2024, https://www.slobodnaevropa.org/a/srbija-sasluanje-aktivisti-protesti-protiv-litijuma/33084587.html (in Serbian).

that he had, indeed, created lists of persons who were unwanted in Serbia because of their public statements.[61] Although Vulin denied that such lists existed for the Serbian citizens, local NGOs and commentators suspected that the lists of people guilty of the so-called "verbal crimes" were behind the incidents of local activists facing similar treatment on the borders.[62]

In a joint statement, a group of 13 lawyers in Serbia condemned the "campaign of baseless" arrests and detention of many activists based on their public statements or mere participation in the protests, calling it a "harsh abuse of state's repressive apparatus" against citizens who are legitimately exercising their rights.[63] Indeed, legal experts agree that the charges of "incitement to violent overthrow of the constitutional order" are vague, difficult to prove and clearly aimed at persecuting and silencing those who speak up.[64]

In August, the Belgrade-based National Convention on the European Union, a network of 850 NGOs, addressed the President of the National Assembly and the Prime Minister and condemned "unjustified and baseless detentions" of their members.[65] It further noted that that these actions created "an atmosphere of fear and insecurity that severely hinders, if not entirely prevents" the continued work of civil society and are contrary to international law and international human rights obligations of Serbia.[66]

ARBITRARY SEIZURE OF TELEPHONES AND COMPUTERS

Amnesty International accounted for or interviewed at least nine activists and journalists who were detained or questioned between July and November 2024 and whose telephones or computers were temporarily seized and searched by the police. In some cases, the police called the activists for informational interviews in relation to charges of "incitement to the violent overthrow of the constitutional order," while in others, they seized the telephone devices during searches of their apartments, which were authorised by court. Activists in Serbia suspect that the authorities have been using serious and baseless criminal charges to justify the highly intrusive procedures, including the seizure, searches, and extraction of digital data from activists' mobile devices and computers to learn more about their social networks and future plans.

In August, police searched the apartment belonging to Zorana Crnojević, an activist from the town of Vršac, and confiscated her telephone in the context of an investigation relating to the charges of "incitement to violent overthrow of the constitutional order." Although, at the time of writing, Zorana was not formally charged, her telephone remains with the police undergoing forensic investigations.[67] Zorana, who is an administrator of several social media groups, including one with over 100,000 followers, was five months pregnant at the time and had not been a part of the ongoing protests. Predrag Žunić, an administrator of the Facebook group Aktivizam, which has over 20,000 followers, was also called for questioning and had his telephone and computer seized in August. His device also remains with the police.[68]

According to interviews with activists and lawyers representing them, the telephones belonging to the activists were put through an inspection, then an extensive digital forensic search and analysis of the extracted data from the devices to allegedly enable the prosecutors to decide whether to press charges against the individuals.[69] No criminal charges were formally filed against any of the activists at the time of the publication of this report.

---

[61] Al Jazeera, "Vulin: Postoji popis ljudi koji su zbog verbalnog delikta nepoželjni u Srbiji" ["Vulin: There is a list of people who are undesirable in Serbia because of a verbal offense"], 27 August 2024, https://balkans.aljazeera.net/news/balkan/2024/8/27/vulin-postoji-popis-ljudi-koji-su-zbog-verbalnog-delikta-nepozeljni-u-srbiji (in Serbian).
[62] Radar, "Granični poremećaj" ["Borderline disorder"], 7 September 2024, https://radar.nova.rs/politika/spiskovi-verbalni-delikt-bia-policija/ (in Serbian).
[63] Nova, "Zajedničko saopštenje 13 advokata: Privođenje građana zbog protesta je zloupotreba policije" ["Joint statement of 13 lawyers: Arresting citizens for protesting is an abuse of the police"], 21 August 2024, https://nova.rs/vesti/drustvo/zajednicko-saopstenje-13-advokata-privodjenje-gradjana-zbog-protesta-je-zloupotreba-policije/ (in Serbian).
[64] Istinomer, "Optužbe za "rušenje ustavnog poretka" – sve češće, olako izrečene, teško dokazive?" ["Accusations of "overturning the constitutional order" - increasingly frequent, easily stated, difficult to prove?"], 20 September 2024, https://www.istinomer.rs/analize/analize-analize/optuzbe-za-rusenje-ustavnog-poretka-sve-cesce/ (in Serbian).
[65] National Convention on the European Union, letter to the President of the National Assembly of the Republic of Serbia, Mrs. Ana Brnabić, and to the Prime Minister of the Republic of Serbia, Mr. Miloš Vučević, 27 August 2024, https://eukonvent.org/otvoreno-pismo-nkeu-predsednici-nsrs-i-predsedniku-vlade-rs/
[66] National Convention on the European Union, letter to the President of the National Assembly of the Republic of Serbia, Mrs. Ana Brnabić, and to the Prime Minister of the Republic of Serbia, Mr. Miloš Vučević (previously cited).
[67] Amnesty International conversation with Zorana Crnojević's lawyer, 12 December 2024.
[68] Amnesty International conversation with Predrag Žunić's lawyer, 12 December 2024.
[69] Interview with Sarah El-Sarag, lawyer, xx September 2024.

4. SPYWARE TARGETING HRDS AND JOURNALISTS IN SERBIA

The Serbian Security Information Agency (BIA), the national security and intelligence agency of Serbia, has been publicly linked to the procurement of highly invasive spyware tools since at least 2014. Until recently, however, there has been little direct evidence to show how state agencies may be using or abusing such technologies in practice.

This chapter documents how at least three different spyware systems, including Pegasus, Predator and a locally developed Android spyware system, have been deployed or used in Serbia in recent years, including to covertly spy on protest organizers, journalists and civil society leaders. The use of spyware against civil society in Serbia was first forensically confirmed in 2023,[70] and this chapter expands significantly the evidence on how such tools are used and deployed. This research has identified at least seven cases where signs of spyware targeting, or infection were confirmed against civil society members.

This research reveals for the first time how Serbian authorities have developed or acquired an Android spyware system - which for the sake of clarity we will refer to as NoviSpy from hereon - to systematically and covertly infect mobile devices during arrest, detention, or in some cases, informational interviews with civil society members. In multiple cases, the arrests or detentions appear to have been orchestrated to enable covert access to an individual's device to enable data extraction or device infection.

As described in Section 7, the lack of an adequate legal framework controlling the use of spyware, or meaningful mechanism for independent oversight in Serbia raises concerns that such spyware and surveillance products can be used in ways that are incompatible with human rights standards, especially in the context of a widespread intimidation and pressure on activists and civil society organizations. The use of spyware as such is not explicitly regulated by the laws in Serbia. However, the relatively widespread use of these technologies to hack phones and other electronic devices indicates that the authorities in Serbia consider spyware as a legitimate means of secret communications surveillance - not just to be used against criminal suspects, but also against activists, opposition politicians and journalists.

Serbia is not alone in Europe in failing to have in place an adequate legal framework to control the use of spyware. Indeed, previous research by Amnesty International, media investigations, and a recent European Parliament's Committee of Inquiry on spyware (known as PEGA Committee) report found, this has been the case in several EU Member States, where law-enforcement and security agencies have purchased and used highly invasive spyware, such as Pegasus and Predator, for law-enforcement and security purposes.[71] The report also found that some governments misused the spyware for purely political purposes, i.e., to target

[70] Amnesty International, "Serbia: Civil society threatened by spyware", https://securitylab.amnesty.org/latest/2023/11/serbia-civil-society-threatened-by-spyware/

[71] European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of the Union law in relation the use of Pegasus and equivalent surveillance spyware, 22 May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

critics and opponents of the parties in power and used the information gathering through these activities to monitor, blackmail, intimidate, and harass the people targeted.[72]

4.1 PREVIOUS REPORTS OF SERBIAN SPYWARE PROCUREMENT

The evidence presented in this report on the use of different spyware systems to target Serbian civil society does not mark the first time Serbian authorities have been linked to the procurement or use of spyware systems. A 2015 leak of internal emails from now-defunct Italian spyware vendor Hacking Team revealed a series of emails exchanges between BIA officials and the Hacking Team to arrange a demo of Hacking Team's Android spyware product.[73] It is unclear if a contract with BIA was completed; however, evidence shows that the Hacking Team performed a demo of their products in Belgrade in 2012.[74]

----- Messaggio originale -----
Da: [redacted] [mailto:[redacted]@bia.gov.rs]
Inviato: Tuesday, April 10, 2012 01:36 PM
A: [redacted]
Oggetto: Info RCS - again

Dear [redacted],

Earlier this year you made a presentation of Remote Control System in Belgrade.

I would like to inform you that we are interested in see the system again, but only RCS for mobile device.
Please tell me whether it is possible presentation in Belgrade and when.

Thanks in advance.

[redacted]

Figure 1: Screenshot of email exchange between BIA and Hacking Team

A 2015 report by Citizen Lab identified Serbia as being among suspected customers of the FinFisher FinSpy spyware, produced by the Germany-based company FinFisher GmbH.[75] The report relied on internet scanning techniques to map the location of FinFisher backend customer systems in 32 countries around the world. In the case of Serbia, Citizen Lab went further and specifically attributed the FinFisher system to BIA. The Finfisher spyware server was hosted on the same /26 IP address range (195.178.51.xxx) as BIA's public website and email server.[76]

Amnesty International reviewed the technical records published by Citizen Lab and can confirm that the IP range identified by Citizen Lab (195.178.51.xxx) remains associated with the BIA at the time of publication of this report. The public website of BIA at bia.gov.rs is currently hosted at 195.178.51.195.

4.2 PREDATOR SPYWARE DEPLOYED IN SERBIA

Predator is a form of highly invasive spyware developed and sold by Intellexa, a consortium of surveillance and spyware vendors based in Cyprus, Greece, Hungary and North Macedonia, among others. The Predator spyware is designed to allow Intellexa's government customer to target and infect Android and iPhones typically using 1-click infection links sent over SMS or messaging apps (see Glossary). If successfully installed, the Predator spyware has the technical capability to access unlimited amounts of data on the device and the spyware's actions on the device cannot be independently audited.

As part of the October 2023 *Predator Files* collaborative investigation, Amnesty International revealed the use of Predator to target activists, journalists, academics and political figures world-wide.[77] Predator spyware was

[72] European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of the Union law in relation the use of Pegasus and equivalent surveillance spyware, 22 May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html
[73] Share Lab, "Hacking Team: The "Italian job" of Serbian security services", 14 July 2015, https://labs.rs/en/hacking-team-the-italian-job-of-serbian-security-services/
[74] Email correspondence on file with WikiLeaks, 16 April 2012, https://wikileaks.org/hackingteam/emails/emailid/568788
[75] Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, 15 October 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/
[76] Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation* (previously cited).
[77] Amnesty International Security Lab, Case study: The Predator Files, https://securitylab.amnesty.org/case-study-the-predator-files/ (accessed on 20 November 2024).

also linked to the hacking of journalists, opposition, and numerous public figures in Greece, triggering what has become known as #PredatorGate.[78]

In mid-2021, Amnesty International's Security Lab identified multiple Predator 1-click infection domains imitating popular Serbian news websites. Spyware domains that closely mimic legitimate websites are frequently used in spyware attacks to trick a target into clicking on an attack link which appears to be a real website. In this case, the fact that Amnesty International identified several domains that are designed to closely imitate legitimate Serbian news websites suggests that there was a Predator customer that specifically wanted to target individuals in Serbia. A sample of the identified Serbian related Predator domains are listed in Table 1.

Predator Domain	Legitimate Website	Registration Date
danas[.]bid	danas.rs	2020-05-23
novosti[.]bid	novosti.rs	2020-05-23
politika[.]bid	politika.rs	2020-05-22

Table 1: Predator spyware domains imitating Serbian news website

Additionally, Amnesty International identified two IP addresses hosted in Serbia which had the same configuration and fingerprint as other Predator backend customer servers during 2020 and 2021. Both IP addresses were located on the Telekom Srbija network in the same /24 IP range 93.86.50.0/24.

Telekom Srbija is a Serbian state-owned telecommunications operator. A number of the identified Serbian-themed Predator domains were at times also hosted on these Telekom Srbija IP addresses 93.86.50.174 and 93.86.50.218 (see Annex 5). This suggests that this Predator customer was not only targeting people in Serbia, but that the Predator customer was also operating the spyware system from Serbia.

Amnesty International does not have evidence to attribute the use of the Predator spyware to a particular government customer in Serbia: however, the identification of Serbian-themed Predator domains and the presence of multiple Predator servers physically located in Serbia, suggest that this Predator attack infrastructure is tied to a Serbian government customer of Intellexa. The presence of Predator servers on the Telekom Srbija network helps rule out the alternative hypothesis that these Predator domains are tied to a non-Serbian Predator customer with an interest in targeting Serbian users.

The Serbian Predator customer was active from early 2020 until at least December 2021. Amnesty International has not identified any specific cases where the Predator spyware was used to target Serbian civil society. However, such spyware systems are intended to be difficult to detect both by the targets and by researchers working to document abuses.

The evidence of Predator infrastructure associated with a Serbian customer presented here is consistent with the findings of an independent 2021 investigation into Predator by Citizen Lab, which also identified Serbia to be a likely customer for the Predator spyware.[79] The initial Predator infrastructure associated with Serbia was shut down in December 2021 following the public exposure of the Predator spyware by Citizen Lab.

Intellexa did not respond to the report findings, the details of which were shared with the company ahead of the publication.

4.3 PEGASUS SPYWARE TARGETING CIVIL SOCIETY IN SERBIA

Pegasus spyware, developed by Israeli company NSO Group, has been linked to the unlawful surveillance of numerous journalists, human rights defenders and opposition activists worldwide. In July 2021, Amnesty International, in partnership with Forbidden Stories and media partners, revealed the scope of global harms

[78] Amnesty International, "Greece's surveillance scandal must shake us out of complacency", 26 January 2023, https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/
[79] Citizen Lab, *Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, 16 December 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

from the spyware in the Pegasus Project.[80] The collaborative research showed that the Pegasus spyware was used to facilitate human rights violations on a massive scale, with around 50,000 phone numbers, including those of human rights defenders, journalists, academics, and opposition politicians, identified as potential surveillance targets.

Amnesty International has continued to track the activity and proliferation of Pegasus spyware. This section summarises the evidence, including technical evidence from digital forensics carried out on activists' devices and further mapping of Pegasus infrastructure and OSINT investigations, that indicate that Pegasus spyware is being used to target civil society in Serbia.

4.3.1 TWO SERBIAN THINK-TANK ACTIVISTS TARGETED BY PEGASUS (CASE 1)

In October 2023, two activists associated with prominent think-tanks in Serbia received individual notifications from Apple about a possible "state-sponsored attack" targeting their devices. Although they did not wish to be identified for this report due to fear of personal and professional repression, they both spoke extensively to Amnesty International about their cases. The individuals contacted the Belgrade-based SHARE Foundation who worked with Amnesty International and Access Now to carry out separate forensic analyses of iPhones from both notified individuals.

Amnesty International's forensic analysis, which concurred with an independent forensic analysis by Access Now and Citizen Lab, found that both devices showed signs of spyware targeting on 16 August 2023. In November 2023, Amnesty International published its finding on targeting of the two activists, but noted that it was not possible at that point to confirm if the devices were successfully compromised, or make a conclusive finding on the spyware used.[81]

Further technical and forensic research allows Amnesty International to now confirm that both individuals were indeed targeted with NSO Group's Pegasus spyware, although it remains difficult to determine if the targeting was successful in this instance.

The two devices were targeted with minutes of each other from two different attacker-controlled iCloud email addresses. Amnesty International attributes both email accounts to the Pegasus spyware system. Amnesty International has frequently found similar iCloud accounts used to send zero-click Pegasus attacks to target devices over iMessage.[82]

Case	Timestamp (UTC)	Trace
Pegasus Target 1	2023-08-16 12:**:**	Traces of Pegasus targeting from attacker-controlled iCloud account laiaotero@outlook.com against Apple HomeKit
Pegasus Target 2	2023-08-16 12:**:**	Traces of Pegasus targeting from attacker-controlled iCloud account blaserdavid@protonmail.com against Apple HomeKit

Table 2: Traces related to Pegasus zero-click targeting using Apple HomeKit

The traces of spyware targeting through Apple's HomeKit service closely resemble the attack techniques seen in other NSO Group Pegasus attacks observed by Amnesty International's Security Lab in the same period. The Security Lab confirmed that a separate group of individuals in India, who received notifications from Apple in the same round of notifications, were indeed targeted by NSO Group's Pegasus in August 2023.[83] These devices in India also showed similar traces of HomeKit exploitation before the full Pegasus exploit was sent over iMessage.

[80] Amnesty International, Case study: The Pegasus Project, https://securitylab.amnesty.org/case-study-the-pegasus-project/ (accessed on 20 November 2024).
[81] Amnesty International Security Lab, "Serbia: Civil society threatened by spyware", 28 November 2023, https://securitylab.amnesty.org/latest/2023/11/serbia-civil-society-threatened-by-spyware/
[82] Amnesty International, "Forensic Methodology Report: How to catch NSO Group's Pegasus", 18 July 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/
[83] Amnesty International, "India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists", 28 December 2023, https://securitylab.amnesty.org/latest/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/

Amnesty International's Security Lab research has also identified multiple Pegasus infection domains in the Serbian language which indicate that NSO Group's Pegasus spyware continues to be used in the country since at least October 2021, with continued activity at time of publication in December 2024.

Amnesty International attributes these Serbian-language domains to Pegasus, as their configuration matches a fingerprint of a Pegasus domain used in a forensically confirmed attack by another Pegasus customer.

4.3.2 PROTEST ORGANIZER TARGETED BY PEGASUS (CASE 2)

In a separate case, following the initial civil society targeting revealed in November 2023, Amnesty International carried out further investigation into the use of Pegasus spyware in Serbia. This research, including infrastructure mapping and OSINT investigations, led to the identification of an additional case of Pegasus spyware targeting a high-profile individual involved in wide-scale Serbian protest movement.

The observed Pegasus attack consisted of a Serbian-language 1-click Pegasus infection link sent over WhatsApp, from a Serbian phone number, in an attempt to hack the protest organizer. Evidence of this attack was publicly disclosed by the targeted individual, but not attributed to NSO Group's Pegasus spyware at the time.

Amnesty International is not naming the individual at this stage. Although the case was identified from public information, Amnesty International has not been able to interview the targeted person or carry out a forensic analysis of their device to determine if the targeting led to a successful infection with Pegasus.

NSO Group states that its products and services are "used exclusively by government intelligence and law enforcement agencies to fight crime and terror".[84] However, this statement has been challenged by research from civil society organizations, including Amnesty International, who have found evidence that the spyware has been used systematically to target journalists, activists and HRDs around the world.

Given that the NSO Group has consistently declared that their products are used exclusively by governments, the spyware operator is most likely a state agency. Those targeted with Pegasus spyware in Serbia have all previously faced threats, smear campaigns or other unwanted attention from the Serbian government for their activism. It is unlikely that any other state would have an interest in targeting this particular set of individuals.

Amnesty International wrote to NSO Group on 27 November 2024 to ask whether NSO Group, or other related legal entities had sold, directly or indirectly, any of its products to any government agency or company in Serbia, or any other governments that may have targeted civil society in Serbia. Amnesty International also asked NSO Group whether it had conducted human rights due diligence as per the UN Guiding Principles, during the development of the spyware and prior to any sales, and if any steps were taken to prevent human rights abuses related to the use of Pegasus spyware.

In its response to Amnesty International on 10 December 2024, NSO Group said they could not "comment on specific existing or past customers," but noted that "Serbia received a general score of 57/100 in Freedom House's 2023 report and a score of 6.33 in the Economists' 2023 Democracy Index, so we are talking about a significantly democratic and free country."[85] NSO Group also stated that the company was "fully committed to upholding the UN Guiding Principles on Business and Human Rights."

4.4 NOVEL "NOVISPY" ANDROID SPYWARE DEPLOYED BY SERBIAN AUTHORITIES

Since 2021, Amnesty International has received reports from numerous activists in Serbia who were concerned that their devices or digital accounts may be under digital surveillance by Serbian authorities. In multiple cases, activists and a journalist reported signs of suspicious activity on their mobile phones directly

[84] NSO Group, About us, https://www.nsogroup.com/about-us/ (accessed on 20 November 2024).
[85] NSO Group's response to Amnesty International's Right of Reply letter, 10 December 2024. On file with Amnesty International.

following interviews with Serbian police and security authorities. In at least two cases, individuals had their devices infected with spyware while attending a police station or meeting with BIA officials to make a report as victims of a crime.

In the period from November 2023 to November 2024, Amnesty International's Security Lab carried out forensic analysis on devices of more than 30 Serbian civil society members, the majority of which were Android devices, the most widely used operating system for phones in the country. This research uncovered evidence that a new, previously undisclosed Android spyware system, most likely developed domestically in Serbia, is being used widely to covertly infect the phones of civil society members while their devices are temporarily in the physically possession of BIA or the police.

This section summarises the evidence of the NoviSpy spyware installed on the phones of civil society activists and journalists.

4.4.1 SPYWARE INSTALLED COVERTLY DURING INTERVIEW WITH BIA (CASE 3)

Amnesty International interviewed an activist from the NGO Krokodil who was concerned about the security of their phone following an interview by BIA security service officials in Belgrade in October 2024. Krokodil is an organization promoting dialogue and reconciliation in the Western Balkans. It is also one of the few organizations in Serbia which has very publicly condemned the Russian invasion of Ukraine and provided support to Russian dissidents and Ukrainians living in the country. This has led to frequent threats against their organization and vandalization of their office, mostly by groups of local football hooligans.

On 20 September 2024, a group of Russian-speaking people wearing shirts featuring the faces of Serbian convicted war criminals entered the premises of the organization while the staff were working and forcibly removed the Ukrainian flag. Because the intruders seemed to be foreign citizens and the incident differed from the usual harassment by the Serbian hooligans, it alarmed everyone in the organization.

Krokodil staff immediately reported the incident to the nearest police station and the police visited the office shortly after. Although they spoke with the staff, the police decided not to issue an official incident report, which was not in line with the usual procedure. The police also asked Krokodil staff to provide them with the footage from the office security camera.

Several days later, on 1 October 2024, following the staff's request for a meeting with BIA, which deals with issues of foreign threats, the activist was called for an interview about the incident. The meeting took place at the Ministry of Interior building in the Savski Venac area of Belgrade.

As soon as the activist entered the office, the plain-clothes officers asked them to restart their phone to "make sure that the conversation was not being recorded." The activist opened their Android phone in front of the men by using the pattern-configured PIN code. Although the officers present could not have seen the PIN, there were many cameras in the room and the activist believes they could have captured the unlock pattern on camera. During the interview the phone was left unattended in the activist's jacket outside the interview room.

The activist remained in the interview room between 10:17 and 11:40. The conversation revolved around the violent incident, and the activist shared their frustration with the police and authorities for failing to protect civil society from attacks by foreign nationals.

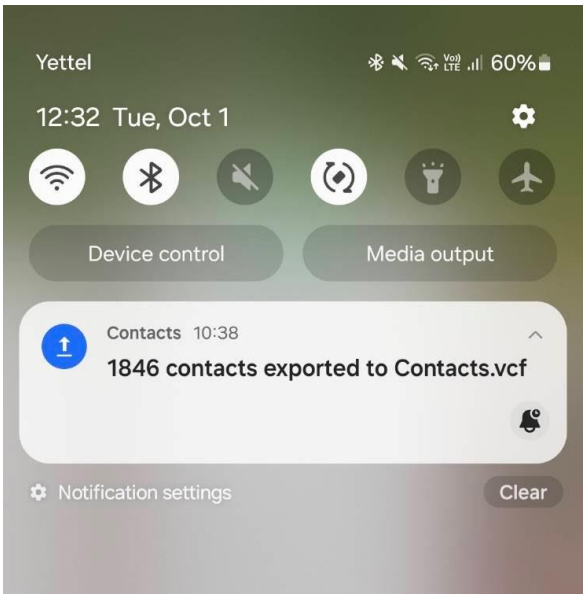


Figure 2: Screenshot showing the export of contacts during police interview

As soon as the activist left the office, they noticed suspicious signs on their device, including a notification suggesting that their saved contacts had been exported from the phone at 10:38 (see Figure 2), which was during the period when they were being interviewed. Following these observations, the activist decided to contact Amnesty International's Security Lab. At the same time, the activist confronted BIA officials directly and asked them why they exported their saved telephone contacts, but the officials denied having anything to do with this.

Amnesty International's Security Lab performed a forensic analysis of the activist's Samsung Galaxy S24+ device which revealed that two Android spyware applications were installed on the activist's phone during the interview with BIA officers.

Around 10:20, minutes after beginning the interview, the activist's phone was powered on and connected to a ThinkPad X1 Yoga computer using a USB cable. The authorities appear to have already known the unlock pattern at this point. At 10:24, Android developer mode was enabled on the phone and shortly afterwards, the authorities connected to the phone using the ADB debugging protocol.

Over the following minutes, a computer user "spartan" made a series of changes on the device. Some changes were made automatically using ADB, and other manual steps were taken to disable security features such as automatic security updates and Google Play Protect.

Time (local time)	Event
2024-10-01 10:17 (approx)	Police interview begins. Phone left unattended
2024-10-01 10:20:45	Phone turned on
2024-10-01 10:24:03	USB cable connected
2024-10-01 10:24:23	Android developer mode enabled
2024-10-01 10:25:54	Google Play Protect disabled over ADB
2024-10-01 10:25:55	Install of spyware app com.serv.services
2024-10-01 10:27:04	Install of spyware app com.accesibilityservice
2024-10-01 10:27:05	com.accesibilityservice enabled as accessibility service over ADB
2024-10-01 10:31:17	Android developer mode disabled
2024-10-01 10:31:17	Automatic system security updates disabled

2024-10-01 10:38	Saved contacts exported from phone
2024-10-01 10:39:51	Phone disconnect from USB
2024-10-01 11:40 (approx)	Police interview with the activist finishes
2024-10-01 12:32	Activist identifies and screenshots notification about exported contacts

Table 3: Forensics traces showing spyware installation

The authorities installed two malicious Android applications on the phone over the Android ADB protocol, with package names "com.serv.services" and "com.accesibilityservice". Amnesty International's Security Lab was able to recover samples of both spyware applications from the activist's phone.

Both Android applications are novel Android spyware apps which Amnesty International attributes with high confidence to BIA. Amnesty International is referring to this newly disclosed spyware family as the NoviSpy spyware. More information about the NoviSpy spyware and the technical attribution of the spyware to the Serbian BIA is outlined in Section 4.5.

Android Package	Name	APK Hash
com.serv.services.apk	NoviSpyAdmin	087fc1217c897033425fe7f1f12b913cd48918c875e99c25bdb9e1ffcf80f57e
com.accesibilityservice	NoviSpyAccess	99673ce7f10e938ed73ed4a99930fbd6499983caa7a2c1b9e3f0e0bb0a5df602

Table 4: Samples of the two related NoviSpy Android spyware apps

The "com.serv.services" app, NoviSpyAdmin, requests extensive permissions including Device Admin permissions, which allow the app to collect sensitive records from the infected device including call logs, phone contacts lists, and SMS messages, as well as to record audio through the phone's microphone.

The second "com.accesibilityservice" spyware app, NoviSpyAcccess, misuses legitimate Android accessibility features in order to covertly collect screenshots from the device, in addition to exfiltrating saved files, tracking the phone's location, and activating and recording from the camera on the phone.

At 10:27, the phone was reconfigured to trust and enable the new NoviSpyAcccess app as the active accessibility service on the phone. The forensic logs also suggest the authorities manually browsed through the device and photo gallery after the spyware was installed. During this time the phone contacts were also exported. Forensic traces show that the device was finally disconnected at 10:41.

SPYWARE ACTIVELY RUNNING ON THE DEVICE DURING ANALYSIS

During the Security Lab's forensic analysis of the activist's phone, it became apparent that the Samsung Galaxy S24+ was still actively infected and collecting surveillance data while analysis was being carried out. Amnesty International was able to successfully recover surveillance logs and screenshots, generated by the NoviSpyAcesss spyware application and stored encrypted on the device before upload to an attacker-controlled spyware server hosted at 195.178.51.251. The NoviSpyAdmin spyware communicated with a spyware command and control hosted at 178.220.122.57. This IP address is associated with Telekom Srbija, a government-controlled internet service provider.

The recovered data included numerous screenshots captured by the NoviSpyAcesss spyware while the activist was using their phone including screenshots of their email accounts, Signal and WhatsApp messages, and social media activity. While the spyware does not have capabilities to download all data from installed apps, the ability to capture and regularly upload data from the screen still reveals a substantive amount of personal information to the agency controlling the app.

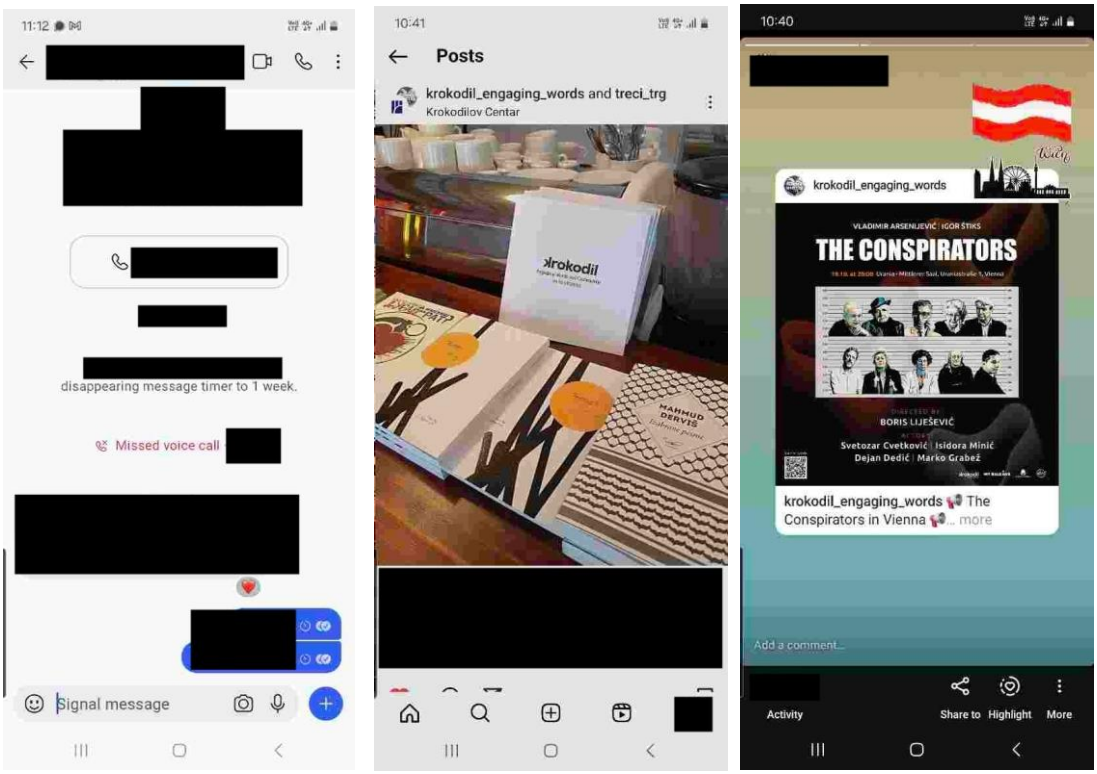


Figure 3: Screenshots taken by NoviSpy spyware as the activist was using Signal and Instagram; recovered and decrypted from infected phone.

4.4.2 SPYWARE INSTALLED ON PHONE OF JOURNALIST FOLLOWING TRAFFIC STOP (CASE 4)

Amnesty International forensically analysed the device of a Serbian journalist, Slaviša Milanov, who also had strong suspicions that his Android mobile phone had been tampered with by Serbian authorities.

Slavisa is a journalist from Dimitrovgrad, who works with the news portal FAR, which covers issues of local interest. He focuses on investigative pieces and reports on local politics, including sensitive topics of public spending at the local level, government financial, corruption, and other issues of public interest.

On 21 February 2024, Slaviša and a colleague were travelling toward the town of Pirot for a business meeting. At around 10:30 in the morning, they were stopped by the traffic police and, during the checks, Slaviša was told that he would need to undergo additional tests (for alcohol and drugs) at the police station. "I was quite surprised because it was fairly early in the morning."

At the police station, Slaviša was told that he would need to leave all his belongings, including the phone. "A traffic policeman arrived after 20 minutes and conducted an alcohol and drug tests, which both came negative. I expected them to let me go immediately." Slaviša had the impression that the police were delaying for more time. Slaviša told Amnesty International that two men in civilian clothes took over the interview, and after moving to another building they began asking Slaviša questions about his journalistic work and the financing of FAR media portal.

Following the questioning, his devices were returned, and he was released. He was immediately suspicious that his phone had been tampered with, as he saw that mobile data and wi-fi on the phone were turned off and certain applications on his device were using excessive battery power. He suspected that the authorities had accessed his device while it was out of his possession. A few days later he installed an Android security app which showed that some apps on his phone were accessed while he was in custody. There were also signs that some new applications were installed on the phone too.

Amnesty International's Security Lab carried out a forensic analysis of Slaviša's Xiaomi Redmi Note 10S which revealed forensic traces confirming that the same two NoviSpy spyware apps were also covertly installed on his mobile phone during the time he was being questioned.

The forensic analysis also uncovered evidence suggesting that Cellebrite's UFED mobile forensic product was used to unlock the device to allow infection with the spyware.

Time (local time)	Event
2024-02-21 11:10 (approx)	Slavisa's phone is left unattended during interview with Serbian authorities
2024-02-21 11:56:07	Xiaomi file manager app is granted permission to install Android APK packages.
2024-02-21 11:56:09	Android package installer app is opened to install an Android app
2024-02-21 12:01:32	The Android *ACCESS_RESTRICTED_SETTINGS* option is modified to allow enabling of Android Accessibility service apps. This is necessary to enable the functionality of the NoviSpy spyware.
2024-02-21 12:16:10	Second Android package installed through Android package installer
2024-02-21 12:40:18	NoviSpy spyware app com.accesibilityservice recorded communicating with spyware server at 195.178.51.251
2024-02-21 13:27	Phone returned to Slavisa by authorities at this point
2024-02-26 09:24	com.accesibilityservice NoviSpyAccess spyware app removed by Slavisa using an Android security app.
2024-02-26 09:26	com.serv.services NoviSpyAdmin spyware app removed from phone.

Table 5: Forensic traces of NoviSpy spyware application on phone of Slavisa Milanov

The full background of this case and the use of Cellebrite products is described in Section 5.2.1.

4.4.3 NOVISPY SPYWARE INSTALLED ON DEVICE OF YOUTH ACTIVIST (CASE 5)

In November 2024, Amnesty International forensically analysed the phone of Nikola Ristić, a youth activist. This analysis confirmed a second case of an individual whose device was unlocked with Cellebrite UFED and infected with the NoviSpy while in possession of Serbian authorities.

Nikola was one of the key organizers of the protest in Belgrade following the tragic incident in Novi Sad in November, where a collapsed roof on the city's train station killed 14 people and injured dozens of others. "The idea was to bring people together and paint Trg Republike (Belgrade's main square) in red paint, alluding to the fact that the authorities have blood on their hands and are responsible for this tragedy," Nikola told Amnesty International.

On 3 November, Nikola and his partner arrived on the square around 10:00, two hours before the scheduled protests, carrying cans of paint. Shortly after they arrived, they were stopped by four men who subsequently introduced themselves as BIA officers, and asked Nikola to accompany them to a police station for an informational interview. He initially resisted because the officers did not have a warrant or a court order to bring him in, but after a brief altercation, which his partner recorded on her phone, and after he was assured that the questioning would be brief, he agreed to go.

"One of the officers was particularly unpleasant and aggressive. He pushed me into the car, pressed his fist against my forehead and told me that he could do this with his gun instead and drag me around the square, to give me a reason to complain about an 'unpleasant arrest.'"

At the police station, Nikola was asked to empty his pockets and the officers put all his belongings, including his phone, into a plastic bag, and told him that these would be returned to him after the interview.

Once in the interview room, the officers handed Nikola's phone back to him and requested that he call his partner and ask her to remove the footage of his arrest, which was by this point circulating on social media,

from the internet. After he made the call [and his partner refused to take down the video], he locked his phone and gave it back to the officer, who took it out of the room.

During the time he was in BIA custody, Nikola was asked about his activism, plans for future protests and told that his engagement had been putting his, the safety of his family and the community as a whole in danger. "They said that we are all just naive and idealistic kids who don't know what they're doing and that we don't realize that we are endangering everyone's safety by protesting." Nikola was kept in the station for little over two hours, but he felt that there was no point or purpose in his questioning and that the officers were only trying to buy time.

As he was finally released, Nikola asked for a court order but the officers told him that the prosecutor was still in the process of deciding whether his post on the social media in which he called for the peaceful protest warranted his case being turned over the police or not and could not share any documents. Nikola was finally released around 13:30. As soon as he was released, Nikola suspected that his phone had been accessed and contacted Amnesty International's Security Lab.

FORENSIC ANALYSIS SHOWS INSTALLATION OF NOVISPY SPYWARE

Amnesty International's Security Lab carried out a forensic analysis of Nikola's Huawei Honor 20 Pro which showed traces confirming the NoviSpy spyware apps were installed on his mobile phone during the time he was being questioned by BIA officers.

Time (Local Time)	Event
2024-11-02 01:56	Phone was switched on
2024-11-03 10:00 (approx.)	Nikola taken to the police station by BIA officers.
2024-11-03 10:48:44	Process crash associated with Cellebrite UFED exploitation; logs deleted
2024-11-03 11:39:19	Security prompt in Settings app
2024-11-03 11:40:29	Installation of NoviSpy spyware app com.serv.services
2024-11-03 11:42:05	Installation of NoviSpy spyware app com.accesibilityservice
2024-11-03 12:12:39	Huawei file manager app provided access to external storage
2024-11-03 13:30 (approx.)	Nikola is released by BIA.
2024-11-05 09:08:01	New NoviSpy upload interval ("*UIR*" option) changed from 30 seconds to 180 seconds

Table 6: Traces of NoviSpy spyware installation on phone of Nikola

The forensic traces show that Nikola's phone was also infected with the NoviSpy spyware through physical access to the device during the BIA interview. Log files record that the phone was connected to a computer using the Android ADB protocol, and changes were again made on the device to try avoid detection including disabling device security updates and Google Play Protect (similar to Case 3).

The phone was still actively infected with the NoviSpy spyware at the time of analysis, one week after the initial infection. Evidence extracted from the device shows that the spyware operators had reconfigured the spyware infection on 5 October 2024, telling NoviSpy to upload data to the spyware server every 3 minutes (180 seconds) rather than the default of 30 seconds, which shows that operators were actively managing the infected device.

Forensic traces indicate that Cellebrite UFED was again used to exploit the phone before the spyware installation. The Cellebrite evidence for this case is documented in Section 5.2.2.

4.4.4 ATTEMPTS TO INSTALL SPYWARE ON DEVICE OF ENVIRONMENTAL ACTIVIST (CASE 6)

Ivan Milosavljević Buki is an environmental activist and a leader of an environmental organization, Rangers of Eastern Serbia ("RIS"), in Petrovac na Mlavi and Homolje. In August 2024, Buki worked with the Serbian media outlet N1 to document unlawful collection of drinking water for use in mining operations on Homolje

mountain. Buki frequently faced physical threats while documenting the role of the local public water company in collecting drinking water for use in mining operations. In August 2024, he published a video recording of one such incident. A few days later, he was confronted by three men working with the local municipal office who told him that it would be a "shame if [he] were to be torn apart by the wolves in the forest," which he perceived as a direct threat.

After publicly speaking about these incidents, Buki was asked to come in for an informational interview with BIA in their office in Požarevac on 22 August 2024.[86] He did not consider this unusual as he, like other prominent environmental activists, normally has a great deal of interaction with BIA, which takes special interest in their activism. As he entered the building, as in the case of the Krokodil activist, BIA officers asked Buki to restart and unlock his phone so that the agent could check if any audio or video recording apps were running on his phone. Buki had a complex PIN code on his device, and after trying for a moment, he succeeded in unlocking his phone, which was quickly checked by BIA officers. After checking it, the officers told Buki to lock his phone in a cell phone locker and handed him the key.

Buki then entered another room where the interview was conducted. After a few minutes, an agent entered the room and began asking him about an assault which he had reported and asked to see a recording of it. Buki told the officers that the recording was available all over the internet because a media outlet had recorded it live, and that they could look it up for themselves.

The officers said that they could not access the internet from the computers in the room, and instead asked Buki to unlock his phone to show them the video. He retrieved his phone from the locker, played the video and gave his device to the officer. The officer started scrolling randomly on the device, and Buki believed he was no longer watching the video but instead keeping the device active to prevent it from locking. Eventually the officer's own phone rang, and he walked out of the room to take the call, while taking with him Buki's still unlocked phone.

After few minutes, the officer came back with the locker key and gave it back to Buki. following this encounter, Buki strongly suspected that his phone was tampered with during the time his phone was unlocked and in the possession of the authorities.

Amnesty International performed a forensic analysis on Buki's phone which revealed that the authorities had attempted, apparently unsuccessfully, to install Android applications through the Files app while the unlocked phone was out of the interview room.

Time (local time)	Event
2024-08-22 12:00 (approx)	Buki enters the police building
2024-08-22 13:26:35	Buki's Android phone connected over USB to transfer files
2024-08-22 13:37:35	Google File app granted permission to install Android APK application from disk
2024-08-22 13:51:26	Google File app in foreground granted permission for second time to install Android APK application from disk
2024-08-22 13:56:10	Google Play Protect blocked attempted installation of untrusted application and prompted for additional biometric or PIN verification before allowing app installation.
2024-08-22 14:08:17	Additional traces showing connection of phone over USB
2024-08-22 16:00 (approx)	Buki leaves the BIA office

Table 7: Forensic traces showing attempted installation of Android apps during BIA interview

Over a period of twenty minutes the phone was connected to a computer by USB and at least two attempts were made to approve the installation of untrusted Android applications copied to the phone and opened in the Files application.

Amnesty International believes an attempt to install the NoviSpy spyware may have been blocked due to a recently introduced security feature in Google Play Protect. The installation of untrusted Android APK files outside the Play Store can raise an "Unsafe app blocked warning." While previously this warning could be clicked through, Play Protect can now require reauthentication using biometrics or the device pin code to

[86] N1, "Aktivista sa Homolja na razgovoru u BIA" ["An activist from Homolje at an interview in the BIA"], 22 August 2024, https://n1info.rs/vesti/aktivista-sa-homolja-na-razgovoru-u-bia/ (in Serbian).

approve the potentially unsafe installation. In this case, BIA officers had the unlocked phone but not the device PIN and may have not been able to install the spyware app as intended.

As the installation attempts were unsuccessful, no forensic records are available confirming that the applications the authorities tried to install were the NoviSpy spyware. However, considering the involvement of BIA in the interview, and forensic traces confirming attempts to install two untrusted Android apps during the time the device was in BIA's possession, Amnesty International strongly believes that the authorities were attempting to install the NoviSpy spyware in this case too.

4.5 ATTRIBUTION OF THE MALICIOUS APPLICATIONS TO BIA

An analysis of the obtained NoviSpyAccess spyware sample (`com.accesibilityservice`) recovered from the phone of the Krokodil activist (Case 3), revealed that the spyware was configured to communicate and upload stolen data to a spyware command-and-control server hosted at the IP address 195.178.51.251.

```
public static long maxCriticalTemperature = 90;
public static long minFreeMemory = 50;
public static String simNumbers = RecordedQueue.EMPTY_STRING;
public static String serverIp = "195.178.51.251";
public static long serverPort = 8080;
public static boolean locationMonitoring = true;
public static long minPeriodForUpdates = 30;
```

Figure 4: BIA server IP address hardcoded in "com.accesibilityservice" (99673ce7f10e938ed73ed4a99930fbd6499983caa7a2c1b9e3f0e0bb0a5df602)

Amnesty International associates this IP address directly with the Serbian BIA. This IP address is also in the same narrow IP range identified by Citizen Lab as hosting a Finfisher spyware system in 2014. Indeed, Citizen Lab identified this exact same IP address, 195.178.51.251, as being linked in 2014 to specific BIA employee through the computer name of a public server at that IP. The computer name contained part of the employee's name.[87]

Amnesty International has reviewed open-source intelligence indicating this same individual had communicated with the now defunct spyware vendor Hacking Team about testing their Android spyware agent in 2012 (see Chapter 4.1). Amnesty International also has evidence that this same named individual has links to deployment of the newly identified NoviSpy Android spyware described in this report. Specifically, a phone number embedded in the spyware configuration, potentially as a test, appears to be associated to the same named individual in public caller ID databases.

```
Г-Т\",\"minCriticalTemperature\":70,\"simNumbers\":\"+381[redacted]80\",\"audioFileLength\"
ɜ,\"maxCriticalTemperature\":90,\"codeName\":\"TEST-T\",\"minCriticalTemperature\":70,\"
```

*Figure 5: Configuration option in spyware sample contain phone number associated to BIA individual +381*******80*

The multiple links connecting the NoviSpy spyware directly to the IP network of the BIA, and the fact that the NoviSpy sample was installed covertly while the phone was in the possession of the BIA allows for clear attribution of this spyware family and campaign to BIA. Amnesty International cannot determine if the NoviSpy spyware was developed in-house by BIA or by another organization on their behalf.

Multiple NoviSpy spyware samples contained log messages and other strings written in the Serbian language. This is consistent with the spyware being developed domestically in Serbia, rather than being purchased from a foreign spyware vendor. At this time, there are no indications that the NoviSpy spyware has been used by other organizations outside of Serbia.

[87] Citizen Lab, Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation, 15 October 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

```
    }
    if (Services.this.TimeOfDataRefresh > 15) {
        Services.this.TimeOfDataRefresh = 0;
        File fFile = Services.this.getApplicationContext().getDir("AndroidFiles", 0);
        Services.this.LD.LoadAllData(fFile);
        Log.v("Proba", "ucitavanjepodataka");
    }
    Calendar calendar = Calendar.getInstance();
```

Figure 6: NoviSpy log messages written in Serbian

Amnesty International identified additional samples of an older variant of the NoviSpy spyware on VirusTotal, a security industry database of potentially malicious files, which indicated that the development of this spyware has been ongoing since at least 2018.

Amnesty International wrote to BIA with detailed questions about the NoviSpy spyware but did not receive a response before publication.

4.6 WIDER TARGETING USING SERBIAN ANDROID SPYWARE

As detailed in this chapter, Amnesty International identified four instances where the NoviSpy spyware was used in attempts to infect Android devices of civil society in Serbia between February and mid-November 2024. These cases, identified through outreach to civil society, provide a partial glimpse into the wider pool of likely NoviSpy spyware victims. Technical artefacts present in the NoviSpy spyware samples can be used to infer that NoviSpy spyware deployment is occurring at a much wider scale.

Each identified NoviSpyAdmin spyware sample contains an apparently unique and incrementing user ID used to uniquely identify the victim device when connecting to the spyware server over the FTP protocol, which allow computers to exchange files over a network. The sample installed on the Krokodil activist's phone on 1 October 2024 was configured with user ID *621*.

```
public static String fileNameSecureRecording = "SRN";
public static String userName = "621";
public static String userPassword = "hOcY[redacted]KF";
public static String serverIP = "178.220.122.57";
public static String cryptPassword = "7s60[redacted]VvjK";
public static boolean userWifiStatus = false;
```

Figure 7: Unique user ID included in NoviSpyAdmin sample

A newer NoviSpyAdmin sample recovered from the device of another individual, Nikola (Case 5), infected a month later in early November 2024, contained a hardcoded user ID *644*. This technical evidence suggests that twenty or more unique NoviSpy spyware samples were generated and potentially installed in just one month.

This limited information about the purpose of user IDs in the samples makes it difficult to determine if these ID numbers are indicative of the overall number of targeted devices. The user ID value may not start at zero, and not all generated spyware samples may have been used in live infections.

However, the evidence of more than 20 unique user IDs generated over a one-month period suggests that the full scale of targeting is much more extensive then the four NoviSpy spyware cases identified and described in this report. The NoviSpy spyware has likely been used against a range of surveillance targets. There is no suggestion that all uses of the NoviSpy spyware were targeted against civil society, or indeed that the spyware has not also been used as a component of a legitimate criminal investigation in some instances.

4.6.1 GOOGLE CONFIRMS MALICIOUS NATURE OF NOVISPY SPYWARE

Amnesty International reported these malicious Android spyware applications to the Google and Android security teams before publication of this report. In response, Google informed Amnesty International that it performed its own investigation, which confirmed that both NoviSpy applications reported by the Amnesty International's Security Lab were indeed malicious and designed to collect information covertly from the infected devices.

Drawing upon technical leads shared by Amnesty International's Security Lab, Google reported that its researchers were able to identify additional actively compromised devices and remove the spyware from affected devices.

In order to further protect targeted individuals, Google also sent a "government-backed attack" threat notification to all Google users who were identified by Google as targets of this spyware campaign.

Amnesty International has published a new set of indicators of compromise (IOCs; see Glossary) for the Mobile Verification Toolkit (MVT) to assist technical individuals to screen devices for signs of compromise with this spyware.[88] A set of YARA signatures for this spyware is available on the Amnesty International investigation repository.

A detailed technical analysis of the uncovered spyware applications has been published as a separate technical appendix at the end of the report.

[88] Amnesty International, Serbia NoviSpy Indicators of Compromise, https://github.com/AmnestyTech/investigations/tree/master/2024-12-16_serbia_novispy

5. MISUSE OF CELLEBRITE DATA EXTRACTION TOOLS IN SERBIA

Over the past year, an increasing number of individuals from Serbian civil society reported to Amnesty International that their mobile devices were seized or searched by Serbian authorities, sometimes without a clear legal justification for carrying out the device searches and without the device owner's knowledge or consent. This included environmental activists, journalists and others involved in various peaceful protest movements.

Amnesty International's Security Lab carried out forensic analyses on iPhones and Android devices of more than a dozen persons who suspected their devices were seized or covertly accessed by Serbian authorities during periods of detention or questioning. These forensic investigations have uncovered technical evidence confirming that Serbian authorities have systematically used mobile data extraction technology, sold by cyber-intelligence company Cellebrite, to unlock and extract data from seized devices, sometimes without the consent or knowledge of the device owner.

Cellebrite is a publicly-traded company, founded and headquartered in Israel but with offices globally. According to Cellebrite, their technology provides a comprehensive investigative platform that "helps customers legally collect and review, analyse and manage digital data in lawful, ethical and auditable manner while protecting privacy." [89] Cellebrite digital forensics products are used by companies, law enforcement and security agencies across the world; Cellebrite's parent company, Sun Corporation, claims that their products are used in over 150 countries.[90] The company is most well-known for its flagship Universal Forensic Extraction Device (UFED) suite of mobile phone extraction products. Cellebrite's UFED and related products enable Cellebrite's customers to bypass security defences in order to unlock and extract data from a wide range of mobile devices.

Cellebrite's UFED Cloud is an additional product that enables Cellebrite customers to use passwords and tokens extracted from a target phone to "extract, preserve and analyze public- and private-domain, social-media data, instant messaging, file storage, web pages and other cloud-based content" not necessarily stored on the phone.[91] Cloud extraction productions extend the intrusiveness of the searches being performed, probing beyond the seized device and deeper into a target's entire historical digital life. It enables

[89] Cellebrite, "Cellebrite Provides Facts About its Business and Solutions", https://cellebrite.com/en/cellebrite-facts/#:~:text=Cellebrite%20is%20a%20cellphone%20hacking%20company.&text=Cellebrite's%20comprehensive%20Investigative%20DI%20Platform,auditable%20manner%20while%20protecting%20privacy (accessed on 9 December 2024)
[90] Overseas Offices | Sun Electronics Co., Ltd.
[91] Cellebrite, Cellebrite Digital Intelligence Glossary, https://cellebrite.com/en/glossary/cloud-data-extraction-digital-forensics-en/ (accessed on 20 November 2024).

the Cellebrite operator to access even deleted files, photos or other digital content no longer stored on the device, and potential exposing a decade or more of data.[92] Cellebrite's central management and analytics products also allow data from multiple individual targets to be combined, providing deep insights into the organization and communication of social networks such as protest movements or communications between journalists and their sources.[93]

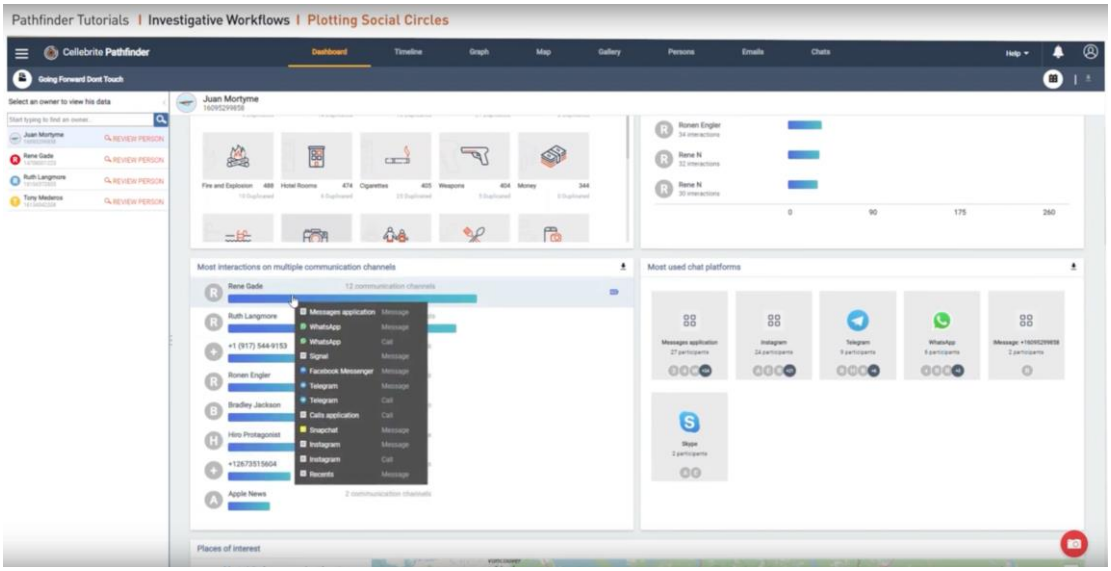


Figure 8: Cellebrite AI-powered Pathfinder analytics software combines current and historical data from multiple targets

Cellebrite states that the company has strict licencing policies and restrictions to govern how customers use their technology.[94] However, Privacy International[95] and Access Now have extensively documented weakness in Cellebrite's human rights due diligence policies, resulting in sales of Cellebrite to governments with spotty human rights track record and where there is a high-risk that such products could be used to target civil society.[96] Cellebrite technology has been used in countries including Belarus, Myanmar, and China, raising suspicions of misuse for political purposes, prompting the company to stop doing business with some of them.[97] In an email to Amnesty International in October 2024, the Cellebrite senior director for communications wrote that "Cellebrite's digital forensics solutions are licenced strictly for lawful use, require a warrant or consent to help law-enforcement agencies with legally sanctioned investigation *after* (original italics) a crime has taken place," and that Cellebrite does not provide cyber-surveillance technology.[98]

Amnesty International's Security Lab, however, has uncovered forensic evidence confirming that Cellebrite's UFED product can and has been used to enable surveillance operations. Specifically, the investigation found that Cellebrite products were used to covertly unlock at least two Android phones, including of an investigative journalist and a civil society activist in Serbia, without their knowledge or consent. After gaining access to the phones - only possible through the use of Cellebrite - Serbian authorities were able to infect the phones with the invasive NoviSpy Android spyware (See Case 4A described in Section 5.2.1) with capabilities to intensively track and monitor the targeted people and their communications.

Amnesty International believes these are the first forensically documented cases confirming the use of Cellebrite's UFED product to enable the covert infection of a locked and secured device with spyware during police detention.

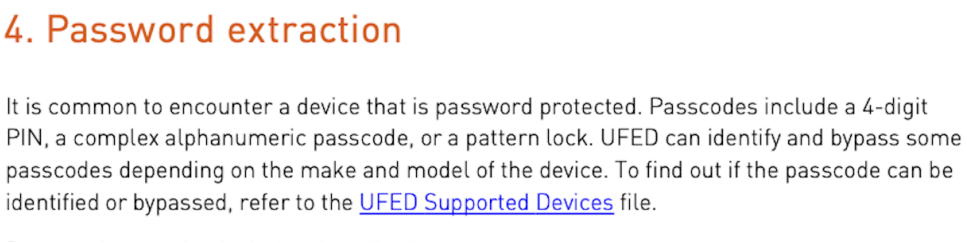
---

[92] Privacy International, Cloud Extraction https://privacyinternational.org/learn/cloud-extraction (accessed on 20 November 2024).
[93] Cellebrite, "Pathfinder Tutorials I Investigative Workflows I Plotting Social Circles", 27 September 2023, https://www.youtube.com/watch?v=UxJ-1yU5aKk
[94] Cellebrite, "Cellebrite Provides Facts About its Business and Solutions", https://cellebrite.com/en/cellebrite-facts/
[95] Privacy International, "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers", 3 April 2019, https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers
[96] Access Now, "What spy firm Cellebrite can't hide from investors", 26 May 2021, https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/
[97] See Access Now, "What spy firm Cellebrite can't hide from investors", 26 May 2021, and also https://www.sec.gov/Archives/edgar/data/1854587/000121390021034768/ff42021a1_cellebritedi.htm#T23
[98] Email from Cellebrite's Senior Director for Corporate Communications, to Amnesty International in response to the organization's research letter of 20 September 2024, 5 October 2024. On file with Amnesty International.

5.1 HOW CELLEBRITE CAN BREAK INTO PHONES

Cellebrite's flagship UFED system is a suite of products enabling Cellebrite customers to unlock and extract data from a wide range of mobile devices including some of the most recent Android devices and iPhone models. Cellebrite's UFED-powered products such as Cellebrite Inseyets, use highly sophisticated zero-day exploits and other advanced data extraction techniques to gain access to mobile devices and user data. Zero-day exploits take advantage of non-publicly known software security issues which are difficult to defend against.

Cellebrite products can use these software flaws to bypass device security mechanism such as pin codes and encryption and gain access to the target device as described in the following Cellebrite manual.


4. Password extraction

It is common to encounter a device that is password protected. Passcodes include a 4-digit PIN, a complex alphanumeric passcode, or a pattern lock. UFED can identify and bypass some passcodes depending on the make and model of the device. To find out if the passcode can be identified or bypassed, refer to the UFED Supported Devices file.

Figure 9: Description of Cellebrite unlocking feature in publicly leaked UFED manual

UFED provides different capabilities depending on the status of the phone, either **unlocked** (where the passcode is known) or **locked** with an unknown passcode. A more detailed analysis of how Cellebrite UFED products work, based on a review of public and leaked Cellebrite marketing materials is included as Annex 1.

Unlike mobile spyware products, Cellebrite UFED and similar mobile data extraction systems are not intended to be used remotely or covertly, and typically require some form of physical access to the targeted device. However mobile forensic tools such as Cellebrite UFED and advanced spyware both frequently exploit unpatched zero-day vulnerabilities, and both can be used to gain non-consensual access to mobile devices by bypassing built-in device security mechanisms once physical access is possible.

5.1.1 ZERO-DAY EXPLOIT DISCOVERED FROM PHONE OF SERBIAN ACTIVIST

While conducting research for this report, the Security Lab also uncovered forensic evidence leading to the identification of **a zero-day Android privilege escalation vulnerability** used to escalate privileges on the device an activist from Serbia. The vulnerability, identified in collaboration with security researchers at Android-maker Google, affected numerous Android devices using popular Qualcomm chipsets impacting millions of Android devices worldwide. The vulnerability was reported to Qualcomm in August 2024, and a patch fixing the security issue was released in the October 2024 Qualcomm Security Bulletin as CVE-2024-43047.[99]

Drawing on the Security Lab findings about the zero-day vulnerabilities exploited by Cellebrite, researchers at Google's Project Zero were able to identify an underlying software flaw and report the vulnerability. Google Project Zero have published a separate technical report analysing the exploited software vulnerability, as well as additional security issues found in their investigation.[100]

[99] Qualcomm, October 2024 Security Bulletin (updated on 17 October 2024), https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html (accessed on 20 November 2024).
[100] Google Project Zero, "The Qualcomm DSP driver - Unexpectedly Excavating an Exploit", 16 December 2024, https://googleprojectzero.blogspot.com/2024/12/qualcomm-dsp-driver-unexpectedly-excavating-exploit.html

5.2 PHONES UNLOCKED WITH CELLEBRITE UFED AND INFECTED WITH SPYWARE

5.2.1 JOURNALIST'S PHONE UNLOCKED WITH CELLEBRITE BEFORE INFECTION WITH NOVISPY SPYWARE (CASE 4A)

Amnesty International forensically analysed the Android device of Slaviša Milanov, a Serbian journalist who had his devices seized during a supposed traffic stop (see Case 4 in Section 4.4.2).

Amnesty International's Security Lab analysed forensic records from Slaviša's device, which showed clear forensic evidence that his mobile phone, a Xiaomi Redmi Note 10S, was accessed without authorization between approximately 11:20 and 13:25, during which time he was questioned by police and other officers. The phone was returned to Slaviša at approximately 14:40.

Amnesty International found distinctive forensic traces on the device which the Security Lab attributes to Cellebrite's UFED product, including a copy of a Cellebrite binary named **falcon**. An identical **falcon** binary was also found on the phone of activist Ivan Bjelić (see Case 7 in Section 5.3.1) following a Cellebrite extraction, demonstrating that both phones were hacked with a similar version of Cellebrite's mobile forensic product. Amnesty International has identified Cellebrite documentation which references **falcon** as a tool linked to their Android data extraction capability (see Annex 2).

Binary Name	SHA 256
Falcon	3621ffeb67efa3eccb9c1f20cd671b81b286a02425e582a8a1553e85b012403d

Table 8: Cellebrite falcon binary found on phone of Slavisa Milanov

Additionally, as previously outlined in Section 4.4.2, the forensic records show that during the time Slaviša's phone was in the possession of Serbian authorities, the NoviSpy Android spyware applications were installed on his device. The NoviSpy spyware applications remained installed on the device for two days until manually removed by Slaviša using an Android security application.

CELLEBRITE UFED USED TO BYPASS PHONE LOCK SCREEN AND ENCRYPTION

Slavisa was neither asked for, nor did he provide, the passcode for his Android device. The authorities did not disclose to Slavisa that they wanted to search his device, nor did they declare any legal basis for such a search. The phone was switched off by Slavisa before handing it to the police. Given the circumstances, the Serbian authorities likely needed to use Cellebrite's Before-First-Unlock (BFU) flow to bypass the phone's screen lock, brute force guess or otherwise recover the pin, and extract content from the device. Leaked Cellebrite support documents show that brute-force unlocking and decryption of MediaTek devices like Slavisa's Xiaomi Redmi Note 10S was supported by Cellebrite UFED.

The Xiaomi Redmi Note 10S uses a MediaTek chipset. Leaked Cellebrite documentation from April 2024 states that the latest UFED software version supports unlocking non-Samsung MediaTek-based (MTK) devices from Xiaomi, Huawei and other vendors from a cold and turned off state.[101] The UFED device support matrix also states that 'brute-forcing' or recovering the encryption password is supported on these devices.

[101] Graphene OS Discussion Forum, "Claims made by forensics companies, their capabilities, and how GrapheneOS fares" (Thread opened on 18 May 2024), discuss.grapheneos.org/d/12848-claims-made-by-forensics-companies-their-capabilities-and-how-grapheneos-fares

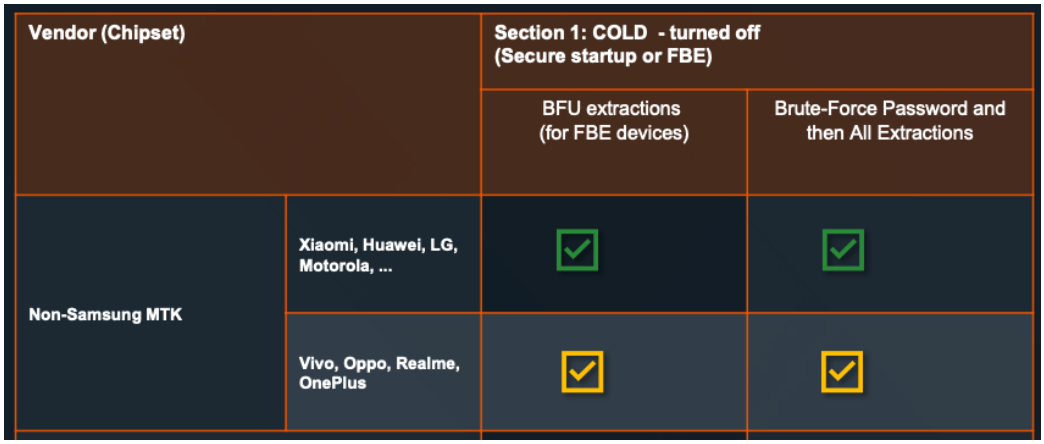


Figure 10: Cellebrite support matrix includes BFU extraction and password brute force

By 11:32 local time it appears the phone was successfully exploited by Cellebrite UFED, and initial indicators of UFED post-exploitation activity were observed on the device.

Timestamp (Local Time)	Event
2024-02-21 11:10 (approx.)	Slavisa turn off his phone and left it on the reception at the police station
2024-02-21 11:28:30	Traces related to non-standard boot
2024-02-21 11:31:08	Process crash associated with Cellebrite UFED unlock exploit.
2024-02-21 11:32:33	An **init** binary written to temporary folder on device with root privileges confirming successful exploitation.
2024-02-21 11:53:41	Device reboot. The device unlock code appears to have been obtained.
2024-02-21 11:56:07	Xiaomi File Manager app granted permission to install Android applications.
2024-02-21 12:01:32	ACCESS_RESTRICTED_SETTINGS reconfigured to enable accessibility service
2024-02-21 12:40:18	Logs show malicious NoviSpy app **com.accesibilityservice** running on the device.
2024-02-21 12:40:21	NoviSpy spyware attempts to establish a network connection to spyware server at **195.178.51.251:8080** from the app c**om.accesibilityservice**
2024-02-21 12:40:24	Kernel Panic when handling Linux USB HID device disconnection triggers reboot of the phone.
2024-02-21 12:48:52	The Cellebrite **falcon** binary is copied to temporary folder using ADB.
2024-02-21 12:50:02	Process crash associated with Cellebrite UFED usage.
2024-02-21 12:56:35	The init binary in the temporary folder is accessed again.
2024-02-21 13:38:55	Device rebooted again
2024-02-21 13:40 (approx)	Slavisa gets his phone back.

Table 9: Forensic traces for Cellebrite and NoviSpy use on Slavisa's phone

At 11:53 local time, approximately 30 minutes after Cellebrite unlock process was started, forensic traces indicate the device was successfully unlocked. The phone was rebooted and the authorities were able to

access the device and install the NoviSpy spyware apps. Later, at 12:48, the Cellebrite falcon binary was copied to the device and was likely used to switch the phone into Cellebrite Mode and perform a data extraction.

Amnesty International believes that the Cellebrite UFED system enabled the Serbian authorities to brute force, recover or bypass the phone lock code and install spyware on the device. The subsequent traces of the Cellebrite falcon are indicative of a Cellebrite UFED extraction being carried out after the initial UFED unlock, and installation of the NoviSpy spyware.

5.2.2 CELLEBRITE USED TO UNLOCK PHONE OF YOUTH ACTIVIST INFECTED WITH SPYWARE (CASE 5A)

In November 2024, Amnesty International identified a second case, where the phone of Nikola Ristić, a youth activist, was also unlocked with Cellebrite UFED and subsequently infected with the NoviSpy while in possession of Serbian authorities (more background on the case previously in Section 4.4.3).

Like Slavisa, Nikola was not asked to provide the pin or lock screen code for his Honor 20 Pro phone. The Honor 20 Pro uses a HiSilicon Kirin 980 chipset. The phone was had also not received Android security patches since August 2020, as such it was likely vulnerable to a significant number of security issues, both zero-days and n-days (known but unfixed vulnerabilities).

Forensic traces indicate that Cellebrite UFED was again used to exploit the phone before the spyware installation. The phone shows almost identical process crash logs as Slavisa's case, which Amnesty International associates with use of Cellebrite UFED. The phone appears to have been in an AFU ("After-First-Unlock") state when the phone was connected to the Cellebrite system. The log traces indicate exploitation of the device was successful, as certain log files were deleted from the devices.

Approximately one hour after the exploitation, the phone was accessed using the Android ADB protocol and the spyware applications were installed. Based on the limited log files available, it difficult to determine exactly was actions were taken on the device using Cellebrite UFED. Unlike with Slavisa, there is no evidence suggesting that ite was used to extract further data from the device infection with the NoviSpy spyware.

Time (Local Time)	Event
2024-11-02 01:56	Phone was switched on
2024-11-03 10:00 (approx.)	Nikola taken to the police station by BIA officers.
2024-11-03 10:48:44	Process crash associated with Cellebrite UFED unlock exploit. Logs deleted
2024-11-03 11:40:29	Installation of NoviSpy spyware app com.serv.services
2024-11-03 11:42:05	Installation of NoviSpy spyware app com.accesibilityservice
2024-11-03 13:30 (approx.)	Nikola is released by BIA.

Table 10: Traces of Cellebrite usage and NoviSpy installation on Nikola's phone

5.2.3 IMPLICATIONS OF CELLEBRITE USE TO ENABLE SPYWARE INFECTIONS

The cases suggests that the use of Cellebrite technology to enable spyware infection of phone appears to be an established and ongoing tactic, used by Serbian authorities to covertly hack human rights defenders and journalists.

As Slaviša and Nikola did not provide their phone passcodes, the NoviSpy spyware apps could only have been covertly installed on their phones through the use of a forensic tool like Cellebrite's UFED system capable of bypassing or recovering the lock code for the device.

Amnesty International did not find any public reference to specific Cellebrite features for modifying data or installing spyware apps on a targeted phone after unlocking. However, with access to a recovered pin code or the unlocked phone, it would be straightforward for the operator of Cellebrite UFED to perform further actions such as the installation of apps, including spyware, manually on a device after it is unlocked with Cellebrite. Direct access to a device can also lead to the modification of evidence, raising questions about the forensic integrity of the devices which have been unlocked using Cellebrite UFED.

Amnesty International is not aware of any previous cases with forensic confirmation of spyware installation after use of Cellebrite to unlock a device, although this is a frequently raised fear expressed by human right defenders who contact the organization following temporary device seizure. The potential of Cellebrite UFED products to enable spyware deployment highlights a serious danger enabled by advanced data extraction tools which are sold to thousands of police, intelligence, defense and military agencies world-wide.[102]

As methods for infecting phones remotely become more technically challenging or unfeasible, the use of "close access" methods, such as infection through physical access as described above, may become an increasingly prevalent threat to civil society. Some jurisdictions have proposed legislation allowing police to secretly break-in to the homes of suspects for the express aim of infecting devices with spyware, suggesting such practices are become more prevalent.[103]

Amnesty International wrote to Cellebrite with detailed questions about the UFED system and its capabilities which could allow for spyware to by installed. Cellebrite did not respond to the specific questions, but in a letter sent to Amnesty International ahead of the publication, it said that their "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."[104] Cellebrite also said that the company would investigate the findings from this report. "Should they be validated, we are prepared to impose appropriate sanctions, including termination of Cellebrite's relationship with relevant agencies."

5.3 CELLEBRITE USED ON ENVIRONMENTAL ACTIVISTS AND PROTESTORS

5.3.1 CELLEBRITE ZERO-DAY EXPLOIT USED TO EXTRACT PHONE OF ENVIRONMENTAL ACTIVIST (CASE 7)

Ivan Bjelić is a 26-year-old environmental activist and freelance journalist who is active in grass-roots campaigns against the expansion of lithium mining and extractive industries in Serbia. He has regularly experienced undue police scrutiny for his role in non-violent civil disobedience campaigns. In August 2024, Ivan was detained for four days following his arrest during mass protests, and road and rail blockades, against the opening of the Rio Tinto lithium mine in the Jadar valley. The charges involved a misdemeanour offence for violations of public peace and order. This was Ivan's seventh arrest in less than two years.

On 17 December 2023, Ivan was stopped while traveling to Belgrade on a bus and taken to the Ministry of Interior building in Belgrade, where he was questioned by police and BIA officers. The arrest occurred on the same day as a disputed general and local elections which sparked widespread anti-government protests.

During the several hours that he was held at the police station, officers presented Ivan with a formal written order, compelling him to provide his pin code and unlock his phone, a Xiaomi Mi 10T Pro. The authorities then retained his device for several hours while Ivan continued to be questioned in a separate room.

Shortly after the search, the officers told Ivan that they did not find anything incriminating, i.e., indications or evidence that he was engaged in attempts at "violent overthrow of constitutional order" or acts of terrorism, the charges on which he was brought in and released him. Ivan said that authorities have been accusing him of such serious charges for a long time in response to his campaigning.

Amnesty International forensically examined Ivan's phone following his release and identified forensic evidence confirming that Cellebrite's UFED product was used to gain elevated system privileges on his

[102] Cellebrite, About, https://cellebrite.com/en/about/ (accessed on 20 November 2024).
[103] DW, "Will German police get to do secret house searches?", 9 August 2024, https://www.dw.com/en/will-german-police-get-to-do-secret-house-searches/a-70154300
104 Email from Cellebrite to Amnesty International, 13 December 2024. On file with Amnesty International.

phone, allowing the authorities to extract all data from his device. A summary of Amnesty International's forensic findings for "Ivan" are included in Annex 2. As was the case with all other activists and journalists whose devices were accessed through Cellebrite, Ivan was not formally charged with any crime.

In this case, the authorities presented Ivan with a search warrant and also asked him to enable access to his phone to allow for the search to take place. While, through the lens of domestic legal procedure, this could be considered a legal use of Cellebrite's digital forensic technology, it raises serious questions about the legitimacy of the use. Amnesty International considers that the use of advanced forensic software and serious terrorism and sedition charges, against people solely for exercising their human rights to expression and peaceful assembly can never be a legitimate aim, and therefore might be in violation of human rights law.

5.3.2 SUSPECTED USE OF CELLEBRITE PRODUCTS TO INSPECT AND SEARCH PHONES OF ENVIRONMENTAL PROTESTORS

Amnesty International also believes that Cellebrite forensic products were among the digital forensic tools used to inspect and search telephones of dozens of other activists whose devices were temporarily seized when they were questioned by the police following the anti-lithium mine protests in July and August 2024.

Although the activists interviewed were called in for informational interviews, rather than as suspects in connection with a criminal offence, they were forced to surrender their devices, provide police with PIN codes or physically unlock their telephones, to enable a forensic search. At least three individuals, including a lawyer who witnessed the searches in the police premises, described in detail the process and equipment, which closely resembled components of Cellebrite's UFED product line which is widely used by the police in Serbia.

The procedure as described is in line with Serbia's Criminal Procedure Code and relevant court rulings, which found that the inspection ("uvidjaj"), search ("pretres") and expert analysis ("veštačenje") of mobile devices that have been temporarily seized did not represent a "special evidentiary action," including secret communications surveillance (see Chapter 7). While procedurally in line with laws in Serbia, using such intrusive digital surveillance measures against activists engaging peacefully on issues of public interest raise numerous questions about whether such interference complies with people's right to privacy and freedom of expression and association, which are inextricably linked in the digital age.[105]

5.4 NORWEGIAN DONATION OF CELLEBRITE TO SERBIA'S MINISTRY OF INTERIOR

Cellebrite technology has been in use in Serbia since 2019. As a part of multi-year assistance to Serbia's Ministry of Interior from 2017-2021, the Norwegian government provided it with considerable support, including hi-tech equipment and training, to strengthen the Ministry's capacity to fight d crime.[106] This project, which was worth at least USD 678,688 included the procurement of the full range of Cellebrite UFED technology, the system for forensic analysis of mobile devices and computers, and the licencing of 30 National Crime Technical Centre (NCTC) staff in basic and advanced digital forensics.[107]

The Norwegian Embassy records show that the project was a part of the broader package of assistance envisaged to help Serbia meet the requirements for integration into the EU and, specifically, those from Chapter 24: Justice, Freedom and Security, including "full harmonisation with the acquis in the area of developing criminal intelligence system" and " cooperation in the Field of Drugs."[108] According to the Memorandum of Understanding concluded in 2019 between the Norwegian Embassy, Serbia's Ministry of Interior and the United Nations Office for Project Services (UNOPS), the completion of the project was to

[105] University of Novi Sad, Prikupljanje elektronskih dokaza iz mobilnog telefona u praksi vrhovnog kasacionog suda republike Srbije [Collection of electronic evidence from a mobile phone in the case-law of the supreme court of cassation of the republic of Serbia], 2020, https://hrcak.srce.hr/file/367372 (in Serbian).
[106] Royal Norwegian Embassy in Belgrade, Additional grants and Addendums to previous agreements approved in 2021, August 2022, https://www.norway.no/contentassets/0cf812d763e046a29a4c081850c1c364/embassy-supported-projects-2010---2021---aug-2022.pdf
[107] According to the Final Project Report, the training aspect of the grant was later cancelled at the request of the beneficiary. Support of the Kingdom of Norway to the Ministry of Interior of the Republic of Serbia, 29 October 2021.
[108] Royal Norwegian Embassy in Belgrade, Additional grants and Addendums to previous agreements approved in 2021 (previously cited).

"lead to the establishment of a systemic mechanism to tackle drugs in compliance with the European standards, harmonization with the acquis in the field of fight against terrorism and cybercrime."[109] According to the agreement signed between the Norwegian Ministry of Foreign Affairs and UNOPS (represented by the Norwegian Embassy in Belgrade and UNOPS Serbia Operations Centre, respectively) on 11 December 2017 and email exchanges between the Embassy and UNOPS obtained by Amnesty International though the Freedom of Information Act, UNOPS was to determine technical specifications for and the list of the necessary equipment and organize the procurement and delivery of items.[110] In 2018, the Norwegian government temporarily stopped the delivery of ICT/Cellebrite UFED.[111] In the suspension letter addressed to the UNOPS, the deputy head of the Norwegian Embassy in Belgrade noted that "Norway cannot engage in any sort of support to projects that could increase the risk of sensitive data failing [sic] in the wrong hands."[112] In the letters it is not clear what the specific concerns were, but following a commitment from the Serbian Ministry of Interior to "cooperate on information and security," UNOPS eventually delivered the equipment to the Ministry on 21 June 2019.[113] In an email to Amnesty International, UNOPS explained that this request was the result of the Embassy's concern regarding information and cyber security within the MoI [Ministry of Interior] and agencies under their responsibility," and that, in April 2019, "the Embassy informed UNOPS that it can deliver the equipment due to positive response from the MoI to cooperate on information security," after which time, the UNOPS delivered the equipment.[114]

The project records of the Norwegian Ministry of Foreign Affairs, which Amnesty International obtained through the Freedom of Information Act, indicate that this donation in hardware and software was essential in setting up a system for forensic analysis of mobile devices and computers at the Serbian Ministry of Interior. While the Cellebrite UFED donation aimed to improve the Ministry's capacity to fight organized crime and corruption, Amnesty International's research indicates that the Serbian authorities have also used Cellebrite to unlawfully surveil and intimidate critical activists, human rights defenders and independent journalists.

It is not clear whether the Norwegian Embassy or UNOPS Serbia, which managed the projects and conducted the procurement for the equipment, conducted a due diligence process to assess and mitigate potential risks of this assistance to human rights; however, as outlined above, documents show that the Norwegian Embassy was aware of some risks. Furthermore, according to the Final Project Report prepared by UNOPS, in its role of the implementing partner for the grant, the portion of the grant relating to specific training and licencing of the Ministry staff was cancelled at the request of the Ministry of Interior and it is unclear if the staff in charge of the new sophisticated and highly invasive equipment was trained in the lawful use of Cellebrite and other digital forensic equipment.[115]

This Norwegian assistance was intended to contribute to Serbia's efforts to meet the requirements for EU accession. Given the sensitive nature of the equipment and the potential for its misuse, the project should have included a component on the harmonization of Serbia's legislation and regulatory framework governing the acquisition, use and oversight of secret communication surveillance, including digital forensics, for law enforcement purposes with the EU acquis and regular independent monitoring.

The project was a missed opportunity for the Norwegian government to couple the assistance with human rights guarantees so this assistance did not have an unintended adverse impact on human rights in Serbia. Indeed, the recent evaluation of Norway's development aid provided globally between 2018-2022 indicated that a large proportion of the Norwegian Agency for Development Cooperation (NORAD) projects had weak or completely missing human rights risk assessments and that only a third included an analysis or a report on the risks noted following the implementation.[116]

An obligation to promote and protect human rights, including through its international development aid is one of the guiding principles of Norwegian foreign assistance. The 2015 Report to Storting states that when considering aid, the Norwegian government will consider "the recipient country's willingness to govern in accordance with principles of human rights, democracy and rule of law," and that "developments in these

[109] Memorandum of Understanding between the Norwegian Embassy, Serbia's Ministry of Interior and UNOPS.
[110] Agreement between the Norwegian Ministry of Foreign Affairs and the United Nations Office for Project Services regarding "Support of the Kingdom of Norway to the Ministry of Interior of the Republik of Serbia" PTA Number SRB-17/0003, 11 December 2017.
[111] Letter from the Royal Norwegian Embassy to United Nations Office for Project Services (UNOPS), 21 August 2018.
[112] Letter from the Royal Norwegian Embassy to United Nations Office for Project Services (UNOPS), 21 August 2018.
[113] Letter from the Royal Norwegian Embassy to the United Nations Office for Project Services (UNOPS), 2 April 2019.
[114] UNOPS Serbia, Multi-country office Director letter to Amnesty International, 12 December 2024. On file with Amnesty International.
[115] UNOPS, Final Project Implementing Report 11 December 2017- 31 May 2021.
[116] Norwegian Agency for Development Cooperation (Norad), Oversendelsesnotat: Evaluering av tverrgående tema i utviklingssamarbeidet (Rapport 5/2024) [Submission note: Evaluation of cross-cutting theme in development cooperation (Report 5/2024)], 23 August 2024, https://www.norad.no/globalassets/filer/evaluering/oversendelsesnotat_evaluering-av-tverrgaende-tema-i-utviklingssamarbeidet.pdf (in Norwegian)

areas will be significant in determining whether or not Norway can provide" such support.[117] The document sets three priority areas, including individual freedom and public participation, emphasizing specifically the rights under threat, such as the right to freedom of expression, freedom of assembly and association and support for human rights defenders. It also sets a commitment for the Norwegian aid to set "clear requirements for recipients...to take steps to promote human rights, democracy and the rule of law."[118]

Amnesty International wrote to the Norwegian Ministry of Foreign Affairs to request information as to whether the Norwegian Embassy or the UNOPS, the local partner, conducted any due diligence to understand potential risks to human rights associated with the donation of Cellebrite UFED. In a response to Amnesty International on 11 December, 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 to 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." [119]

The Ministry also said that UNOPS, which was responsible for all project activities, including "investigating any financial irregularities in the Project", is expected to conduct "a thorough investigation of the alleged misuse."[120] "The UNOPS Internal Audit and Investigation Group (IAIG) shall keep the Foreign Service Control Unit informed of the progress and outcome of its investigations. Norwegian authorities will follow up the matter with UNOPS as well as with Serbian authorities."[121]

However, in an email to Amnesty International, UNOPS office in Serbia said that the "forensic equipment was procured in accordance with UNOPS rules and regulations, through an open international competition," and that "to the extent feasible, UNOPS was monitoring the effects of interventions during the life cycle of the Project and identified indicators of positive contribution to the set objectives."[122]

UNOPS also added that the "procurement of the forensic equipment contributed to the renewal of the accreditation of the National Forensic Centre Laboratories during the supervisory visit of the European Network of Forensic Science Institutes' Accreditation Body," which UNOPS considered as "indicators of positive contribution [that] also include human rights dimensions."[123] In the email, UNOPS did not explain whether or not they conducted any human rights impact assessment to determine any possible adverse affects.

[117] Report to the Storting (white paper) 2014–2015 Opportunities for All: Human Rights in Norway's Foreign Policy and Development Cooperation law, https://www.regjeringen.no/contentassets/261f255d028b42cab91ad099ee3f99fc/en-gb/pdfs/stm201420150010000engpdfs.pdf
[118] Report to the Storting (white paper) 2014–2015 Opportunities for All: Human Rights in Norway's Foreign Policy and Development Cooperation law, pp. 10-11, https://www.regjeringen.no/contentassets/261f255d028b42cab91ad099ee3f99fc/en-gb/pdfs/stm201420150010000engpdfs.pdf
[119] Letter from the Royal Norwegian Ministry of Foreign Affairs, Directorate for European and International Trade, to Amnesty International, 11 December 2024. On file with Amnesty International.
[120] Letter from the Royal Norwegian Ministry of Foreign Affairs, Directorate for European and International Trade, to Amnesty International, 11 December 2024. On file with Amnesty International.
[121] Letter from the Royal Norwegian Ministry of Foreign Affairs, Directorate for European and International Trade, to Amnesty International, 11 December 2024. On file with Amnesty International.
[122] UNOPS Serbia Multi-country Office Director letter to Amnesty International, 12 December 2024. On file with Amnesty International.
[123] UNOPS Serbia Multi-country Office Director letter to Amnesty International, 12 December 2024. On file with Amnesty International.

6. SURVEILLANCE IS SILENCING CIVIL SOCIETY IN SERBIA

6.1 THE CHILLING EFFECT

Digital surveillance technologies, including spyware, and widely used but highly invasive digital forensic tools, such as Cellebrite, may be used to target and intimidate human rights defenders and journalists, silence dissent and sanction criticism. The targeted surveillance interferes with the right to privacy, freedom of expression, and freedom of peaceful assembly and can have a profound 'chilling effect'[124] on civil society as a whole.

Activists and journalists in Serbia who have been subjected to invasive surveillance 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. They understood that the authorities used it as a tactic of intimidation and fear.

"Goran" explained that finding out that he was targeted by Pegasus was "horrifying." 'I knew that the attack was not directed against my organization, but me personally. They [the authorities] wanted to find something compromising from my personal life and use it against me. This realization was absolutely horrifying. We all have something in our personal lives that could be seen in a different light if it goes public."[125]

"Slavisa" said that being a target of secret surveillance, in his case through the NoviSpy spyware and digital forensic tools that could access everything on his mobile device, had a huge effect on him and his family and created a persistent sense of fear. "I am always looking over my shoulder now. I worry that they may have found something compromising on my phone and that that information could end up with some criminal gangs who could use it for blackmail. This has happened before."[126] He said that even the realization that the State Information Agency (BIA) may be interested in one's work was in itself incredibly scary.

For "Aleksandar," being targeted by Pegasus created a feeling of vulnerability. "My privacy was invaded, and this completely shattered my sense of personal security. It caused a huge anxiety…I felt a sense of panic and became quite isolated."[127] "Aleksandar" told Amnesty International that the attack had a serious impact on his mental health.

---

[124] The term "chilling effect" has been defined as "the negative effect any state action has on natural and/or legal persons, and which results in pre-emptively dissuading them from exercising their rights or fulfilling their professional obligations, for fear of being subject to formal state proceedings which could lead to sanctions or informal consequences such as threats, attacks or smear campaigns." See Laurent Pech, The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, The Rule of Law, and Fundamental Rights in the EU, March 2021, https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect, p. 4.
[125] Interviews with "Goran", conducted on xx May 2024 and 16 September 2024.
[126] Interview with "Slavisa", conducted on 21 August 2024.
[127] Interview with "Aleksandar", conducted on 19 September 2024.

Apart from creating a sense of personal vulnerability, digital surveillance also had a significant impact on the professional lives of the people targeted. It forced some to self-censor or stay away from controversial issues altogether. Others considered resigning from their positions or disengaging from activism, and some developed a deep distrust of digital technologies and social media.

6.2 SELF-CENSORSHIP

One of the most notable consequences of persistent state repression, including digital surveillance is that it creates an environment of self-censorship. According to Slavisa, a number of his journalist colleagues whose telephones were confiscated by the police or BIA decided to be more cautious or even completely avoid reporting on controversial topics. According to a survey conducted in December 2023, 53.8% of journalists polled said that they had been in a situation where they decided not to report on a topic, due to a combination of factors, including fear for personal safety, political pressure and government interference.[128]

For "Goran", the impact was clear. "This is an incredibly effective way to completely discourage communication between people. Anything that you say could be used against you, which is paralyzing at both personal and professional levels. We are all in the form of a digital prison, a digital gulag. We have an illusion of freedom, but in reality, we have no freedom at all. This has two effects: you either opt for self-censorship, which profoundly affects your ability to do work, or you choose to speak up regardless, in which case, you have to be ready to face the consequences."[129]

However, many people who are the victims of surveillance do not fear only personal retribution for the work they do but worry about the risks this brings for the people close to them – their friends, family, colleagues, their sources and people from their social networks.

After learning that he was targeted, Slavisa said he was very concerned that some of his sources could have been compromised and had to change the way in which he does research for his articles and engages 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."[130]

"Goran" told Amnesty International of his fears for others with whom he is communicating were affected. "What about my 75-year-old parents? What about my child? Will they be affected by the knowledge that I was a target of such an attack? Will they be reluctant to engage with me on the phone? One of the worst effects of an attack by Pegasus is that you become practically excommunicated from society. This was the case in Armenia, where Pegasus was routinely used and people affected were completely ostracized. Others become reluctant to communicate with them. Once it is known that you were the target of such an attack, people don't want to speak with you. It is as if you have a communicable disease, and you are contagious."[131]

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression highlighted how targeted surveillance does not only affect the targets but also their networks of contacts. "In the environment subject to rampant illicit surveillance, the targeted communities know of or suspect such attempts at surveillance, which in turn shapes and restricts their capacity to exercise the right to freedom of expression, association…Interference with privacy through targeted surveillance is designed to repress the exercise of freedom of expression."[132]

6.3 DISENGAGEMENT

Another major consequence of invasive digital surveillance is a deep distrust of digital technology and reluctance to use it to communicate or facilitate activism. It can cause an erosion of trust and weaken protest movements. In some cases, human rights defenders decide to completely withdraw from activism.

---

[128] Council of Europe, Journalists' Association of Serbia, the Independent Journalists' Association of Serbia "Safety of Journalists, Behind the headlines: Threats, attacks and pressure on journalists in Serbia," February 2024, https://rm.coe.int/hf42-research-threats-attacks-onjournalists/1680aee322

[129] Interviews with "Goran", conducted on xx May 2024 and 16 September 2024.

[130] Interview with "Slavisa", conducted on 21 August 2024.

[131] Interviews with "Goran", conducted on xx May 2024 and 16 September 2024.

[132] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights,* 28 May 2019, UN Doc. A/HRC/41/35, para. 21.

Although he himself remained steadfast and determined to stay engaged, Ivan explained that the government's repressive measures, such as digital surveillance and frequent arrests, have a significant impact on activism and youth engagement in Serbia. "It is increasingly difficult to encourage and mobilize young people to be a part of activist groups. People are afraid of being compromised and not being able to get a job later, while others fear that they could lose the jobs they have."[133]

"Goran" was one of the activists targeted with Pegasus. 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 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."[134]

Aleksandra, an environmental activist who was called for questioning and kept in custody for nearly four hours after the anti-lithium protests in August 2024, over her post about the blockades and sit-ins on social media decided to disengage almost entirely from the movement.[135] "When my young son found out that I was questioned by the police and possibly surveilled, he completely freaked out and asked me to stop my public engagement over these issues. When they got to my child, this was a red line for me," she told Amnesty International.[136]

"Boris", an environmental activist from Belgrade, remains active despite the weeks-long ordeal he went through over the summer, when police searched his apartment and seized his phone after he organized an anti-lithium protest. "Sure, I am certainly little more careful, but this has not reduced my will to stay engaged. I don't think I have an alternative. I can't stay in my little bubble content with my comfortable life and ignore what is happening around me. Even if you try to ignore it, politics inevitably enters your life - we all have to drink the same water, breathe the same air and send our children to schools where they can be victims of mass shootings. I simply can't stay out of it. My life is here, and I don't want to be forced to leave."

In addition to the personal impact, surveillance had a profound effect on the organizations to which targeted individuals belong. Both Krokodil activist and "Goran" recounted having to spend inordinate amount of time improving digital safety and security inside of their organizations and finding different ways to communicate with external partners. For the organizations already facing numerous Strategic Lawsuits against Public Participation suits (SLAPP; see glossary) filed by government officials and persistent smear campaigns, having to deal with digital security issues was yet one more distraction from doing the core work. "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," Krokodil activist told Amnesty International.[137] Another activist, "Branko", also felt that digital surveillance was depleting civil society and activists. "The authorities have learnt how to use all these measures to create false emergencies and very effectively distract us from real issues. On surface, it looks like a normal life, but there is a quiet repression underneath."[138]

[133] Interview with "Ivan" conducted on 16 August 2024
[134] Interviews with "Goran", conducted on xx May 2024 and 16 September 2024.
[135] Interview with Aleksandra, 12 October 2024
[136] Interview with Aleksandra, 12 October 2024
[137] Interview with Milena, 15 October, Belgrade.
[138] Interview with Branko, 16 October 2024, Belgrade.

7. NATIONAL LEGAL FRAMEWORK ON DIGITAL SURVEILLANCE IN SERBIA

The covert nature of most digital surveillance, including communications surveillance, presents a serious risk to the protection of human rights – in particular, to the right to privacy. Given the potential for serious infringement of peoples' rights, such surveillance may only be conducted if it is absolutely necessary and under strict conditions defined by law with appropriate safeguards and oversight.

Serbia's Constitution does not explicitly mention privacy rights, but it provides guarantees for the confidentiality of correspondence and other forms of communication (Article 41) and personal data protection (Article 41). The Constitution allows for limited restrictions of the privacy rights of data subjects, only for a limited time and based on a court decision, in only two instances: if this is necessary for purposes of a criminal procedure (i.e., identifying, preventing, and investigating serious criminal offences) or for the protection of national security.[139] Secret communication surveillance, which includes surveillance of communication carried out by telephone or other technical means, of email or letters and other shipments is regulated - under different names - by several different laws, including Law on Criminal Procedure Code, Law on Police, Law on Security Information Agency (BIA), Law on Electronic Communications, as well as Law on Military Security and Information Agency and Law on Military Intelligence Agency (however, the activities of the latter two are not covered by this research).

Serbia's Criminal Procedure Code does not use the term "digital evidence", but it considers computer data which could be used as evidence in criminal proceedings as a document ("isprava").[140] Surveillance of communications, including digital data, could be obtained through ***general evidentiary measures***, such as ***inspection*** and ***searches*** of mobile devices or other equipment which store digital records. These measures are typically not secret and are conducted with the knowledge of and in the presence of a suspect.[141]

Secret communication surveillance, as its name suggests, is conducted covertly and is covered by different terms depending on which body is conducting it. Secret communications surveillance to gather evidence for criminal procedure could be applied by the Security Information Agency (BIA) or the police, in which case these measures are considered ***special evidentiary measures*** and are regulated by the Criminal Procedure Code. Police can also conduct secret communications surveillance in order to arrest a suspect, but in this

[139] According to Article 41 of the Constitution, the confidentiality of correspondence and other means of communication is inviolable and exceptions are permitted only for limited periods and based on judicial approval, if they are deemed necessary to conduct criminal proceedings or protect the national security of the Republic of Serbia, in a manner stipulated by the law. The derogation are permitted only: (1) for a limited period, (2) on the basis of a court decision, (3) if it is deemed necessary for the conduct of criminal proceedings or in order to protect the Republic of Serbia and (4) in a manner regulated by law.
[140] See Milana Pisarić, "Collection of electronic evidence from a mobile phone in the case-law of the Supreme Court of Cassation of the Republic of Serbia", Criminalistic theory and practice, Vol.7, No.2/2020., 2020.
[141] Criminal Procedure Code, Article 156.

case, the surveillance is called a *measure of targeted search* and is considered one of the police powers regulated by the Law on Police. In addition, BIA can also conduct secret communications surveillance if this is necessary for the protection of national security.

The term "spyware" is not explicitly mentioned in or regulated by any law in Serbia. However, given the scale of spyware used to target civil society, it is possible that the authorities consider the use of spyware to be a legitimate means of covert communications surveillance or other special evidentiary measures or special measures, which can be applied with judicial oversight (as described below). The individual measures and actions related to digital surveillance are discussed in more detail below.

7.1 SPECIAL EVIDENTIARY MEASURES

Under Serbia's legislation, digital surveillance per se is not explicitly defined. However, covert data collection, including covert communications surveillance, falls under the so-called "special evidentiary measures" which are regulated by Serbia's Criminal Procedure Code.[142]

The law lists criminal offences for which special evidentiary measures could be applied (Article 162) and sets conditions under which such measures can be applied and special approval procedures for these measures. Accordingly, law enforcement agencies can apply special evidentiary measures only if (i) there are grounds for suspicion that the person targeted has committed or is preparing to commit one of the serious criminal offences listed in the law, and (ii) when other means of evidence collection are not available and would cause disproportionate difficulties or grave danger.[143] In order to apply the measures, the bodies authorized to use them have to assess whether the same result could be achieved in a manner which is less restrictive of the rights of citizens.[144]

The Criminal Procedure Code also sets conditions under which such measures can be applied and special approval procedures in such instances. Law enforcement agencies can only use these exceptional powers with a court-issued warrant, based on the request of the public prosecutor. Among other information – the warrant has to include details of the criminal offence, grounds for suspicion, and the scope and duration of special measures, as well as the phone number or the address of the suspect.[145]

In Serbia, special evidentiary measures could be used by the police, Security Information Agency (BIA) and Military-Security Information Agency (VBA). This research focuses specifically on the measures of the police and BIA. The data collected through special evidentiary measures can be used as evidence in criminal proceedings.[146]

7.2 TARGETED SEARCH MEASURES

The Law on Police provides for the Targeted Search Measures. Targeted Search Measures refer to special measures applied by police in order to arrest or detain a suspect. Police can apply these measures only if (i) the suspect is subject to an arrest warrant and (ii) the suspect cannot be apprehended by other means or when other means would cause disproportionate difficulties.[147] These exceptional measures are listed as one of the police powers and can be applied only with the approval of the President of the Supreme Court of Cassation on the request of the Police Director.[148] The approved measures can be applied for six months, with a possibility of a six-month extension. The data collected through targeted search measures are used to aid the arrest or detain a suspect and cannot be used in criminal procedure.

[142] Criminal Procedure Code of Republic of Serbia, Section III, Articles 161-187, Combined version. Criminal Procedure Code defines six special evidentiary actions: covert interception of communications (Arts. 166-170); covert surveillance and audio and video recording (Arts. 171-173); simulated [business] deals (Arts. 174-177); computer search of data (Arts. 178-180); controlled delivery (Arts. 181-182); and undercover investigator (Arts. 183-187).
[143] Criminal Procedure Code, Article 161, Para 1 and Para 2.
[144] Criminal Procedure Code, Article 161, Para 3.
[145] Criminal Procedure Code, Article 167. The duration of the interception is limited to three months, with a possible extension by a further three months. In cases of organized crime and war crimes, two extensions of three months are possible.
[146] Criminal Procedure Code, Articles 161 and 163.
[147] Law on Police of Republic of Serbia, Article 60.
[148] Law on Police of Republic of Serbia, Article 60, Para 2.

7.3 SURVEILLANCE FOR THE PURPOSE OF NATIONAL SECURITY

The BIA carries out tasks that relate to national security; namely, the discovery and prevention of activities that threaten to undermine the constitutional order; and the acquisition, processing and analysis of security-intelligence information relevant to national security.[149]

According to the Law on BIA, in carrying out its tasks, the BIA can apply four "special measures" that deviate from the principle of inviolability of correspondence secrecy and other communications: (1) covert surveillance and recording of communications regardless of the technical means, as well as surveillance of electronic and other addresses; (2) covert surveillance and recording of communications in public places, places of limited access and premises; (3) statistical electronic surveillance of communications in information systems with the aim of gathering data on communications or locations of used mobile devices; and (4) computer searches of processed personal and other information and its comparison with data gathered in the application of measures from points (1) to (3).[150]

In addition to special measures such as covert surveillance and recording of communications, the BIA can conduct secret surveillance and recording of places, premises and objects, including devices for automatic data processing and equipment on which electronic records are stored or can be stored.[151] Special measures could be used against an individual, group or organization only if: (1) there is a reasonable suspicion that the individual, group or organization is engaged in or preparing activities threatening the security of the Republic of Serbia and (2) the circumstances of the case indicate that other measures would not be sufficient to detect, prevent or prove these activities or that their application would result in disproportionate difficulties or grave danger.[152]

The determination of special measures should include an assessment of whether the same result could be achieved in a manner that is less restrictive to citizens' rights to the extent necessary to satisfy the purpose of the restriction in a democratic society.[153] The application of these measures requires a warrant signed by the president of the Higher Court in Belgrade, or a designated judge, upon request of the BIA Director.[154] The duration of the special measures is limited to three months, with the possibility of a three-month extension three times.[155]

In addition to carrying out the tasks from the Law on BIA, in special circumstances, BIA operatives can take over and directly carry out tasks which are under the purview of the Ministry of Interior.[156] In contrast to most European countries where police and security services are clearly separated, BIA officials can still exercise police powers, albeit in cases of serious criminal offenses.[157]

The data collected for the purposes of national security cannot be used in criminal proceedings but could be referred to a responsible prosecutor who could initiate a separate gathering of evidence.

7.4 INSPECTION AND SEARCHES OF DIGITAL DATA

The Criminal Procedure Code considers computer data which could be used as evidence in criminal proceedings as a document stored on a device. To lawfully obtain the content of digital data that could be used as evidence, law-enforcement agencies can temporarily seize[158] and search[159] the devices on which such data are stored. The collection, processing and analysis of digital data using digital forensics tools are considered *general evidentiary measures* - as opposed to special evidentiary measures, which cover secret communications surveillance. This indicates that the Serbian law does not seem to consider the search of

[149] The Law on Security Information Agency, Article 2.
[150] The Law on Security Information Agency, Article 13.
[151] The Law on Security Information Agency, Article 13, Para 2.
[152] The Law on Security Information Agency, Article 14, Para 1.
[153] The Law on Security Information Agency, Article 14, Para 2.
[154] The Law on Security Information Agency, Article 15, Para 3.
[155] The Law on Security Information Agency, Article 15a.
[156] The Law on Security Information Agency, Article 16.
[157] Law on BIA, Article 12 specifies that BIA can use police powers when detecting, monitoring, documenting, preventing, suppressing and interrupting the activities of organizations and persons aimed at committing organized crime and criminal offences with a foreign element, domestic and international terrorism and the most serious forms of criminal offenses against humanity and international law and against the order and security of the Republic of Serbia.
[158] Criminal Procedure Code, Article 147.
[159] Criminal Procedure Code, Article 152.

digital data on the phone as intrusive on the right to privacy as secret surveillance, for which laws provide additional safeguards.

In pre-investigative procedure, police can temporarily seize[160] and undertake an ***inspection***, including forensic inspection, of the device. An inspection takes place in order to establish, or clarify through observation, a fact necessary for a criminal investigation.[161] In this process, the suspect must provide police with access to the device.[162] Criminal procedure code specifically refers to access to the seized "item"; however, in the context of the phone searches, according to interviewees, the police in practice equates the obligation to provide access to the device as an obligation to either reveal their PIN code or physically unlock the device.[163]

During the inspection, however, police can only view, but not seize any digital data. In order to actually obtain such data and use it as evidence in court, police, with the approval of a judge, can conduct a ***search*** of the device.[164] The search of a telephone is carried out - often with the assistance of forensic experts - if it is likely that it could reveal (digital) traces of a criminal act.[165] The search is more invasive than the inspection as it allows police to determine and access the content of the telephone's memory and SIM card, including the content of messages, photographs, videos, etc. In this instance also, the suspect must provide access to the device, or face a fine of up to 150,000 RSD (1280 euro).[166] Despite the fact that the inspection and search of telephones that include large amounts of personal data by means of digital forensic technology is undoubtedly invasive of personal privacy, Serbia's courts ruled that these measures are not considered special evidentiary measures.[167]

7.5 DATA RETENTION

The Criminal Procedure Code stipulates that data collected through special evidentiary measures that are not used to initiate criminal proceedings within six months from the time the prosecutor became acquainted with the materials, must be destroyed.[168] The destruction ruling is approved by a judge, but the Criminal Procedure Code does not provide any timeline for this. A judge can inform the person who was subjected to special evidentiary action of the decision to dispose of the data if this would not jeopardize the investigation, but this is not a legal requirement.[169]

Any evidence collected contrary to the Criminal Procedure Code cannot be used in criminal proceedings and is sealed until the end of criminal proceedings and subsequently disposed.[170] The data collected by police through targeted search measures can never be used in criminal proceedings and are destroyed at the end of the police investigation. The data are destroyed by the president of the court of cassation who has to prepare a report on the disposal.[171]

The data that are used in criminal proceedings are included in the criminal case file and kept by a responsible court. Concluded cases are kept in court offices for no longer than two years and are then moved to the archives. The timelines for the disposal of the data depend on the penalty in a given case and can range from 10-30 years. It is not clear, however, how long can BIA keep the data collected through special measures for the cases of national security because these procedures are regulated by BIA bylaws that are not publicly available. The data collected through special evidentiary measures, in particular through secret communications surveillance, are considered classified and are kept separately.

---

[160] Criminal Procedure Code, Article 147.
[161] Criminal Procedure Code, Article 133.
[162] Criminal Procedure Code, Article 135.
[163] Criminal Procedure Code, Article 135. It is not only the police that interprets this provision as an obligation to unlock the device or reveal the PIN code, but even some of the lawyers Amnesty International interviewed had a similar view. Also, see Pisarić, pg. 41. Other legal experts strongly disagree with such interpretation arguing that it undermines the principle of self-incrimination.
[164] Criminal Procedure Code, Article 152, Para 3.
[165] Criminal Procedure Code, Article 152, Para 1.
[166] Criminal Procedure Code, Article 148, Para 2.
[167] Milana Pisarić, "Collection of electronic evidence from a mobile phone in the case-law of the Supreme Court of Cassation of the Republic of Serbia," Criminalistic theory and practice, Vol.7, No.2/2020., 2020.
[168] Criminal Procedure Code, Article 163, para 1.
[169] Criminal Procedure Code, Article 163, para 2.
[170] Criminal Procedure Code, Article 84.
[171] Law on Police, Article 60.

7.6 OVERSIGHT OVER SPECIAL MEASURES

Courts, independent state institutions, such as the Data Protection Commissioner and Ombudsman's Office, and the National Assembly can exercise control and oversight over special measures employed by law enforcement and security agencies in Serbia.[172]

Judicial control is exercised primarily in advance of the use of the measures (*ex-ante* scrutiny), as only the court can approve a decision to use special evidentiary measures. The court can also monitor the process, and it is the judges who can authorize the disposal of materials that are not used for criminal proceedings and are collected unlawfully.

The Ombudsman's Office can also oversee the use of special evidentiary measures on their own initiative or upon a complaint of citizens.[173] The Ombudsman can access the offices of law enforcement and security agencies and request any information, including secret information, for inspection.[174] If the inspection finds any gaps, the Ombudsman can issue recommendations to address them, which has to be done within two months, and ultimately could ask public prosecutors to press charges against officials who violated the law.[175]

The Serbian Data Protection Commissioner can oversee the work of any institution that processes the personal data of citizens, including ensuring that the data are kept securely, that access to data is strictly regulated and that the data are not used for other purposes.[176] The Commissioner can request any information from law enforcement and security agencies and can issue warnings in case of violations.[177] It can also request the agencies to stop processing data.

Serbia's National Assembly Committee for control over security services can oversee the legality of use of special measures, including secret gathering of data (*ex-post* scrutiny).[178] In addition to external mechanisms of oversight, internal control units within the police and BIA also have the authority to monitor whether all special measures are conducted lawfully. However, these internal control units are not independent in their operations and report to the Minister of Interior and the BIA Director, respectively, raising questions about their effectiveness and impartiality.

If a person suspects that they were a target of unlawful surveillance, they can address any of the mechanisms of internal and external control and oversight. As a first step, the person can request information about whether their personal data are being processed or if they are under special measures from the body which is suspected of being engaged in unlawful surveillance, including their internal control units.[179] Serbian Law on Data Protection allows for these bodies, however, to withhold such information in specific circumstances, including if that would jeopardise investigations or if this is necessary to protect national security.[180]

After addressing the bodies or their internal control units, the person who suspects that their rights have been violated can also write an application or file a complaint to the Data Protection Commissioner[181] and the Ombudsman's Office. Neither institution can inform the person if their data are being processed, but could investigate whether the bodies processing the data, i.e., engaging in secret communications surveillance, for example, are doing so lawfully.[182] The Data Protection Commissioner and the Ombudsman's Office can review the legality of special investigative measures based on a request or independently (ex officio) if they become aware of potential violations.

---

[172] Law on confidential data determines who, and under which conditions, could access classified information. Ombudsman, Data Protection Commissioner and members of the parliamentary committee for the control and oversight over security and defense sectors have the authority to oversee the application of special measures but must undergo security clearance and obtain a certificate to access classified information. See Arts. 37-39 of the Law on Confidential Data of Republic of Serbia.
[173] Zakon o Zaštitniku gradjana, Article 19 Službeni glasnik RS, 105/2021,
[174] Zakon o Zaštitniku gradjanja, Article 24, Para 1
[175] Zakon o Zaštitniku gradjana, Article 23. Para 2
[176] Data Protection Law, Article 78
[177] Data Protection Law, Article 79
[178] Article 16, Para 1, item 4 of the Law on foundations of structure of security services (Zakon o osnovama uredjenja službi bezbednosti)
[179] Data Protection Law, Article 27.
[180] Data Protection Law, Article 28.
[181] Data Protection Law, Article 35.
[182] Data Protection Law, Article 35, Para 3.

7.7 LACK OF NECESSARY SAFEGUARDS

As seen above, legislation in Serbia provides a general framework for law enforcement and security agencies to use exceptional measures to covertly gather data if necessary for criminal proceedings, to apprehend a suspect or to protect national security. While means of digital surveillance as such are not explicitly mentioned in the Criminal Procedure Code, the findings in this report indicate that the police and BIA consider the framework broad enough to include measures such as covert digital surveillance through spyware and other invasive technologies.

While Serbia's Criminal Procedure Code and related laws (Law on Police and Law on BIA) provide for exceptional measures, the use of advanced technologies, including spyware and other advanced digital forensic tools that collect vast amounts of personal data, is not sufficiently regulated by law. The generic provisions regulating the application of special evidentiary measures in the Criminal Procedure Code, the Law on Police and the Law on BIA, 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 an 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. As such, invasive digital surveillance tools used in Serbia may constitute indiscriminate mass surveillance, which is never a proportionate interference with the rights to privacy, freedom of expression and association.

7.7.1 WEAK JUDICIAL OVERSIGHT

Serbian legislation, including the Criminal Procedure Code, prescribes an obligation for law-enforcement and security agencies applying special evidentiary measures, that is i.e. actions involving covert and intrusive measures that take place without the knowledge or the consent of the target, to "assess whether the same aim could be achieved in a manner which is less restrictive to citizens' rights."[183]

This threshold is even higher when surveillance targets expression on matters of public interest. In other words, states should exercise exceptional caution when applying targeted surveillance against journalists and human rights defenders and other speaking on issues of public interest. The European Court of Human Rights stressed that secret surveillance measures should be used only in case of "an 'aggravated' (serious) threat" and when traditional investigative means have proven to be inefficient."[184]

Given the scale of digital surveillance targeting civil society activists often only over their posts on social media (as described further in the report) or their public engagement on controversial issues (such as publicly criticizing the Russian invasion of Ukraine or protesting against development projects that may cause environmental damage), it is not clear whether such assessments to determine whether less-restrictive measures could be just as effective are taken seriously in practice. Legal experts and practitioners in Serbia have warned about an overreliance on special evidentiary measures by police, security services and prosecutors, even when other, more conventional investigative methods are available.[185]

The vastly expanded digital surveillance in Serbia has to be viewed in the context of the weakening rule of law. Serbia ranks 93rd out of 142 countries globally on the World Justice Project Rule of Law Index, with particularly low score on the measures of government accountability and constraints on government power.[186]

As the European Parliament's study on the use of spyware concluded, judicial authorization "can easily be manipulated and gutted of any meaning... in case of politicization, or state capture of the judiciary."[187] Judicial professionals and civil society in Serbia have long expressed concerns about the undue political influence of the authorities on courts and prosecutors. Following the adoption of the new Constitution in 2006 (which was only amended in February 2023), the European Commission for Democracy through Law

[183] Criminal Procedure Code, Article 161, para 3.
[184] Hungarian Constitutional Court, Decision no. 32/2013. (XI.22.) AB, para. 75 (as cited by the ECtHR in Szabó and Vissy, para. 20).
[185] https://bezbednost.org/krivicne-istrage-u-srbiji-previse-se-oslanjaju-na-prisluskivanje/
[186] https://worldjusticeproject.org/rule-of-law-index/country/2024/Serbia/
[187] European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of the Union law in relation to the use of Pegasus and equivalent surveillance spyware, 22 May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN

(Venice Commission) criticized the" excessive role" of the National Assembly in the selection and appointed of judges at all levels, noting that it posed a "serious danger that political parties will control the judiciary."[188]

In its 2024 report on Serbia, the European Commission noted that the pressure on prosecution and judiciary "remains high".[189] The Commission further noted that "Government officials, including some at the highest level, and Members of Parliament continue to comment publicly on ongoing investigations or court proceedings, as well as on the work of individual prosecutors and judges." Given the above, it appears that judicial approval does not provide the necessary safeguards against abuse, but rather, a semblance of legality for routine surveillance.

7.7.2 INEFFECTIVE OVERSIGHT AND LACK OF REMEDY FOR VIOLATIONS

Although on paper, the remedies available to someone whose rights have been violated seem adequate, in practice, they do not provide effective protection. In the context of widely recognized state capture, neither the internal controls nor external bodies of oversight, including independent institutions such as Ombudsman's Office and Data Protection Commissioner, are often willing to confront the established practices. In its annual report on Serbia in October 2024, the European Commission reiterated that the Ombudsman's Office "needs to more vocally address violations of human rights and improve their cooperation with civil society."[190]

Judges in Serbia agree that it is virtually unknown in practice that a judge informs a person that they were the target of surveillance and that their data were destroyed, despite the fact that the law provides for this possibility.[191] Moreover, there is also a broad acknowledgment that it is practically impossible for citizens to find out if they were subjected to unlawful surveillance because responsible institutions generally refuse to provide such information.[192] Not being able to obtain this information severely curtails victims' ability to seek and obtain remedy, both through judicial and non-judicial means.

In the context of increasing state capture of institutions in Serbia by the ruling Serbian Progressive Party, the internal and external means of oversight are ineffective. In a study of the security sector in 2020, the Belgrade Centre for Security Policy noted a complete absence of any oversight:

"Oversight mechanisms [over the security sector] have ceased to function. Internal control departments are insufficiently independent from the directors; members of the National Assembly have shown no interest in overseeing security sector activities – one of their constitutionally mandated duties; independent oversight institutions, which established good practices early on, have been hamstrung by their new leadership; judicial oversight has been neutralized by the appointment of loyal personnel to key offices (for the implementation of covert data-gathering measures); and relations between the services and the public have deteriorated significantly. Under these conditions, the security services increasingly overstep their powers and jurisdictions and increasingly act as a political police force that focuses its attention on critics of the regime, all the while tolerating or actively assisting organized crime and corruption."[193]

In a field dominated by secrecy that can undermine civil liberties, a strong independent oversight is crucial, both to ensure that actors employing special measures are held accountable for their actions, and to encourage the development of more effective internal safeguards within police and security services. Yet, in the case of Serbia, a genuinely independent oversight is virtually non-existent.

7.7.3 BLURRY LINES BETWEEN POLICE AND SECURITY SERVICES

Finally, the lack of sufficiently clear separation between the police and BIA, whose operatives have police powers and can participate in criminal investigations (in contrast to many other European countries) and the need for the police to rely on BIA's technical capacity in order to conduct secret communications

[188] Venice Commission, Opinion on the Constitution of Serbia, 17-18 March 2007, CDL-AD (2007) 004, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2007)004-e
[189] European Commission, Serbia 2024 Report, 30 October 2024, https://neighbourhood-enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf
[190] European Commission, 2024 Serbia Report, 30 October 2024, https://neighbourhood-enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf
[191] Beogradski centar za bezbedonosnu politiku, "Krivične istrage u Srtbiji se previše oslanjaju na prisluškivanje," ["Criminal investigations in Serbia rely too much on wiretapping"], 18 June 2021, https://bezbednost.org/krivicne-istrage-u-srbiji-previse-se-oslanjaju-na-prisluskivanje/ (in Serbian).
[192] Beogradski centar za bezbedonosnu politiku, "Krivične istrage u Srtbiji se previše oslanjaju na prisluškivanje," (previously cited).
[193] Belgrade Centre for Security Policy, Security Sector Capture in Serbia, June 2020, https://bezbednost.org/wp-content/uploads/2020/06/NED-eng-screen-fin.pdf

surveillance, create an opaque situation that gives the BIA large room for maneuver without much accountability. The European Commission warned Serbia that the use of security services in interception of communications in criminal proceedings should be forbidden or limited to exceptional cases and the regulations and remits of the two services should be clearly separated.[194] The murky regulation and operational co-dependence between police and BIA significantly increases the risk of surveillance being misused for political purposes. As evidenced by the testimonies of activists and journalists in this report, the targets of surveillance were often not sure if they were speaking with police or BIA because the officers interrogating them often failed to clearly identify themselves. The lack of transparency of such operations only adds to the inability of victims to obtain any right to redress in case of unlawful surveillance.

Amnesty International fully recognizes that states must safeguard national security and protect citizens and may have a legitimate need to conduct covert surveillance, including interception of private communication, in some circumstances. However, any surveillance activities must balance the needs of the state with the human rights of individuals, including their right to privacy and provide safeguards against unwarranted or arbitrary restrictions. As described above, Serbian legislation and practice seem to fall below this standard, with overreliance on special measures by all involved actors, lack of adequate oversight and ineffective mechanisms for remedy – all of which are further exacerbated by the government's extensive control over all branches of the authority in Serbia. This has allowed for the proliferation of broad and virtually unchecked secret surveillance without accountability.

[194] European Commission, 2024 Serbia Report, 30 October 2024, https://neighbourhood-enlargement.ec.europa.eu/document/download/3c8c2d7f-bff7-44eb-b868-414730cc5902_en?filename=Serbia%20Report%202024.pdf

8. HUMAN RIGHTS ANALYSIS

The practices outlined in this report, such as using digital surveillance to target civil society activists, journalists and human rights defenders, or to search their devices, for expressing strong opinions on social media or organizing and participating in peaceful protests undermines their rights to privacy, freedom of expression and peaceful assembly, and is clearly incompatible with international human rights law and standards.

The right to privacy is guaranteed under Article 17 of the International Covenant on Civil and Political Rights, as well as under Article 8 of the European Convention on Human Rights. Privacy is both a right itself, and a cross-cutting right, meaning that violations of the right to privacy may "affect the enjoyment of human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."[195]

Under international law, interference with the right to privacy is permitted only where it is "authorised by domestic law that is accessible and precise", is in pursuit of the legitimate aim and strictly meets the test of proportionality and necessity.[196] The requirement of a legitimate aim means that it is never valid to interfere with the right to privacy in response to the exercise of human rights, such as organizing peaceful protests, or exercising the right to free expression, nor is it permissible to interfere with the right to privacy in a discriminatory manner. A measure cannot be necessary or proportionate if it is not in pursuit of a legitimate aim.

To meet the test of necessity and proportionality, "the state has the burden of showing that the restriction is rationally connected to the legitimate aim being pursued" (in other words, that it is 'an appropriate response to a pressing social need') and also, that the restriction is the least intrusive measure capable of serving that aim.[197] Similarly, the European Court of Human Rights considered that in order for restrictive measures to be considered as necessary and proportionate, there must be no other means of achieving the same end that would interfere less seriously with the right concerned.[198]

Crucial to the question of whether these requirements are met in a specific case is the question of whether the law and practice governing surveillance or other privacy invasive measures are governed by safeguards

[195] United Nations General Assembly Resolution 78/213, Promotion and protection of human rights in the context of digital technologies (2023).
[196] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights,* A/HRC/41/35, para.24
[197] United Nations Human Rights Committee, "General comment No. 37 (2020) on the right of peaceful assembly (article 21)", GC37, para. 40, documents.un.org/doc/undoc/gen/g20/232/15/pdf/g2023215.pdf
[198] ECtHR, Glor v. Switzerland, Application 13444/04, Judgment 30 April 2009, https://hudoc.echr.coe.int/fre?i=002-1569 para. 94

capable of preventing abuse.[199] The absence (or inadequacy) of such safeguards may render the overall regime governing surveillance powers incompatible with human rights.[200]

The lack of adequate safeguards against abuse results not only in violations of the right to privacy of those targeted, but also creates a chilling effect on society at large. Chilling effect in this context refers to the phenomenon whereby people refrain from exercising their rights out of fear they could be subject to unlawful surveillance. In other words, "Even the mere possibility of communications being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[201]

Such self-censorship is decidedly the fault of states. This is because where states fail to enact adequate safeguards, it may be impossible to know who is subject to surveillance, how, or why. In such cases, "widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified […]. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to private and family life]."[202]

Special procedures and measures such as digital surveillance are therefore permitted only in investigation of serious crimes or grave threats to national security, provided that reasonable suspicion exists of such activity and are, even then, applied only when objectives cannot be achieved through other means less likely to infringe on rights.

The threshold for lawful surveillance is even higher in the context of surveillance of civil society actors or when expression of public interest is implicated. The UN Human Rights Council has expressed concerns about the chilling effect of targeted surveillance of civil society, noting that it "creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information."[203] This is because digital surveillance creates a fear of retribution for legitimate work, which is disproportionate to the aim pursued and strikes at the core of the right to freedom of expression.

The UN Human Rights Council has noted that digital surveillance should never be used as justification for "muzzling of any advocacy of multiparty democracy, democratic tenets and human rights," and emphasized the need to protect journalists and others who publish human rights-related reports and the confidentiality of their sources.[204]

In the context of Serbia, the authorities have used measures that severely encroach on people's rights to privacy and freedom of expression without the necessary consideration of the principles of legality, necessity and proportionality. Although Serbia's Criminal Procedure Code requires competent authorities, including the police and BIA, to assess the necessity and proportionality of the special evidentiary measures, such as digital surveillance, there is no evidence that such assessments have been carried out.

---

[199] See, e.g. CASE OF ROMAN ZAKHAROV v. RUSSIA (Application no. 47143/06), European Court of Human Rights (Grand Chamber) (2015). "236. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see *Kennedy*, cited above, § 155; see also *Kvasnica*, cited above, § 84). The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse."

[200] Pietrzak and Bychawska-Siniarska and Others v. Poland (applications nos. 72038/17 and 25237/18), European Court of Human Rights (2024).

[201] UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, 30 June 2014 (hereinafter UNHCHR Privacy in the Digital Age), para. 20.

[202] Roman Zakharov v. Russia, European Court of Human Rights, paragraph 171.

[203] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights,* A/HRC/41/35, para.25

[204] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights,* A/HRC/41/35, para.26

8.1 HUMAN RIGHTS COMPATIBILITY OF THE USE OF SPYWARE

8.1.1 HIGHLY INVASIVE SPYWARE

The compatibility of surveillance measures with human rights law depends not only on the law and practice of state agencies, but also on the particular tools used. Many forms of modern highly invasive spyware used by states are incompatible with human rights by dint of their design.

This report documents the use of Pegasus spyware, as well as the likely presence of an operator of Predator spyware. Amnesty International calls for a global ban on these forms of highly invasive spyware, because they allow unlimited access to a device and their use cannot be independently audited. Because of these features, even a human rights compliant regulatory framework would be inadequate to prevent human rights violations linked to highly invasive spyware with these characteristics.[205] Similarly, the European Data Protection Supervisor noted that "the level of interference with the right to privacy is so severe that the individual is in fact deprived of it. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate - irrespective of whether the measure can be deemed necessary."[206] This aligns with the reasoning presented by the former Special Rapporteur on Counter-Terrorism, who argued that spyware that it is incapable of being meaningfully limited in its functionality, and whose use cannot be audited independently, should be subject to a ban.[207]

In human rights terms, the inability of highly invasive spyware, such as Pegasus or Predator, to be limited in the amount of data it accesses means that its use cannot comport with the human rights law requirement of necessity and proportionality, since by definition it cannot be the least intrusive tool. The inability to independently audit the use of such spyware – which intentionally obscures the traces of its use – means that the human rights safeguards of independent oversight (which is also crucial to the right to remedy) cannot be effective at detecting abuses. As such, highly invasive spyware can never be used in a human rights compliant manner and should be permanently banned.

8.1.2 SERBIAN NOVISPY SPYWARE

The report also documents for the first time the use of NoviSpy, a novel and not previously publicly known Android spyware, by Serbian authorities. While NoviSpy does not allow unlimited access to all data on the device as does software like Pegasus, it does gather extremely sensitive private information on its target, raising questions about whether its use can be compatible with human rights law and standards. This includes the collecting of screenshots of all actions on the phone, tracking the target location, recording from the camera and microphone, and collecting sensitive files and photos. It is unclear whether in practice this can be limited in specific use cases. Without such functionality, the scale and the amount of data capable of being collected would generally violate the human rights requirement of proportionality. Even if NoviSpy is technically capable of being limited in functionality or subject to meaningful audit and oversight, all spyware used in Serbia should be subject to a moratorium until such time as a system of human rights safeguards is in place capable of addressing the types of abuses documented in this report.

Amnesty International wrote to Serbia's Ministry of Interior and BIA asking them to clarify the procedure but have not received response before the publication.

---

[205] See, for example, Amnesty International, *Thailand: "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand* (Index: ASA 39/7955/2024), 16 May 2024, https://www.amnesty.org/en/documents/asa39/7955/2024/en/, Section 5.1.

[206] European Data Protection Supervisor, Preliminary remarks on modern spyware, 15 February 2022, p.8

[207] UN Special Rapporteur on Counter-Terrorism, Position Paper, Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, December 2022, para. 46, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

8.2 HUMAN RIGHTS IMPACT OF THE USE OF CELLEBRITE AGAINST JOURNALISTS AND HRDS IN SERBIA

Phone extraction software such as Cellebrite raises many similar human rights concerns as the use of spyware or other forms of surveillance. By granting total access to information stored on a mobile device, it allows for an enormous interference with the right to privacy, and as such must also meet the tests of legality, legitimate aim, and necessity and proportionality. The use of Cellebrite software against people in Serbia for exercising their human rights to expression and peaceful assembly can never be a legitimate aim, and therefore is in violation of human rights law.

Because of its intrusive capabilities, many of the human rights safeguards that are required to prevent the abuse of spyware are also necessary, to the use of phone extraction software. The question of whether such safeguards would be capable of preventing abuses of this tool depend in part on questions regarding the design of Cellebrite products. Accordingly, Amnesty International wrote to Cellebrite to ask detailed questions about the technical safeguards such tools employ.

In response to Amnesty International's written queries, Cellebrite stated that their products are not "spyware" and that they "do not provide cyber surveillance technology" (see Chapter 5). The former is accurate in the sense that unlike most spyware, Cellebrite tools generally require physical access to a device. The latter is, at a minimum, dependant on one's definition of "surveillance." Cellebrite, for example, allows for authorities to access private communications. Whether such an activity amounts to surveillance arguably depends more on whether it is conducted with the knowledge or consent of the target, rather than the manner in which they are accessed. The similarities to spyware, and consequent human rights concerns, are even more pronounced when considering Cellebrite's UFED Cloud product; since it enables operators to use passwords and tokens from target phones to "extract, preserve and analyse public- and private-domain, social-media data, instant messaging, file storage, web pages and other cloud-based content" not necessarily stored on the phone, therefore extending the intrusiveness beyond a device search, and also potentially offers ongoing access to the communications of the target. Further, as documented in this research, without adequate safeguards in place, Cellebrite's products can be used by authorities to covertly install spyware on a device.

By allowing broad access to data stored on mobile devices, as well as potentially to cloud-based personal data, Cellebrite creates a serious infringement with the right to privacy. Since there is no universally-agreed definition of "surveillance," the distinction between spyware and invasive digital forensic technology is ultimately less important in human rights terms than the issue of whether the interference with privacy and other human rights that Cellebrite creates is compatible with the requirements of human rights law.

The use of advanced forensic software gives rise to multiple and compound interferences with the rights to privacy, expression and peaceful assembly. Where such software enables the unlimited extraction of data and where its functioning cannot be subjected to independent and meaningful scrutiny, it is crucial that such tools be subject to rigorous safeguards in their deployment, authorization and oversight that is capable of catching and providing remedy for the types of abuses documented in this report.

In Serbia, the use of these tools to target people for their activism, or the use of such tools in contravention of domestic law, clearly violates human rights law.

8.3 HUMAN RIGHTS RESPONSIBILITIES

As the research in this report shows, the Norwegian Ministry of Foreign Affairs, which donated the Cellebrite UFED technology, and UNOPS, which managed procurement for the Norwegian government's grant to Serbia's Ministry of Interior and worked closely with the Ministry to identify their needs and set up their digital forensic capacity, may not have conducted a due diligence process to assess and mitigate for the potential risks of this technology to human rights or provide safeguards against its abuse. In light of the weak regulatory environment for digital technologies and surveillance in Serbia and persistent reports of increasingly more repressive measures used by the government against 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 a state with a questionable

human rights record. In this sense, they both contributed to Serbia's violations of people's rights to privacy, freedom of expression, association and peaceful assembly through unlawful digital surveillance. In response to Amnesty International's Right of Reply letter, the Norwegian Ministry of Foreign Affairs said it found it "alarming that digital forensic tools, purchased through a project funded by Norway, may have been misused to 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." [208] The Ministry noted that the Internal Audit and Investigation Group (IAIG) of UNOPS, which managed the project, would thoroughly investigate the alleged misuse and that the Ministry would follow up the matter with both UNOPS and the Serbian authorities.[209]

In an email to Amnesty International, however, UNOPS office in Serbia, seemed to suggest that their mandate was limited to procurement of the equipment. UNOPS said that the "forensic equipment was procured in accordance with UNOPS rules and regulations, through an open international competition," and that "to the extent feasible, UNOPS was monitoring the effects of interventions during the life cycle of the Project and identified indicators of positive contribution to the set objectives."[210] UNOPS also added that the "procurement of the forensic equipment contributed to the renewal of the accreditation of the National Forensic Centre Laboratories during the supervisory visit of the European Network of Forensic Science Institutes' Accreditation Body," which UNOPS considered as "indicators of positive contribution [that] also include human rights dimensions."[211] In the email, UNOPS did not explain whether or not they conducted any human rights impact assessment to determine any possible adverse affects.

While states have the primary duty to uphold human rights law, companies have a responsibility to respect human rights wherever they operate in the world and across all their business activities. This is a widely recognized standard of expected conduct as set out in international business and human rights standards including the UN Guiding Principles on Business and Human Rights (UN Guiding Principles) and the OECD Guidelines for Multinational Enterprises (OECD Guidelines).[212]

This responsibility to protect human rights requires that business enterprises "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur as well as "seek to prevent or mitigate human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[213] This responsibility is independent of a state's own human rights obligations and exists over and above compliance with national laws and regulations protecting human rights.[214]

The UN Guiding Principles clearly state that companies should use their leverage to address human rights issues that they may be involved in through linkage, even if they are not causing or contributing to any harm. Additionally, a company can be found to contribute to human rights impacts through, or in parallel to, third parties including other business enterprises or States due to a weak human rights due diligence process that failed to identify the risk and allow the company to address it accordingly.

8.3.1 HUMAN RIGHTS DUE DILIGENCE ACROSS THE VALUE CHAIN

The UN Guiding Principles stipulate that to meet the corporate responsibility to respect human rights, companies should have in place ongoing and proactive human rights due diligence processes to identify, prevent, mitigate and account for any human rights risks across their products, services and operations. In order to fulfil this responsibility, an adequate human rights due diligence process should cover adverse impacts that the company itself may cause or contribute to through its own activities, or which may be

[208] Letter from the Royal Norwegian Ministry of Foreign Affairs, Directorate for European and International Trade, to Amnesty International, 11 December 2024. On file with Amnesty International.
[209] Letter from the Royal Norwegian Ministry of Foreign Affairs, Directorate for European and International Trade, to Amnesty International, 11 December 2024. On file with Amnesty International.
[210] UNOPS Serbia Multi-country Office Director letter to Amnesty International, 12 December 2024. On file with Amnesty International.
[211] UNOPS Serbia Multi-country Office Director letter to Amnesty International, 12 December 2024. On file with Amnesty International.
[212] Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011, endorsed by the UN Human Rights Council (UNHRC), UNHRC Resolution 17/4: Human rights and Transnational Corporations and other Business Enterprises, adopted on 16 June 2011, UN Doc. A/HRC/RES/17/4; and OECD Guidelines for Multinational Enterprises, 2011, https://mneguidelines.oecd.org/mneguidelines. In accordance with the UN Guiding Principles, corporate responsibility to respect human rights is independent of a State's human rights obligations and exists over and above compliance with national laws and regulations protecting human rights. See UN Guiding Principles, Principle 11 and Commentary.
[213] UN Office of the High Commissioner for Human Rights (UNOHCHR), "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework", 2011, UN Doc HR/PUB/11/04, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, Principle 13 and commentary.
[214] OHCHR, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011, UN Doc. HR/PUB/11/04, ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, Principle 11 including Commentary.

directly linked to its products by business relationships. This process should include assessing risks and impacts, integrating and acting upon findings, as well as tracking responses and communicating how these are addressed.[215] Finally, the responsibility to respect human rights requires that business enterprises have in place policies and processes through which they can both know and show that they respect human rights in practice. The UN Guiding Principles explain that "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors"[216]

Regarding a company's business relationships, the UN Guiding Principles states that these include "relationships with business partners, entities in the value chain, and any other non-state or State entity directly linked to its business operations, products or services". A company's value chain refers to activities that add value by converting inputs into outputs, as well as entities with which it has a direct or indirect relationship in that process. The 'upstream' part of the value chain refers to activities or entities that *supply* products or services to a company that play a role in its own products or services, such as raw material suppliers. The "downstream" part of a value chain refers to activities or entities that receive products or services from the company, ranging from buyers and distributors to licensees and end-users of a technology.[217] The OECD Guidelines for Multinational Enterprises echo the need for companies to conduct due diligence across the value chain, including business partners that "receive, license, buy or use products or services from the enterprise and any other non-State or State entities directly linked to its business operations, products or services".[218]

In line with these international standards, Cellebrite should be conducting ongoing human rights due diligence across its entire value chain, which includes its sales to any non-state or State linked to its products. Tracking the conduct and behaviours of actors throughout its downstream value chain is crucial for a comprehensive human rights due diligence process, especially in the technology industry where the greatest human rights risks often lie in the usage of a particular product.[219] This is of particular importance given the severity of the human rights risks inherent in the type of technology Cellebrite produces and sells. Additionally, Cellebrite should have been integrating and acting upon its findings, as well as providing transparent information on how it has been conducting its due diligence to relevant stakeholders, such as civil society organizations that advocate for the protection of human rights.

8.3.2 CELLEBRITE'S HUMAN RIGHTS DUE DILIGENCE ACROSS THE VALUE CHAIN

In October 2024, Amnesty international sent a letter to Cellebrite, requesting information on its business relationships and human rights due diligence processes, especially in regard to the deployment of its products in Serbia. Two weeks later, Cellebrite replied with a short statement of broad responses (see Annex X.X for the full response) stating that the company does not consider itself a surveillance company and that it does not provide cyber surveillance technology or spyware. Rather, Cellebrite defined its product as a "digital investigative platform [that] equips law enforcement agencies with technology needed to protect and save lives, accelerate justice and preserve data privacy." The company also referred to its products as "digital forensics solutions that are licensed strictly for lawful use, require a warrant or consent to help law enforcement agencies with legally sanctioned investigations ***after*** *(original emphasis)* a crime has taken place."

In terms of its due diligence policies, Cellebrite stated that it undertakes several human rights due diligence steps before doing business with any country's national, regional or local law enforcement and other defence or civil agencies. To this effect, it described an "independent ethics and integrity committee" to guide its approach and "strict controls ensuring that our technology is used appropriately in legally sanctioned investigations." In conclusion, Cellebrite referred to its due diligence policies and directed Amnesty International towards its website for more information, which claims that its "technology can only be legally

[215] UN Guiding Principles, Commentary to Principle 17.
[216] UN Guiding Principles, Commentary to Principle 21
[217] UN Guiding Principles, UN Guiding Principles Reporting Framework: Value Chain, https://www.ungpreporting.org/glossary/value-chain/
[218] OECD Guidelines for Multinational Enterprises, Part I, Chapter II, Commentary 17.
[219] This rationale undergirded the European Union's 2021 recast of its Dual-use Export Regulation to introduce an "obligation for EU Member States to control exports of cyber-surveillance items which have legitimate civilian uses - in law enforcement or network monitoring, for example - but which could also be misused for internal repression or serious violations of human rights and international humanitarian law, "https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en. Amnesty International and other civil society organisations have documented the abuse of surveillance and other technologies to target human rights defenders and violate human rights across the globe, https://securitylab.amnesty.org/

obtained directly from us or an approved reseller, and we take proactive measures to ensure our technology isn't sold or purchased on secondary markets."[220]

Beyond these statements, Cellebrite failed to describe what these due diligence measures entail and what steps it takes to monitor the possible use of its products by third parties in the downstream value chain. Cellebrite also failed to provide any information on how its product was able to have reached and been misused in Serbia. According to documentation reviewed by Amnesty International, the equipment appears to have entered the country through a procurement organized by UNOPS, which served as an implementing partner on the Norwegian government's grant in support of Serbia's Ministry of Interior. Considering that UNOPS procurement would have to include details about the final customer (i.e. Serbia's Ministry of Interior), it is reasonable to extrapolate that Cellebrite must have been fully aware that its technology was intended for use by Serbian authorities and that a human rights impact assessment should have been carried out to identify, prevent, mitigate and account for any human rights risks posed by the transaction. Even if it was not clear to Cellebrite that Serbia was the final destination for delivery, Cellebrite could have incorporated into its agreement with UNOPS the ability to monitor to where this technology would be disbursed, how it would be used and by whom, for the purposes of analysing any possible adverse human rights impacts.

As noted above, Cellebrite described its product to Amnesty International as "digital forensic solutions". However, while Cellebrite's description of its products may have been the original intended use of these technologies, the company's 20-F/A Securities and Exchange Commission filing on 21 March 2024 as part of Cellebrite's legal disclosure as a publicly traded company demonstrates that the company was well-aware of the significant risk that its products could be misused and lead to adverse human rights impacts.[221] Moreover, Cellebrite's SEC filing makes it clear that the company was aware of the weaknesses in its human rights due diligence processes, which would be unable to adequately avoid such adverse impacts. For instance, in the SEC filing, Cellebrite specifically stated that "some of our government customers may use our solutions in a manner that is incompatible with, or perceived to be incompatible with, generally acceptable human rights standards, without our knowledge or permission"[222]. While the company stated that its license agreements prohibit customers from using their products in a manner that violates human rights, it also acknowledged that it "cannot provide any assurance that customers or others will not manage to circumvent our restrictions or that we will not be subject to claims from third parties alleging that their rights were violated as a result of our customers' use of our products." These statements before the SEC depict a different stance than its response to Amnesty International in October 2024, demonstrating Cellebrite's acknowledgement of the limited impact that its human rights due diligence practices could have in mitigating the risks inherent in its products.

In the same SEC filing, Cellebrite demonstrated that it has taken human rights due diligence measures. Specifically, the company mentioned that it had "adopted policies that would prevent sales to customers in China and Hong Kong" and that they had "proactively stopped selling to customers in Russia, Belarus and a number of other countries," indicating limitations of its current human rights due diligence practice, especially in situations of heightened human rights risks. Cellebrite's website confirms this restriction on sales policy, where it lists examples of countries where the company has chosen to not sell its technology "due to concerns regarding human rights and data security". Cellebrite's website also states that it does not "condone the use of Cellebrite's solutions to access the personal information of journalists, activists or others who are working against the interests of repressive regimes, and doing so outside the bounds of a legally sanctioned investigation expressly violates the terms of our licensing agreements". However, as it acknowledges in its SEC filing, the company's current due diligence practices are unable to detect these instances, posing the question of how the company ensures that its human rights policies are operationalized in its sales activities to achieve their intended goals, as per the UN Guiding Principles.

In an email to Amnesty International ahead of the publication of the report, Cellebrite said that the company "takes 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," and committed to investigate findings of misuse documented in this report. Cellebrite did not provide further details about any due diligence efforts taken in relation to the Cellebrite use in Serbia in the past, but said that the company would be "prepared to impose appropriate sanctions, including termination of Cellebrite's relationship with any relevant agencies."

---

[220] Cellebrite, Ethics & integrity at Cellebrite, https://cellebrite.com/en/ethics-integrity/ (accessed on 20 November 2024).
[221] FORM 20-F, submitted by Cellebrite to the United States Securities and Exchange Commission for the Fiscal year ended December 31, 2023. https://www.sec.gov/Archives/edgar/data/1854587/000185458724000018/cele-20231231.htm (accessed on 9 December 2024).
[222] FORM 20-F, submitted by Cellebrite to the United States Securities and Exchange Commission for the Fiscal year ended December 31, 2023. https://www.sec.gov/Archives/edgar/data/1854587/000185458724000018/cele-20231231.htm (accessed on 9 December 2024).

8.3.3 CELLEBRITE'S HUMAN RIGHTS RESPONSIBILITIES

As per the UN Guiding Principles, Cellebrite has a responsibility to conduct human rights due diligence to ensure that its product does not cause or contribute to adverse human rights impacts. Even if a company's level of responsibility does not amount to 'causing or contributing', the UN Guiding Principles also clearly state that any companies involved in an adverse human rights impact through linkage at the very least should use their leverage to prevent and mitigate any human rights risks.

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. Civil society activists and journalists who have been subjected to invasive digital surveillance, including digital forensic investigations using Cellebrite technology merely for participating in protests and their posts in social media, told Amnesty International that they felt violated, vulnerable and alone as a result of these measures. Apart from the devastating personal impact, digital surveillance has had a profound effect on people's ability and willingness to continue to speak or engage on issues of public interest, leading some to self-censor or completely leave activism. Serbia's use of Cellebrite for political purposes, i.e. to silence and intimidate civil society and critical journalists, has undermined their right to privacy and restricted their capacity to exercise other rights, including the rights to the freedom of expression, association and peaceful assembly. At the very least, Cellebrite is directly linked to the adverse human rights impact and should have used its leverage to prevent them.

Cellebrite's SEC filing and decision not to sell to certain countries due to human rights concerns demonstrates that it was aware of the risk of its product being misused and creating human rights risks. On its website, Cellebrite also 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".[223] Such actions include a decision not to renew licences for Cellebrite products and even "disable customer's connected technology."[224] Yet, all information available to date indicates that in this case, Cellebrite has not taken sufficient and effective measures to use its leverage to address the human rights risks in its downstream value chain.

Cellebrite's lack of transparency in engaging with key stakeholders such as human rights organizations also reflects a weak human rights due diligence process. As explained above, in September 2024, Cellebrite responded to Amnesty International's research questions with general statements that did not reference Serbia or address questions as to how Serbian authorities could have used its product against civil society activists. In November 2024, Amnesty International wrote again to Cellebrite and shared the findings of this research, including the allegations contained in this report. In a response sent immediately before the publication of the report, Cellebrite did not explain whether it took reasonable steps to prevent or mitigate the adverse human rights impacts of their products in Serbia before the company was made aware of Amnesty International's findings. However, it said that "each year, Cellebrite evaluates where it conducts business and determines where to make any changes based on a wide range of factors, including the country's political structure and commitment to democracy, human rights and privacy." Cellebrite committed to investigate the allegations of misuse in Serbia and take appropriate action, including terminating relationship with relevant agencies, if the allegations are "validated." If Cellebrite fails to take concrete steps to address the potential misuse, it ccould be seen to be *facilitating* the continuance of the abuses, and thus be in a situation of 'contributing' to human rights abuses in Serbia due to its continued inaction.[225]

Cellebrite may have fallen short of its corporate responsibility under the UN Guiding Principles. According to the UN Guiding Principles, if a business enterprise identifies that it may contribute – or is already contributing to – human rights abuses, these companies must prevent or cease the negative human rights impacts.[226] In situations where a company has contributed to actual impacts, the company should also provide remedy to affected individuals.

[223] Cellebrite, Cellebrite provides facts about its business and solutions, https://cellebrite.com/en/cellebrite-facts/ (accessed on 9 December 2024).
[224] Cellebrite, Cellebrite provides facts about its business and solutions, https://cellebrite.com/en/cellebrite-facts/ (accessed on 9 December 2024).
[225] UNHCR, *Taking action to address human rights risks related to end-use*, September 2020, taking-action-address-human-rights-risks.pdf
[226] UN Guiding Principles, Commentary to Principle 19.

8.4 HUMAN RIGHTS RESPONSIBILITIES OF NSO GROUP AND INTELLEXA

Amnesty International has identified the deployment of Predator spyware, produced by Intellexa, in Serbia from early 2020 until at least December 2021, as outlined in Section 4.2. Amnesty International has also identified the deployment of Pegasus spyware, produced by NSO Group, in Serbia in 2023 (see Section 4.3). In both cases, technical and circumstantial evidence leads Amnesty International to conclude that there is a high likelihood that the Serbian authorities were responsible for the use of these forms of spyware. In the case of Pegasus spyware, Amnesty International has also identified its use against two civil society activists and one protest organizer.

NSO Group's Human Rights Policy provides that: "In our sales process, we thoroughly evaluate the potential for adverse human rights impacts arising from the misuse of our products by considering, among other factors, the specific customer, the proposed customer use case and the past human rights performance and governance standards of the country involved." Moreover, if Pegasus spyware was used against Serbian civil society, then Israeli export laws would have required an end user certificate that identifies, among other things, the ultimate end user and purpose.

Intellexa has not proactively disclosed any information about their human rights due diligence policies.

Amnesty International wrote to both NSO Group and Intellexa about their human rights due diligence policies and specifically about any due diligence carried out in relation to sales of spyware to Serbia. In a letter to Amnesty International, NSO Group could not "comment on specific existing or past customers," but noted that the company was "fully committed to upholding the UN Guiding Principles on Business and Human Rights."[227]

"In the first half of 2020, NSO Group has adopted its Human Rights Due Diligence Procedure to implement the company's Human Rights Policy which enables the Group to comply with applicable local laws as well as international human rights standards all in accordance with the UNGPs and the US Department of State Guidance on Implementing the UNGP for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities. The multi-step due diligence procedure implemented by the Group requires the assessment of the potential human rights impact of a proposed business opportunity prior to the sale of any Group`s product to a customer, paying particular attention to the state of rule of law, human rights, and safeguards, processes and institutional norms in the customer's country. Consistent with the Human Rights Due Diligence Procedure, we perform extensive due diligence on potential business opportunities. These steps are designed to help identify, prevent, and mitigate the risks of adverse human rights impacts associated with potential misuse of our products.[228]

Intellexa did not respond the report findings, the details of which were shared with the company ahead of the publication. If either NSO Group or Intellexa had conducted such due diligence, and had sold Pegasus and Predator spyware to Serbian authorities, then NSO Group and Intellexa should have been aware of the increasingly hostile environment for civil society, as outlined in Section 3.1; and the lack of legal safeguards to prevent human rights violations (see Section 7.1). With such knowledge, both NSO Group and Intellexa would have been aware that selling spyware such as Pegasus or Predator could or would directly result in human rights harms.

Amnesty International classifies both Pegasus and Predator spyware as 'highly invasive', on the basis that they do not include technical safeguards to ensure that they do not cause human rights harms; they are specifically designed to evade investigation and allow for their users to take the maximum amount of target data possible. Given these capabilities of these forms of spyware, any use of them therefore cannot be in line with the UN Guiding Principles which outlines that companies must respect all human rights. Even if NSO Group and Intellexa had truly conducted appropriate human rights due diligence, their decisions to proceed with the sales of such products that could not be made rights-respecting leads Amnesty International to conclude that NSO Group and Intellexa failed to fulfil their responsibilities under international human rights standards. On this basis, both NSO Group and Intellexa should cease the use, production, sale, transfer and support of Pegasus and Predator spyware respectively, and any other similar highly invasive spyware that does not include technical safeguards allowing for its lawful use under a human rights-respecting regulatory framework. NSO Group should also provide adequate compensation or other forms of effective redress to victims of unlawful surveillance in Serbia.

---

[227] NSO Group's response to Amnesty International's Right of Reply letter, 10 December 2024. On file with Amnesty International.
[228] NSO Group's response to Amnesty International's Right of Reply letter, 10 December 2024. On file with Amnesty International.

9. RECOMMENDATIONS

9.1 TO SERBIAN AUTHORITIES

- Ensure effective remedy to victims of unlawful targeted surveillance and hold perpetrators to account for the violations including by conducting independent, impartial, and transparent investigations into all documented and reported instances of unlawful targeted surveillance and misuse of spyware, including but not limited to the cases mentioned in this report.
- Ensure that blanket secrecy rules do not prevent mechanisms of oversight and the targeted persons access to information on the use of spyware and other invasive digital forensic tools.
- Amend the Criminal Procedure Code, Law on Police and Law on BIA (as well as other laws regulating covert surveillance) to ensure that they are in full conformity with the rulings of the European Court of Human Rights, with regard to quality of the law, authorization procedures, supervision and oversight mechanisms, notification mechanisms and remedies. Specifically, ensure that:
    - Surveillance is governed by precise and publicly accessible laws.
    - Surveillance affects only specified persons, is authorized by a competent, independent and impartial judicial body and that such authorization includes limitations on time, manner, place and scope of surveillance.
    - Authorized digital surveillance is subject to detailed record keeping, in accordance with documented legal processes for a warrant, and targets are notified as soon as practicable without jeopardizing the purpose of surveillance.
    - Agencies authorized to conduct surveillance and judicial authorities authorizing them prepare meaningful assessments to ensure that the objectives of surveillance could not be achieved with means that are less intrusive on human rights.
- Impose a ban on highly invasive spyware, whose functionality cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or whose use cannot be independently audited.
- Implement a human rights regulatory framework that governs surveillance and is in line with international human rights law and standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer and use of all spyware should be enforced.
- Take concrete action to counteract the chilling effect and create a safe and enabling environment where civil society members, activists, and journalists are able to freely and safely exercise their rights to freedom of expression and assembly in digital spaces, without fear of harassment, intimidation and violence, in line with international standards and safeguards:
    - End all criminal proceedings against all people charged solely for their involvement in peaceful protests or for exercising their right to freedom of expression.
    - Establish and enforce codes of conduct on public communications for officials to ensure public officials do not engage in online harassment and smear campaigns against activists, journalists and human rights defenders.

9.2 TO THE NORWEGIAN GOVERNMENT

- Ensure that all development or aid projects involving the provision of digital surveillance equipment and capacity are accompanied by robust human rights risk analyses that assess potential negative effects and propose adequate measures to prevent and mitigate them.
- Refrain from providing digital surveillance equipment and capacity where its use without abuse of human rights could not be guaranteed.
- Conduct meaningful consultations with all relevant stakeholders, including civil society and other independent monitoring bodies, to understand the unforeseen risks of assistance involving the provision of new digital technologies in order to prevent and mitigate negative consequences for human rights.
- Before the provision of assistance that includes digital surveillance technology, ensure that the recipient state has in place at least minimum safeguards against abuse, including:
    - Domestic legislation that includes a clear framework for the use of digital surveillance and safeguards against human rights violations and abuses.
    - Adequate mechanisms for accountability and access to justice, i.e., that rights-holders can claim in practice their rights and seek justice, redress or compensation for violations through accountability mechanisms, both judicial and non-judicial.
    - A track record of respecting human rights, including providing an enabling environment for the freedom of expression, assembly and association.
- Ensure that assistance projects that include digital surveillance technology include a comprehensive training element to ensure that the donated technology is only used lawfully, and reduce possibility of its misuse
- Ensure that companies providing digital surveillance technology comply with the UN Guiding Principles on Business and Human Rights, as well as relevant regional and national corporate sustainability and due diligence frameworks.
- Include an adequate human rights risk analysis in all phases of the project, including design, implementation, and evaluation of the assistance projects.

9.3 TO THE EUROPEAN UNION

Given Serbia's EU candidate status, the EU should ensure that its engagement with the Serbian authorities is used to foster reforms and promote respect for human rights and rule of law, in both law and practice.

The EU and its member states should therefore use their engagement with Serbia, including the financial and technical assistance foreseen within the framework of its EU accession process to urge the Serbian authorities to:

- Conduct independent and thorough investigations into all documented and reported instances of unlawful targeted surveillance and misuse of spyware and other invasive digital forensics tools and ensure effective remedy for the victims.
- Amend the Criminal Procedure Code, Law on Police and Law on BIA, as well as other laws regulating covert surveillance, to ensure that they are in full conformity with the rulings of the European Court of Human Rights, with regard to quality of the law, authorization procedure, supervision and oversight mechanisms, notification mechanisms and remedies.
- Implement a human rights regulatory framework that governs surveillance, includes robust safeguards, including strong independent oversight, and is in line with international human rights law and standards. Until such a framework is in place, both the EU and Serbia should enforce a moratorium on the purchase, sale, transfer and use of all spyware.

More broadly, the EU and its member states should:

- Step up the use of diplomatic channels to support independent journalists, human rights defenders and civil society in Serbia. This could include more vocal public communications expressing

concern over targeting of individuals and statements underlining the EU's support for civil society in the country.

- Raise the issue of unlawful digital surveillance in high-level meetings with senior officials in Serbia and urge them to take concrete measures to ensure the safety of civil society actors and to preserve the right to privacy, as well as the rights to freedom of expression, association and peaceful assembly.
- Use political and technical dialogue with the Serbian authorities to call for and follow up on the progress of any investigations into documented and reported instances of unlawful targeted surveillance or the misuse of spyware and other invasive digital forensics tools. Such investigations should include, but are not limited to, the cases mentioned in this report.

9.4 TO HUMAN RIGHTS DEFENDERS

While it's difficult to fully protect yourself from targeted digital surveillance, the following are key digital security recommendations for at-risk human rights defenders:

- Fully power down your phone in high-risk scenarios such as when crossing a border, at a protest, or if you suspect you may be detained. This will remove the encryption keys from system memory making some attacks more difficult.
- Disable biometric or face ID in situations where your device can be seized.
- Use a long PIN code or ideally passphrase to secure your phone. While many modern devices try to prevent PIN recovery and brute-force using hardware security features, these are frequently bypassed. A strong password or passphrase will need to be brute-forced even if other security mechanism are bypasses.
- Limit the amount of private or critical information stored on your device to reduce risks in case of seizure, detention, or other incidents. Enabling the disappearing messages feature in messenger apps can be helpful.
- Regularly update your phone's operating system and important applications. Not all device vendors regularly provide security updates, and some devices may not receive any updates at all. For security, you should consider upgrading to an actively supported device where possible.
- Be cautious with apps which request extensive permissions. Disable unnecessary or unexpected apps which use Android Accessibility Services or administrative permissions. Ensure features like Google Play Protect are active to scan for malicious apps.
- Any members of Serbian civil society who have received a threat notification from Google, or who otherwise believe they may be at risk from these spyware threats, should contact Amnesty International's Security Lab or other trusted digital security helplines for support in securing their devices or accounts.

9.5 TO MOBILE DEVICE VENDORS

This report documents how the misuse of exploit-based digital forensic tools such as Cellebrite UFED can contribute to human rights violations, particularly when used against journalists and human rights defenders. Forensic tools may also enable the covert installation of spyware or longer-term surveillance through theft of account passwords and security tokens.

Significant engineering efforts have improved platform security against fully remote[229] and baseband attack[230] surfaces, but relatively little work has focused on improving device security against exploits and attacks carried out with physical access to the device, which appear to be significantly more widespread based on the extensive customer base of mobile forensic vendors.

[229] Google, "Eliminating memory safety vulnerabilities at the source", 25 September 2024, https://security.googleblog.com/2024/09/eliminating-memory-safety-vulnerabilities-Android.html
[230] Google, "Hardening cellular basebands in Android", 12 December 2023, https://security.googleblog.com/2023/12/hardening-cellular-basebands-in-android.html

Mobile device manufacturers, chipset vendors and mobile device software maintainers should:

- Recognize the privacy and security threats from the unlawful or inadequately regulated use of exploit-based digital forensic tools when defining mobile device threat models; and when designing and prioritizing new security mitigations and device security improvements.
    - Thoroughly audit highly privileged software attack surfaces which are accessible with physical access including device Linux kernel device drivers, boot ROM, bootloader, *fastboot* service, and debug or recovery services available on a device without authentication. Weakness in such code, especially any vulnerabilities introduced by upstream chipset manufactures or OEMs, can impact a wide range of devices.
    - Implement mitigations to minimize physical access attack surface, such as by disabling the loading of new or unknown USB devices or kernel device drivers when a device is locked in an After First Unlock (AFU) or Before First Unlock (BFU) state.
    - Implement protections against PIN or lock pattern recovery by storing device credentials and credential protected keys in secure hardware such as the Trusted Execution Environment (TEE) or Secure Element (SE). The secure hardware should enforce protections against online brute-force and prevent extraction of key for offline brute-force or recovery.
    - Audit and secure software components which are critical to Secure Boot and maintaining a secure chain of trust. This may include software security enhancements and audits to ensure that test keys or otherwise leaked signing keys are not trusted in product boot chains, or used to secure hardware security enclaves.
    - Provide options to mitigate the risk of AFU forensic attacks, such as triggering a regular device reboot to a BFU state after a certain period of time.
- Mitigate the security risks of sensitive tokens or credentials being stolen during temporary device compromise, either with remote spyware or forensic data extraction products. Multiple spyware vendors and data extraction companies market products to retrieve additional data or perform ongoing surveillance through cloud access to sensitive data such as backups and email accounts using stolen tokens and credentials.
- Mitigations may include storing long-term device and application session keys and tokens in secure hardware, similar to the Device Bound Session Credentials (DBSC) proposal. Device vendors should provide a secure mechanism for application developers to ensure sensitive authentication and session tokens are bound to a physical device and cannot be copied or used from another device.
- Require re-authentication (using credentials, biometrics or both) to perform sensitive actions such as enabling debugging features, disabling security features such as Play Protect, and before installing untrusted applications. Reauthentication can mitigate threats enabled through temporary physical access such as at border crossings, or in situations of intimate partner violence.

Provide reminders or alerts on potentially unwanted or malicious actions taken on a device such as notifying the device owner about applications granted highly-sensitive permissions, or instances where automatic security updates have been disabled.

9.6 TO CELLEBRITE AND DATA EXTRACTION VENDORS

- Review its current human rights due diligence and make any necessary adjustments to ensure its effectiveness to identify the potential human rights impacts of all its products, especially in its downstream value chain. The due diligence process must allow the company to determine whether technical safeguards could ensure its products are rights-respecting or not, and take every measure to ensure that they are not misused in a way that adversely impacts human rights. If the safeguards could serve this purpose, the company must immediately put them in place.
- Implement technical mechanisms to limit the invasiveness of Cellebrite UFED products including limiting data collection to only information which is strictly necessary for a particular purpose, such as limiting extraction to a specific application, and pruning or deleting any extracted data which is outside the time period relevant to the search.

- Implement technical mechanism(s) allowing independent auditing of the use of data extraction technology including but not limited to:
    - Generating and storing a readable and verifiable audit log on the file system of the unlocked or extracted mobile device which records all actions performed on the device including; a list of data extracted (. Full File System vs Application), checksums of any payloads and/or exploits run on the device, detailed information on the licenced customer, the operator using the device, and information on the warrant or other legal justification supplied in the system when initiating the extraction.

      This audit trail would enable the device owner or their legal team to independently verify that any actions using a data extraction product were compliant with relevant local law and international human rights law and standards.
    - Forensic data extraction tools should document all logs, databases, or other files which are added, edited, deleted or otherwise tampered with in the course of a forensic unlock or extraction in order to ensure the integrity of extracted data.
    - Publish a publicly available, detailed technical description of the capabilities and functionality of any forensic extraction tool including methods for data extraction, a public software bill of materials, and any practices to ensure forensic integrity of the device if downloaded binary resources, exploits, or other unauditable code has been run on a targeted device.
- Restrict specific capabilities of forensic tools that pose a risk of evidence tampering or installation of spyware such as functionality to display device unlock codes, disable device lock screens, or export account passwords or tokens which can be used for further surveillance outside of a lawful forensic investigation.
- Provide adequate compensation and other forms of redress to individuals in Serbia whose rights have been violated by misuse of non-consensual forensic data extraction products.
- Immediately terminate the use, transfer, support and sale of forensic data extraction technologies to Serbia until there has been independent, impartial, and transparent investigations into all documented and reported instances f human rights abuses related to the use of Cellebrite, and until there are adequate safeguards to prevent future abuses.
- Immediately terminate the use, transfer, support and sale of forensic data extraction technologies in states where surveillance software or other digital technologies have been misused to unlawfully target HRDs, journalists and members of civil society, or where there are inadequate safeguards to prevent abuse.

9.7 TO NSO GROUP, INTELLEXA AND OTHER SURVEILLANCE TECHNOLOGY VENDORS

- Cease the use, production, sale, transfer and support of Pegasus, Predator or other similar highly invasive spyware that can neither be independently audited nor limited in its functionality, given that technical safeguards and a human rights-respecting regulatory framework would still be insufficient to prevent their adverse human rights impacts.
- Carry out appropriate human rights due diligence to identify the potential human rights impacts of all its other products. The due diligence process must allow the company to determine whether technical safeguards could ensure its products are rights-respecting or not. If the safeguards could serve this purpose, the company must immediately put them in place.
- Provide adequate compensation and other forms of redress to survivors of unlawful targeted surveillance in Serbia.

- Immediately terminate the use, transfer, support and sale of surveillance technologies in states where surveillance software has been misused to unlawfully target HRDs, journalists and members of civil society, or where there are inadequate safeguards to prevent abuse.
- Urgently take steps to ensure that HRDs , journalists and members of civil society do not continue to become targets of unlawful surveillance using its products or services, including by implementing adequate human rights due diligence processes, as set out in international business and human rights instruments such as the UN Guiding Principles, to ensure its activities, or those of its subsidiaries, sub-contractors and suppliers, respect the rights of HRDs and do not hinder their legitimate work.
- Conduct human rights due diligence, including conducting robust human rights risk assessments, for all proposed use, sales and transfers, including engaging with rights holders. The human rights due diligence process should also be transparent.

10. ANNEXES

10.1 ANNEX 1: HOW CELLEBRITE UFED AND EXTRACTION TOOLS FUNCTION

Amnesty International's Security Lab reviewed public and non-public marketing material and product documentation of Cellebrite UFED to understand the capabilities of the system.

Cellebrite UFED products enable Cellebrite customers without advanced technical expertise to unlock and extract data from mobile devices including Android's and iPhone's using advanced exploits and other data extraction techniques. UFED provides different capabilities depending on the status of the phone, either unlocked (the passcode is known) or locked with an unknown passcode.

The data accessible from a device also varies depending on if the running phone has already been unlocked at one point, called After First Unlock ("AFU") or has never been unlocked, referred to as Before First Unlock ("BFU"). A running AFU device will have system encryption keys stored in system memory which can make enable data access and recovery which is not possible with BFU device. UFED supports carrying out Brute Force ("BF") attacks against some devices in order to recovery the device unlock code and device encryption keys.

Cellebrite also offers products with different capabilities for customers in the private sector and those in public institutions such as police, intelligence services and military customers. Previously, public leaks of Cellebrite UFED software led to the identification of zero-day vulnerabilities used in the product. To mitigate the risk of valuable zero-day exploits being discovered, Cellebrite has offered an advanced unlocking service for devices with the latest security mechanism that were unsupported in UFED. Customers could physically ship a target device to a regional Cellebrite lab where the device can be unlocked without risk of fragile and expensive exploits and techniques being disclosed.

Since February 2024, Cellebrite has offered the UFED Inseyets product which combines Cellebrite "access and extraction technologies". The Cellebrite UFED Inseyets product is specifically focused on in this report, as forensic evidence suggests this is the Cellebrite product used by Serbian authorities in the examined cases.

The Inseyets software is used together with a physical "Turbo Link" adapter (previously known as a "Cheetah" adapter) which is used to connect physically to the target phone.

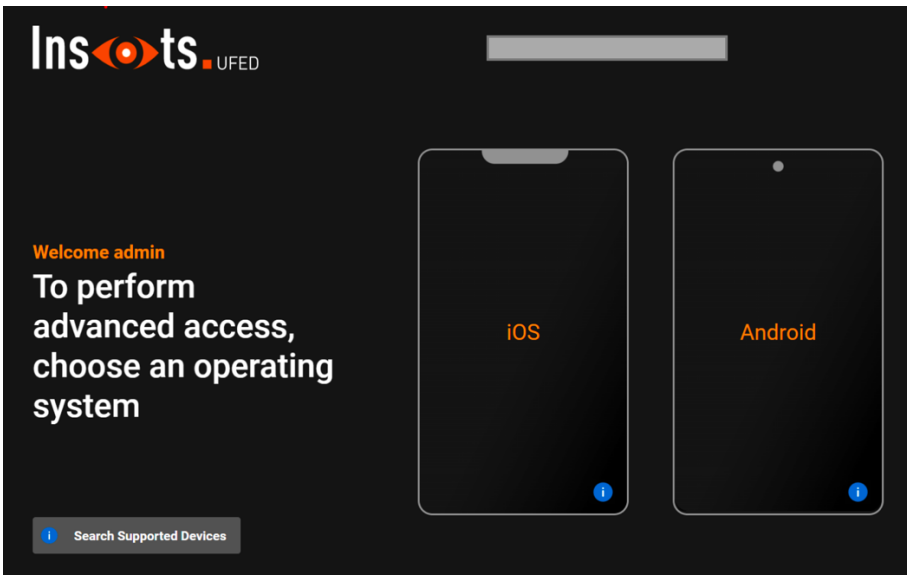


Figure 11: Screen of the Inseyets access (unlocking) flow.

If the phone is locked, the UFED system and Turbo Link adapter is used to fingerprint the model and version of the targeted device and identify possible exploits or attack techniques which can be used to target the device.

UFED Inseyets documentation reviewed by Amnesty International indicates that software exploit code, termed "resources" in Cellebrite documentation, are dynamically downloaded over the internet from a remote system in order to unlock a targeted device.

> The first stage in digital forensic investigations is to gain access to the operating system of the device under investigation.
>
> After the Turbo Link is initialized, it identifies the device, and downloads resources needed to gain access to the device.
>
> There are multiple access methods available to the Turbo Link and it typically tries several methods. The device characteristics determine which method succeeds in gaining access.

Figure 12: "Turbo Link" adapter downloads resources to try exploit the targeted device

Once the phone is connected to the Turbo Link adapter, various techniques and exploits will be attempted in order to try unlocking the device and bypass security mechanisms on the device.

A forensic workflow which involves downloading and executing of opaque and unauditable code to a targeted device during a forensic analysis process raises significant questions on how the forensic integrity of a device can be ensured.

Accessing a device after unlocking:

Once a phone is unlocked, either following a successful "access" or unlock exploit, or following entry of the pin code, the targeted mobile device can be switched into Cellebrite Mode ("CLB" mode). In this mode an initial Cellebrite payload has been installed on the device with elevate privileges which can be used to carry out any subsequent extraction and data collection steps.

2.4. Cellebrite (CLB) Mode

Once access is gained, the user interface will be refreshed, and the device enters Cellebrite (CLB) Mode. Cellebrite Mode is when temporary privileged escalated access to the device has been obtained. The device information screen is updated, and you are presented with several extraction options such as Full File System, Selective, and Secure Container.

Figure 13: Cellebrite (CLB) Mode is started following successful unlock

Where an Android device has a known unlock code, the Cellebrite "Unlocked" extraction workflow can be used. Cellebrite instructs the UFED operator to enable the Android developer mode and USB debugging mode on the target device. This allows the UFED system to have programmatic access to the device using the ADB interface.

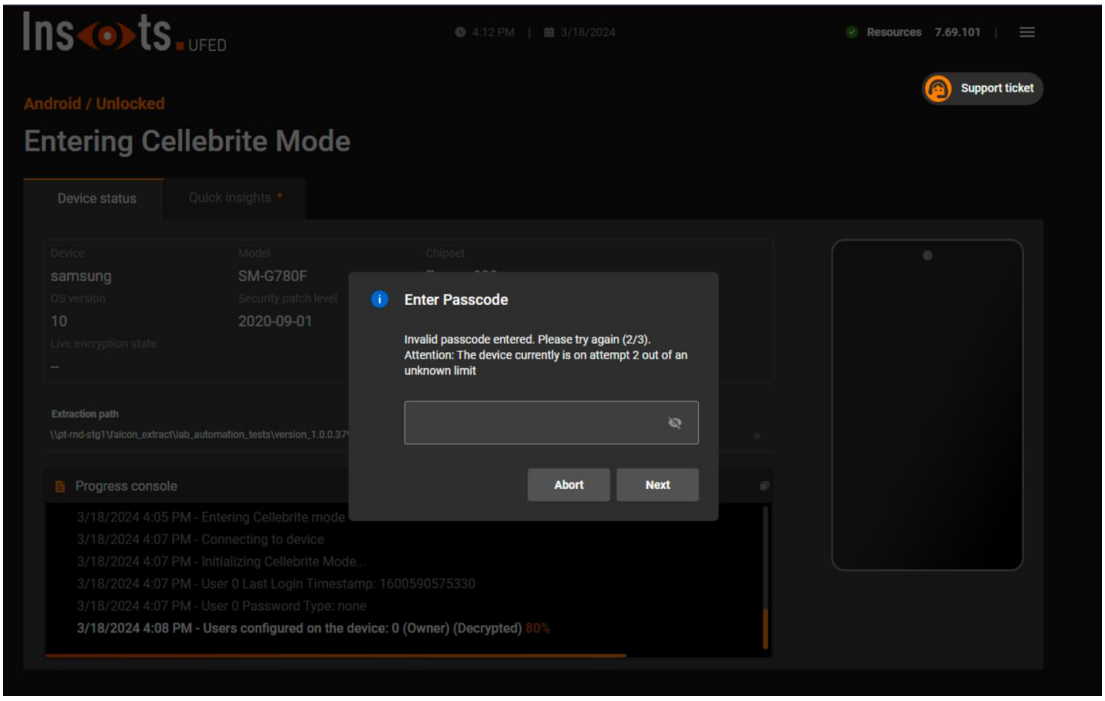


Figure 14: Screenshot of Cellebrite UFED's Cellebrite ("CLB") Mode

Access to a device over ADB does not provide privileged access to device data. Additional privilege escalation exploits are necessary to gain deeper access to the system and access sensitive user data from applications such as WhatsApp, Signal and others.

Amnesty International wrote to Cellebrite with a detailed set of questions on the functionality of their UFED Inseyets product, and the steps the company has taken to ensure the integrity of remotely loaded exploit resources. Cellebrite declined to provide a specific response to the questions.

A set of recommendations on protecting data on your device is available Section 9.1 ("Recommendations to human rights defenders").

Section 5 looks at multiple instances where Cellebrite was used against the devices of civil society members in Serbia. In the Case 7 (Section 5.3.1) a pin code was provided and the device was successfully compromised using an "unlocked workflow". The journalist in Case 4A (Section 5.2.1) did not provide their pin code and an *After First Unlock (AFU)* flow appears to be used to successfully bypass the phone lock screen and compromise the device.

10.2 ANNEX 2: FORENSIC ANALYSIS OF USE OF CELLEBRITE ON THE PHONE OF "IVAN"

Forensic records show that Ivan's phone (Case 7) was connected via a USB cable to an external system around 17:55 local time. Android ADB developer mode was enabled on his device and a number of binaries were copied to the device using the ADB protocol. This is consistent with the Cellebrite workflow for unlocked devices (where the pin code in known).

Amnesty International was able to recover samples of the binaries copied by the Cellebrite system to the targeted Android device. These binaries included **nandshell**, **nandread**, and **falcon**. Nandread and nandshell have publicly identified as binary names used in Cellerbrite UFEDs products.[231]

Binary Name	SHA 256
falcon	3621ffeb67efa3eccb9c1f20cd671b81b286a02425e582a8a1553e85b012403d
nandread	3936a6ec20405990802f59ea2747a1685886bab4f5949d258e84e4646006a4c1
nandshell	556a409603f56ed6e4a833da37263134ca00469970516634e845dccee080ad3c

Table 11: Binaries recovered from the phone of Ivan Bjelić

Amnesty International attributes the **falcon** binary to Cellebrite's UFED product. While the binary itself is heavily obfuscated, it appears to function as a binary loader to load and run exploit code in memory on the targeted device after it has been unlocked. Amnesty International identified a reference to the "falcon" extraction process in a leaked Cellebrite UFED product manual.[232]

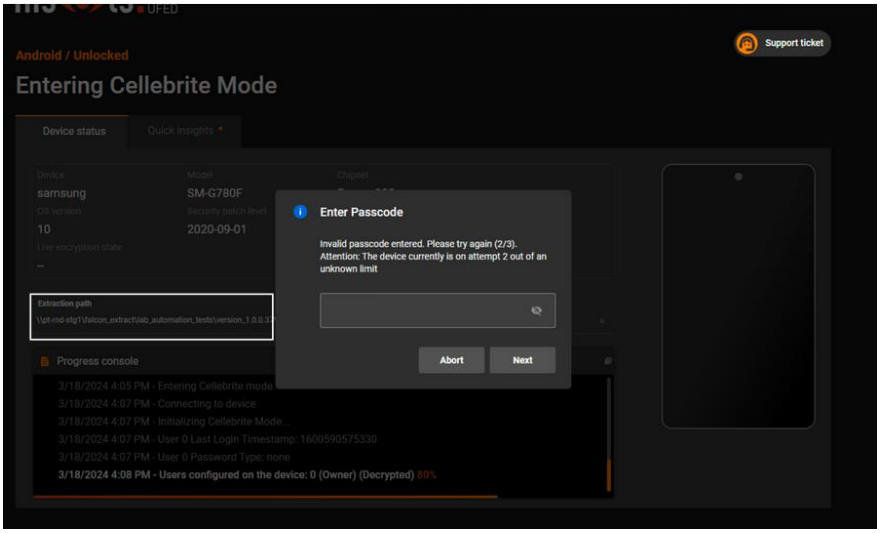


Figure 15: Cellebrite AFU mode interface showing "falcon_unlock"

[231] Matt Bergin, "Anti-Forensics: Reverse Engineering a Leading Phone Forensic Tool ", Black Hat Asia 2021 presentation, https://i.blackhat.com/asia-21/Friday-Handouts/AS-21-Bergin-Anti-Forensics-Reverse-Engineering-A-Leading-Phone-Forensic-Tool.pdf, slide 22

[232] Cellebrite, "Inseyets Offline UFED Version 10.2 User Manual", published on Graphene OS Discussion Forum, "Claims made by forensics companies, their capabilities, and how GrapheneOS fares" (Thread opened on 18 May 2024), discuss.grapheneos.org/d/12848-claims-made-by-forensics-companies-their-capabilities-and-how-grapheneos-fares

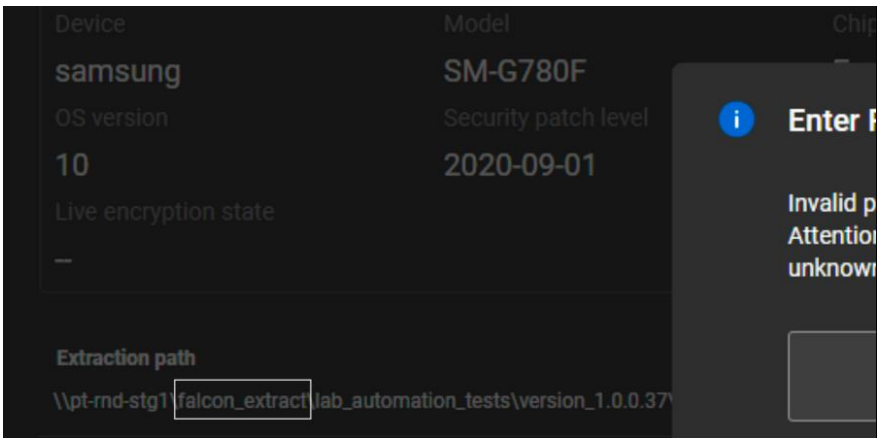


Figure 16: "falcon_extract" included in file path for Android unlock flow

Additionally, the Security Lab recovered log files generated by the Cellebrite system on the phone which confirmed that Cellebrite UFED has successfully exploited the device and was able to read protected files from the phone's filesystem. The recovered log files were stored in a "CLB" directory. Amnesty believes CLB refers to **Cellebrite Mode ("CLB"),** which is the software state Cellebrite UFED uses to perform further data extraction tasks after escalating privileges on the device.

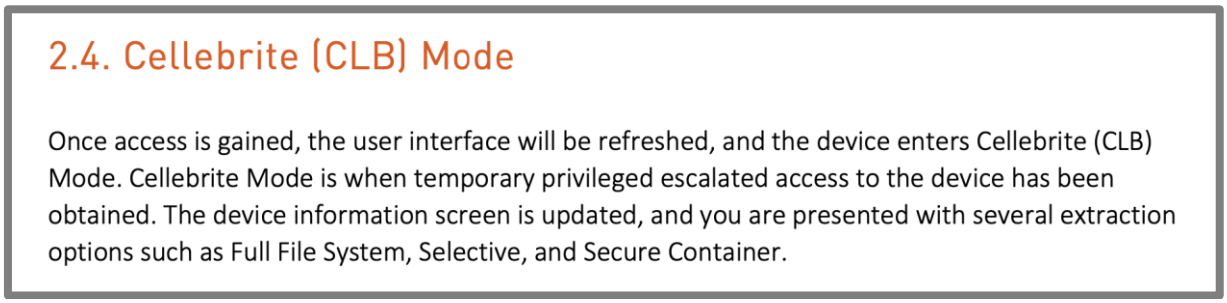


Figure 17: Cellebrite (CLB) Mode following successful unlock. Excerpt from leaked Cellebrite documentation

The Security Lab also identified a series of kernel crashes which were triggered on the phone while the Cellebrite product was being used by the Serbian authorities. Before each kernel crash, a series of kernel log lines were observed from the *adsprpc* driver, a custom Linux kernel driver developed by Qualcomm for efficient memory mapping on devices using a Qualcomm Android kernel fork.

Significantly multiple log lines indicated that an untrusted user application "**falcon**" was attempting to hit the *ADSPRPC* "*fastrpc_internal_mmap*" function among others:

Timestamp	Trace Description
2023-12-17 17:56:15.164660	adsprpc: ERROR: fastrpc_internal_mmap: user application **falcon** trying to map without initialization
2023-12-17 17:56:15.164948	audit: rate limit exceeded
2023-12-17 17:56:15.167510	adsprpc: fastrpc_init_process: untrusted app trying to attach to privileged DSP PD
2023-12-17 17:56:15.202061	adsprpc: mapping not found to unmap fd 0xffffffff, va 0xffffffffffffffff, len 0xffffffff
2023-12-17 17:56:15.202084	adsprpc: falcon: fastrpc_internal_mmap: ERROR: adding user allocated pages is not supported
2023-12-17 17:56:15.207916	adsprpc: mapping not found to unmap fd 0xa, va 0x0, len 0x0

Table 12: Kernel logs from exploitation of adsprpc module by Cellebrite falcon binary

Significantly the kernel crash logs also showed that the kernel corruption occurred in the Cellebrite falcon process:

```
2023-12-17 17:56:45.574680: Process falcon (pid: 10050, stack limit = 0x00000000eac9e565)
2023-12-17 17:56:45.574700: CPU: 0 PID: 10050 Comm: falcon Tainted: G S O 4.19.157-perf-g8779875ad741 #1
2023-12-17 17:56:45.574711: Hardware name: Qualcomm Technologies, Inc. xiaomi apollo (DT)
2023-12-17 17:56:45.574726: pstate: 00400005 (nzcv daif +PAN -UAO)
2023-12-17 17:56:45.574756: pc : pipe_read+0xac/0x308
2023-12-17 17:56:45.574769: lr : pipe_read+0x4c/0x308
2023-12-17 17:56:45.574778: sp : ffffff802e43bc80
2023-12-17 17:56:45.574787: x29: ffffff802e43bcf0 x28: fffffff4ce02c400
2023-12-17 17:56:45.574800: x27: fffffff4ce02c410 x26: 00000000000003ff
2023-12-17 17:56:45.574813: x25: 0000000000000028 x24: 00000000000003ff
2023-12-17 17:56:45.574826: x23: fffffff506d57620 x22: fffffff506d57600
2023-12-17 17:56:45.574839: x21: fffffff4ce02c400 x20: 0000000000000000
2023-12-17 17:56:45.574852: x19: fffffff4ce02c40c x18: 0000000000000000
2023-12-17 17:56:45.574864: x17: 0000000000000000 x16: 0000000000000000
2023-12-17 17:56:45.574877: x15: 0000000000000000 x14: 0000000000000000
2023-12-17 17:56:45.574890: x13: 0000000000000000 x12: 0000000000000000
2023-12-17 17:56:45.574903: x11: 0000000000000000 x10: 0000000000000000
2023-12-17 17:56:45.574916: x9 : 0000000000000001 x8 : 00000000dead0000
2023-12-17 17:56:45.574930: x7 : ffffffff00000000 x6 : 0000000000000002
2023-12-17 17:56:45.574942: x5 : 0000000000000000 x4 : 00000000000003ff
2023-12-17 17:56:45.574954: x3 : 0000000000000001 x2 : ffffff802e43bda8
2023-12-17 17:56:45.574967: x1 : fffffff4ce02c400 x0 : fffffff506d57600
2023-12-17 17:56:45.574982: Call trace:
2023-12-17 17:56:45.574996: pipe_read+0xac/0x308
2023-12-17 17:56:45.575014: __vfs_read+0xf8/0x140
2023-12-17 17:56:45.575027: vfs_read+0xb8/0x150
2023-12-17 17:56:45.575039: ksys_read+0x6c/0xd0
2023-12-17 17:56:45.575053: __arm64_sys_read+0x18/0x20
2023-12-17 17:56:45.575071: el0_svc_common+0x98/0x160
2023-12-17 17:56:45.575083: el0_svc_handler+0x68/0x80
2023-12-17 17:56:45.575097: el0_svc+0x8/0xc
2023-12-17 17:56:45.575114: Code: aa1c03fb aa1c03e1 b840ce68 f8410f69 (f9400529)
2023-12-17 17:56:45.575127: ---[ end trace 72c08623f6dedcd7 ]---
2023-12-17 17:56:45.575174: Kernel panic - not syncing: Fatal exception
```

Table 13: Kernel crash log shown crash in "falcon" binary

The appearance of the Cellebrite falcon binary in kernel logs and backtrace strongly suggests that these indicate an attempted Android kernel privilege escalation exploit targeting the Qualcomm kernel. Mr. Bjelić's phone was running the March 2023 Android security patch level at the time his phone was seized. These crash logs provided initial evidence of an actively exploited vulnerability in a Qualcomm kernel module leading to the identification of CVE-2024-43047.

10.3 ANNEX 3: TRACES OF POSSIBLE ZERO-CLICK SPYWARE TARGETING OF "IVAN"

Since 2022, Ivan had already suspected that he was under some type of surveillance. His phone was acting out of the ordinary; overheating or shutting down, and he was receiving calls from unusual numbers that did not resemble phone numbers in Serbia. Initially he ignored these suspicions.

Following the encounter with Serbian police and BIA officers in December 2023, Ivan shared screenshots with Amnesty International that he took when documenting additional suspicious activity he had observed on his device.

On 22 July 2022, Ivan's Xiaomi Android device registered a series of missed calls consisting of invalid, seemingly random, numbers not valid in Serbia (see Figure 18). After these calls, Ivan said that the battery on his device drained quickly.

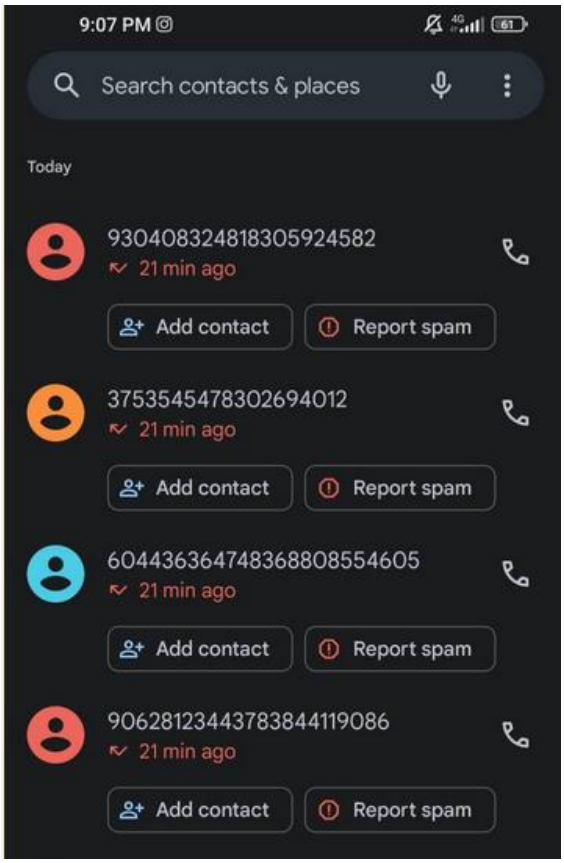


Figure 18: Suspicious missed calls from invalid phone numbers

Amnesty International analysed Ivan's device for any forensic traces of spyware targeting or infection. No indications of device exploitation were found outside of the Cellebrite use in December 2023. However technical limitations inherent in Android devices and various security mechanism make it difficult for researchers like Amnesty International to access sufficient information needed to reliably identify spyware attacks on Android, without access to root exploits similar to those used by Cellebrite. As such it was not possible to reliably determine if the observed missed calls were associated with any other traces of spyware activity on the device.

Amnesty International is publishing this screenshot in hopes of highlighting the knowledge gap around zero-click attacks targeting Android devices. The Security Lab believes these artifacts are consistent with what would be expected from a zero-click attack targeting Android calling features such as Voice-over-Wifi or Voice-over-LTE (VoLTE) functionality used in Android devices for Rich Communication Suite (RCS) calling. Both features were enabled on this phone providing a potential remote attack surface.

Similar missed call traces and artifacts were observed in 2018 and 2019 when Android users were targeted by NSO Group customers using a zero-click vulnerability in WhatsApp. Research by Amnesty International and Citizen Lab has previously documented zero-click attacks against the iOS Voice-over-Wifi (VoWifi) service, exploited to deliver Pegasus spyware to iPhones.[233]

While the Security Lab cannot determine if these missed calls from invalid numbers are indeed traces of a zero-click infection attempt, this incident highlights the need for activists and security researchers to consistently monitor and collect evidence of possible attacks for analysis. Amnesty International believes that spyware companies such as NSO Group - whose Pegasus spyware was used by Serbian authorities during

[233] Donncha O'Cearbhaill (Amnesty International) and Bill Marczak (Citizen Lab), *Exploit archaeology: a forensic history of in-the-wild NSO Group exploits*, Virus Bulletin Conference September 2022, https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Exploit-archaeology-a-forensic-history-of-in-the-wild-NSO-Group-exploits.pdf

this time period in 2022 – continue efforts to develop and offer zero-click spyware vectors targeting Android devices.

10.4 ANNEX 4: FORENSIC ANALYSIS OF CELLEBRITE USE AGAINST "SLAVIŠA"

As Slaviša switched of his Android phone, and did not provide his pin code, it is likely the Serbian authorities needed to use a Before-First-Unlock ("BFU") attack to bypass the device lock screen and gain access to his device.

While it was not possible to confirm the exact vulnerability exploited by Cellebrite's UFED product in this case, traces indicate that phone was rebooted shortly before initial unlocking. Public reporting and leaked Cellebrite documentation describe the long-standing use of bootloader exploits to unlock and decrypt data stored on devices from multiple Android vendors.

Bootloaders customisations introduce by chipset vendors such as MediaTek and Qualcomm may introduce exploitable vulnerabilities, providing broad access to devices from multiple vendors using the same chipset, consistent with Cellebrite's Android support matrix.[234]

There are also indications that the device USB stack was corrupted. Cellebrite UFED and its associated Turbo Link hardware can emulate various USB devices and other peripherals such as HDMI devices. Around one hour after the successful unlocking, around 12:40, the phone experienced a kernel crash in an event handler for USB Human Interface Devices (HID).

The kernel crash may have triggered when the Cellebrite Turbo Link adapter was disconnected. Regardless of the trigger cause, the exception occurred when trying to kfree a USB *hid_device* kernel object which was corrupted. The exception call traces are listed below in Table 14.

Call trace: [2687.607828] -(0)[22123:kworker/0:3]Call trace:
Call trace line: [2687.607845] -(0)[22123:kworker/0:3] dump_backtrace+0x0/0x1b4
Call trace line: [2687.607858] -(0)[22123:kworker/0:3] show_stack+0x14/0x1c
Call trace line: [2687.607874] -(0)[22123:kworker/0:3] dump_stack+0xd4/0x10c
Call trace line: [2687.607892] -(0)[22123:kworker/0:3] mrdump_common_die+0xd0/0x148
Call trace line: [2687.607920] -(0)[22123:kworker/0:3] ipanic_die+0x30/0x40
Call trace line: [2687.607935] -(0)[22123:kworker/0:3] notify_die+0x64/0xb4
Call trace line: [2687.607958] -(0)[22123:kworker/0:3] die+0x118/0x27c
Call trace line: [2687.607979] -(0)[22123:kworker/0:3] bug_handler+0x4c/0x84
Call trace line: [2687.607999] -(0)[22123:kworker/0:3] brk_handler+0x9c/0x164
Call trace line: [2687.608019] -(0)[22123:kworker/0:3] do_debug_exception+0xc4/0x15c
Call trace line: [2687.608040] -(0)[22123:kworker/0:3] el1_dbg+0x18/0xb4
Call trace line: [2687.608060] -(0)[22123:kworker/0:3] kfree+0x4f8/0x578
Call trace line: [2687.608081] -(0)[22123:kworker/0:3] hid_close_report+0xc8/0x1b0
Call trace line: [2687.608100] -(0)[22123:kworker/0:3] hid_device_remove+0x98/0xe8
Call trace line: [2687.608125] -(0)[22123:kworker/0:3] device_release_driver_internal+0x130/0x1d4
Call trace line: [2687.608142] -(0)[22123:kworker/0:3] device_release_driver+0x14/0x1c
Call trace line: [2687.608163] -(0)[22123:kworker/0:3] bus_remove_device+0xdc/0x12c
Call trace line: [2687.608184] -(0)[22123:kworker/0:3] device_del+0x23c/0x3ac
Call trace line: [2687.608206] -(0)[22123:kworker/0:3] hid_destroy_device+0x28/0x5c
Call trace line: [2687.608228] -(0)[22123:kworker/0:3] usbhid_disconnect+0x4c/0x78
Call trace line: [2687.608250] -(0)[22123:kworker/0:3] usb_unbind_interface+0xb8/0x25c
Call trace line: [2687.608270] -(0)[22123:kworker/0:3] device_release_driver_internal+0x130/0x1d4
Call trace line: [2687.608293] -(0)[22123:kworker/0:3] device_release_driver+0x14/0x1c
Call trace line: [2687.608315] -(0)[22123:kworker/0:3] bus_remove_device+0xdc/0x12c
Call trace line: [2687.608334] -(0)[22123:kworker/0:3] device_del+0x23c/0x3ac
Call trace line: [2687.608357] -(0)[22123:kworker/0:3] usb_disable_device+0x90/0x384
Call trace line: [2687.608377] -(0)[22123:kworker/0:3] usb_disconnect+0xf4/0x250
Call trace line: [2687.608399] -(0)[22123:kworker/0:3] usb_disconnect+0xd4/0x250
Call trace line: [2687.608420] -(0)[22123:kworker/0:3] hub_event+0x920/0x15d8

[234] Roee Hay (Aleph Research, HCL Technologies), "*fastboot oem vuln: Android Bootloader Vulnerabilities in Vendor Customizations*". 2017, https://www.usenix.org/system/files/conference/woot17/woot17-paper-hay.pdf

Call trace line: [2687.608442] -(0)[22123:kworker/0:3] process_one_work+0x278/0x4d8 Call trace line: [2687.608461] -(0)[22123:kworker/0:3] worker_thread+0x2c8/0x568 Call trace line: [2687.608482] -(0)[22123:kworker/0:3] kthread+0x17c/0x18c Call trace line: [2687.608504] -(0)[22123:kworker/0:3] ret_from_fork+0x10/0x18

Table 14: Kernel crash in USB HID device handler

10.5 ANNEX 5: INTELLEXA CUSTOMER RELATED INFRASTRUCTURE

Domain	IP	Registrar	Registered	Notes
cellconn.net	93.86.50.174	123-Reg	2020-03-06	
telenorconn.com	93.86.50.218	123-Reg	2020-03-06	
prmopromo.com	93.86.50.174	NameSilo	2020-12-03	
bitlyrs.com	95.216.165.253	NameSilo	2020-12-03	Same IP as svetovid.bid
supportset.net	93.86.50.218	NameSilo	2020-12-03	
politika.bid	95.216.174.108	NameSilo	2020-05-22	
kormoran.bid	93.86.50.174	NameSilo	2020-05-23	Whois country listed as Serbia
bumabara.bid	93.86.50.174	NameSilo	2020-05-23	Whois country listed as Serbia
svetovid.bid	95.216.165.253	NameSilo	2020-05-23	Whois country listed as Serbia
danas.bid	93.86.50.218	NameSilo	2020-05-23	Whois country listed as Serbia
novosti.bid	88.99.173.101	NameSilo	2020-05-23	Whois country listed as Serbia

Table 15: Serbia related Intellexa Predator infrastructure

IP Address	ISP	First Seen	Last seen	Notes
93.86.50.174	Telekom Srbija	2020-06-02 (hosting cellconn.net)	2021-12-15	Matched Intellexa Predator backed fingerprint between 2021-10-18 and 2021-12-15.
93.86.50.218	Telekom Srbija	2020-06-06 (hosting danas.bid)	2021-12-15	Matched different Intellexa Predator backend fingerprint between 2021-10-28 and 2021-12-15

Table 16: Serbian IP addresses linked to Intellexa Predator system

10.6 ANNEX 6: NOVISPY SPYWARE SAMPLES AND INFRASTRUCTURE

Package	Sample	Notes
com.accesibilityservice	99673ce7f10e938ed73ed4a99930fbd6499983caa7a2c1b9e3f0e0bb0a5df602	
com.serv.services	087fc1217c897033425fe7f1f12b913cd48918c875e99c25bdb9e1ffcf80f57e	
com.li.activity	54ee2c4f3e2396b6f92def135d68abd35d63ca7f9c304633a36f705ba4728cb7	Older variant
com.gu.activity	d55e492d5fce87898e065572a5553d1ac1389cd12bf3d28cabc1218cb29780af	Older variant

Table 17: List of NoviSpy samples

Package	IP Address	ISP	Notes
com.accesibilityservice	195.178.51.251	Telekom Srbija	IP address associated with Serbian BIA
com.accesibilityservice	188.93.127.34	mCloud	Serbian hosting provider
com.serv.services	178.220.122.57	Telekom Srbija	
com.li.activity	195.178.51.251	Telekom Srbija	IP address associated with Serbian BIA
com.li.activity	79.101.110.108	Telekom Srbija	
com.li.activity	94.140.125.174	yourserver.se (Sia Nano IT)	Latvian hosting provider which accepts cryptocurrency payments
com.li.activity	185.86.148.174	yourserver.se (Sia Nano IT)	Latvian hosting provider which accepts cryptocurrency payments
com.li.activity	176.223.111.131	QHoster	
com.gu.activity	185.86.148.174	yourserver.se (Sia Nano IT)	Latvian hosting provider which accepts cryptocurrency payments
com.gu.activity	94.140.125.174	yourserver.se (Sia Nano IT)	Latvian hosting provider which accepts cryptocurrency payments

Table 18: Infrastructure associated with NoviSpy

10.7 ANNEX 7: CELLEBRITE RESPONSES TO AMNESTY INTERNATIONAL

Email from Cellebrite's Senior Director for Corporate Communications, to Amnesty International in response to the organization's research letter of 20 September 2024, received 5 October 2024 *(original emphasis)*:

> **Our responses are below:**
>
> Cellebrite's end-to-end Case-to-Closure digital investigative platform equips law enforcement agencies with technology needed to **protect and save lives, accelerate justice and preserve data privacy**.
>
> Cellebrite enables federal, state and local public safety agencies and enterprises around the globe to **ethically** collect, review analyze and manage data, supporting faster investigations and higher crime clearance rates.
>
> Cellebrite's digital forensics solutions 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.
>
> Cellebrite is not a surveillance company, and we do not provide cyber surveillance technology.
>
> Cellebrite's solutions are not "spyware," and using that term to describe Cellebrite's technology is false entirely inaccurate.
>
> We perform several human rights due diligence steps before doing business with any country's national, regional or local law enforcement and other defense or civil agencies countries and also have an independent ethics and integrity committee to guide our approach.
>
> Cellebrite has strict controls ensuring that our technology is used appropriately in **legally sanctioned investigations**.

Amnesty International received an additional statement from Cellebrite's Senior Director for Corporate Communications on 13 December 2024, shortly before publication, in response to a detailed set of research findings shared by Amnesty International with Cellebrite on 27 November 2024.

The response was received after the response deadline; as such it has not be impossible to incorporate this additional response in the report text itself. However, Amnesty International has included Cellebrite's additional response here in full in the interest of fairness:

> **Cellebrite Statement About Amnesty International Report**
>
> December 16, 2024
>
> We are aware of Amnesty International's report detailing its findings on the use of surveillance technologies against civil society in Serbia.
>
> Ethical, judicial and lawful use of our technology is paramount to our mission of accelerating justice and saving lives around the globe. 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.
>
> Cellebrite complies with the sanction lists from the United States and United Nations and Israel's export control regulations that prohibit doing business with certain nations. In addition, since 2020, Cellebrite has voluntarily ceased selling to customers in more than 60 countries, including certain countries specifically cited in the Amnesty International report.
>
> In 2021, we established an Ethics and Integrity Committee that advises our Board of Directors on responsible business practices. Each year, Cellebrite evaluates where it conducts business and determines whether to make any changes based on a wide range of factors, including the country's political structure and commitment to democracy, human rights and privacy. We remain committed to continue evolving our business practices in ways that will promote the ethical and responsible use of our technology by our customers around the world.

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

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 reveals Serbia’s pervasive and routine use of 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 also highlights widespread misuse of Cellebrite’s UFED mobile forensics tools against Serbian environmental activists and protest leaders.

INDEX: EUR 70/8813/2024
DECEMBER 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL