Unsafe anywhere: women human rights defenders speak out about Pegasus attacks

A new investigation led by Front Line Defenders reveals the hacking of two women human rights defenders (WHRDs) from Bahrain and Jordan using NSO Group's notorious Pegasus spyware. The hacking discovery comes on the heels of the Pegasus Project revelations of governments in the MENA region and beyond using the spyware to perpetrate human rights abuses and repress activists and journalists.

The impact of surveillance on women is particularly egregious and traumatizing given how governments have weaponized personal information extracted through spyware to intimidate, harass, and publicly smear the targets' reputations. As a result, women targets of surveillance live in a perpetual state of fear, become socially isolated and restricted in their social lives, work, and activism. As expressed by one of the victims, Ebtisam Al-Saegh, **"personal freedoms are over for me, they no longer exist. I am not safe at home, on the street, or anywhere."**

The investigation: who was hacked and how

Between November and December 2021, Front Line Defenders worked with WHRDs in Bahrain and Jordan through its Digital Protection program, which provides hands-on practical support to human

rights defenders around the world. Front Line Defenders analyzed devices with assistance from The Citizen Lab and Amnesty International's Security Lab for validation of Pegasus targeting.

BAHRAIN

While providing technical advice, researchers at Front Line Defenders examined the mobile device of Bahraini human rights defender Ebtisam Al-Saegh, and found that her iPhone had been hacked at least eight times between August and November 2019 with NSO Group's Pegasus spyware.

Ebtisam Al-Saegh is an internationally respected human rights defender who works for SALAM for Democracy and Human Rights, an NGO that fights for democracy and human rights in Bahrain.

Bahraini authorities have previously harassed Al-Saegh. On March 20, 2017, authorities detained her for seven hours at Bahrain International Airport upon her return from the 34th session of the U.N. Human Rights Council. They thoroughly searched her, interrogated her for five hours, and confiscated her passport and mobile device. The interrogator accused her of delivering false statements about Bahraini human rights violations while in Geneva.

On May 26, 2017, Bahrain's National Security Agency summoned her to Muharraq police station. Interrogators subjected her to verbal abuse, physically beat and sexually assaulted her, and threatened her with rape if she did not halt her human rights activism. They released her at approximately 11:00 pm and she was immediately taken to a hospital.

Front Line Defenders' forensic investigation found that Ebtisam al-Saegh's phone was compromised multiple times in August 2019 (on the 8th, 9th, 12th, 18th, 28th and 31st), on September, 19, 2019, and on November 22, 2019. Traces of process names linked to Pegasus were identified on her phone, including "roleaccountd," "stagingd," "xpccfd," "launchafd," "logseld," "eventstorpd," "libtouchregd," "frtipd," "corecomnetd," "bh," and "boardframed." Amnesty International's Security Lab and The Citizen Lab attribute these process names to NSO Group's Pegasus spyware.

JORDAN

Front Line Defenders also examined the phone of Jordanian human rights lawyer Hala Ahed Deeb, discovering that her device had been infected with Pegasus spyware since March 2021.

Hala Ahed Deeb has worked with a number of human rights and feminist organizations to defend

women's rights, workers' rights, and freedoms of opinion, expression and peaceful assembly in Jordan. She defends prisoners of conscience in Jordan and is a member of the legal team defending the Jordan Teachers' Syndicate, one of Jordan's largest labor unions, which the Jordanian government dissolved in December 2020 in response to mass protests. Deeb also headed the legal committee of the Jordanian Women's Union and continues to defend women victims.

Hala Deeb's phone was compromised by Pegasus on March 16, 2021. Traces of process names linked to Pegasus were identified on her phone, including "bluetoothfs," "JarvisPluginMgr," and "launchafd." Amnesty International's Security Lab and The Citizen Lab attribute these process names to NSO Group's Pegasus spyware.

Many other women human rights defenders and journalists in the MENA region and beyond have also been recently targeted with Pegasus spyware. This includes Emirati activist Alaa Al-Siddiq, Al Araby journalist Rania Dridi, and *Al Jazeera* broadcast journalist Ghada Oueiss, to name a few.

How Pegasus attacks work

Developed by Israeli surveillance firm NSO Group, Pegasus spyware exploits technical vulnerabilities in a victim's device to covertly gain access to the device and extract data, including text messages, emails, media, microphone, camera, passwords, voice calls on messaging apps, location data, call logs, and contacts. The spyware can also potentially allow an attacker to activate the phone camera and microphone, to spy on an individual's calls and activities. As such, Pegasus not only enables the surveillance of the target, but also the target's communications and interactions with other people.

Surveillance as a form of violence against women: the targets speak out

The use of targeted digital surveillance tools such as NSO Group's Pegasus spyware violates the right to privacy, and the rights to freedom of expression, association, and peaceful assembly. Such abuses are abundantly evident in the aftermath of the Pegasus Project, which, as we note above, has been documenting the severe harms surveillance inflicts on human rights defenders, journalists, and activists.

Surveillance technologies are often used to target human rights defenders to dissuade them from continuing their human rights work, to infiltrate their networks, and to gather information for use against other targets, for example. The use of surveillance technology against HRDs and journalists contributes to a chilling effect in which defenders are aware they may be targeted through these

technologies and therefore may become fearful to continue their work. Online spaces have become an increasingly hostile environment for WHRDs, and in some cases, online attacks have led to grave rights violations offline.

The impact of targeted surveillance on women can be particularly grievous, given that political, societal, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing. This can include the publishing of private and intimate photos and conversations online.

The United Nations defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual, or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life." This includes "physical, sexual, and psychological violence perpetrated or condoned by the State, wherever it occurs."

The spyware attacks have had a devastating impact on Ebtisam Al-Saegh and Hala Deeb. Since they discovered their phones were infected, they have each been living in a state of daily anxiety and fear. They are especially afraid of the possibility of exposing other women activists and victims they work with, and concerned that their families and friends are now at risk.

The chilling effect of surveillance has also led to the social isolation of the targets. The malicious capabilities that Pegasus spyware provides to perpetrators not only strip women of privacy, the surveillance also destroys the inviolability of their homes and immediate surroundings. Friends and relatives distance themselves in fear of also being harmed or surveilled.

Furthermore, surveillance has restricted the targets' freedom of movement out of their fear of physical harassment and threat. As Indian digital rights lawyer Vrinda Bhandari previously noted: "When their phone is hacked, women experience this not just as a privacy violation, but also as a violation of their bodily integrity — akin to bodily violence." Before Alaa Al-Siddiq's tragic death, for instance, one of her friends testified to how she changed her habits in fear of surveillance, including "changing routes she traveled on the tube. She tried to be mindful to not stand too close to the edge when she was traveling by train, for fear she could be pushed [onto] the tracks."

In Al-Saegh's case, the hacking of her device deprived her of being fully free at home, forcing her to wear her veil even when she is home alone — afraid of being watched.

For women targets, digital surveillance is a ticking bomb. They live in fear of how their personal information, including private photos, videos, and conversations, could be used against them at any given point, opening the door for harassment and abuse. **This is especially worrying in a region where governments have routinely used doxxing of women and LGBTQ+ activists in order to**

smear and intimidate them into silence.

Recommendations

To Jordanian and Bahraini authorities:

- Conduct independent and transparent investigations into the targeted surveillance of women human rights defenders Hala Ahed Deeb and Ebtisam Al-Saegh, respectively.

To all States:

- Place an immediate moratorium on the use, sale, and transfer of surveillance technologies produced by private firms until adequate human rights safeguards and regulation is in place.
- Hold surveillance companies accountable for their human rights impacts by developing a legal framework which requires surveillance companies to conduct human rights due diligence to identify, prevent, mitigate, and remedy any human rights impacts of the use of their products and services. This should be conducted before the sale or transfer of any surveillance technology and throughout any partnerships with other companies and/or governments and include liability for harms which are not properly prevented.
- Establish an independent mechanism with oversight of companies selling spyware to monitor and investigate their use and ensure that use is consistent with human rights.
- Adopt legislation that mandates transparency on the sale and use of surveillance technologies, including on human rights due diligence processes and outcomes.
- Ensure that any legislation that is adopted to regulate surveillance technology companies is developed in consultation with human rights defenders who have been impacted by the misuse of surveillance technologies.

To the European Union and its Member States:

- Move to take serious and effective measures against surveillance technology providers like NSO Group, including the designation of such entities under the E.U.'s global human rights sanctions regime.
- Raise concerns both publicly and privately with Jordanian and Bahraini authorities over the targeted surveillance of Hala Ahed Deeb and Ebtisam Al-Saegh and redouble support for women human rights defenders in the region.
- Alert potentially affected communities, organizations, and individuals to the risks of private surveillance technology, provide funding and technical support for civil society actors, journalists, and technologists working to identify and mitigate risks related to spyware, and issue advisories to those traveling to and living in countries shown to use spyware to target civil society.

What you can do

These two women human rights defenders have stepped forward to tell their stories — sharing how the use of Pegasus spyware has harmed their lives, their work, and social relations. They do this with the understanding that while being public might carry some additional risk, the awareness that can be raised for others is far more important.

Companies such as NSO Group that profit from such human rights abuses must be held accountable. **Read and share their personal testimonies below to ensure their voices are heard.**

Ebtisam El-Saegh's testimony

I am in a state of daily fear and terror after I was informed by Front Line Defenders that I was spied on, and this terror is connected to the fact that those people who spy on me have no morals and can access personal information and use it in a bad way.

I started to be afraid of having the phone next to me, especially when I am in the bedroom or even at home among my family, my children, and my husband, because I know that this phone is spying on me and perhaps there is someone who is trying to find out what is going on right now.

I work in human rights, but how is my family at fault, such that they are spied on through my phone and their privacy is violated? We live in a conservative social environment and society can be merciless. The publication of personal photos could smear my professional image, which I built over years through my work in society as well as in human rights.

This fear has restricted my work. I am constantly anxious and afraid that I have put others at risk because of their contact with me, and also that I have put my family in a bad position.

I am afraid to leave my house or go out in public spaces to face the unknown after the surveillance and intrusion into my family and home life through this phone.

During my work years and due to its risky nature, I lost many people close to me who were part of my community, including friends with whom I had a relationship for many years. A lot of family members also distanced themselves from me — they are afraid to visit or meet with me. When I learnt I was being surveilled and informed them, their fear grew. It confirmed their theory that someone is spying on me and that I may harm them.

My small family has always supported me, but they never imagined that they would not be safe in

their own home, which is supposed to be a safe space for anyone and any family in the world.

Everyone today has things the family keeps secret, and because of the Corona situation, sensitive family issues are now discussed using online communications. Mobile phones are used extensively in family communication, and everyone has family groups in communication applications.

I can't believe that all of this is exposed, that our personal photos we take to remember the happy moments in our lives can turn into a weapon used against us, into a calamity.

Surveillance will make me lose more friends and family members. More will distance themselves from me. I cannot blame them because previously they had nothing to fear while we were at home.

The victims will also be afraid to communicate with me, especially now as we communicate more online. As I mentioned earlier, this will affect my work as a human rights defender and many of the people I try to help, especially women.

I believe that human rights work has a price to pay, but I did not want to direct my energy and effort to fighting surveillance or addressing the digital security issues I now face. Front Line Defenders helped me a lot and I have become more confident that my information is safer now.

Home used to be the only safe space for me, a place for personal freedom where I can take off the veil and exercise my religious and social freedoms without limits. Now, I wear my veil even inside the house sometimes. I cannot live my life as I used to. Home is not safe anymore.

I do not rule out that this information will be exploited in the future. There were past incidents where personal photos of women at private wedding parties were confiscated and doxxed on the internet, which shattered social relations, especially as we live in a conservative society that sees women differently.

I am also afraid and anxious about accessing my financial information, which could be used to tarnish my reputation or make false accusations against me.

My life has changed completely after I was informed that my phone was hacked. I became afraid and anxious, especially as I use my phone on a daily basis to send and receive information. I'm afraid this information will be used against me, especially as I am in contact with victims sometimes to educate them on human rights.

Uncertainty is frightening, especially when you know that some people have died because they were spied on.

The companies that contributed to our suffering, especially the suffering of us women, must be held accountable. And psychological and moral support must be provided to those affected.

Personal freedoms are over for me, they no longer exist. I am not safe at home, on the street, or anywhere.

Hala Ahed Deeb's testimony

As a human rights defender, I used to believe that human rights are interdependent and indivisible. When I did human rights training, I always started with the question: what is the most important human right? Together with the trainees, we often came to the conclusion that no right is more important than the other and that all rights are necessary; one cannot enjoy one without the other. But suddenly, when I learned that my phone was hacked, I realized that the right to privacy is not just a right that we enumerate with other rights. **When your privacy is violated, you feel violated, naked, and with no dignity— this is how I feel.**

I have often said that I have nothing to hide, but I realized that privacy in itself is my right. I decide what information I want to share and with whom, I decide what image I paint for myself, how I define its contours and features. As a woman, what is considered private becomes bigger, and as a woman living in a conservative society this private realm becomes bigger and bigger.

Today, I feel isolated. I do not communicate with my friends and I avoid talking on the phone as much as I can. I practice a kind of self-censorship sometimes when I wonder what behaviors would provoke those who hacked my phone? How will they use this against me? I apologize for missing meetings, discussions, and sometimes conversations to avoid implicating people talking freely because they might be reached through the hacking of my phone, especially women for whom I take cases or other defenders and activists.

For the first time, I have gotten scared if someone gets close to me on the street, or accidentally walks in the same direction. I've become less communicative with people, I move less. I wonder if there is surveillance in my house, in my office, in my car, the new phone? Because of the hacking of my phone, I feel I no longer have a space to express myself and continue working on the cases I defend, which may be the reason for the targeting. I know there is a price for it and I should have expected it. It will not deter me from continuing my work, no, but I do not deny that it is a high price!

My concern today is about how this hack will be used: will it be a way to threaten others through

what has been collected from my phone? Will it be used to blackmail me? Will my information be shared with other parties? Will legal cases be framed against me or leak my information or photos?

As a woman, our space for movement is often limited, despite being human rights defenders. Surveillance makes it more limited and takes away the ability we have to try to expand our spaces. It forces your close circle of family and friends to deter you and dissuade you from what you are doing, because on the one hand, they are worried about you, and on the other, they too are affected by surveillance.

What is psychologically and mentally disturbing about surveillance is that it does not affect you alone, but also harms others, especially those whom you spend your life defending and protecting. Now you wonder how this may affect them, whether it's by attackers publishing their information or causing them fear and anxiety, just because they are your family or friends.

This report is a collaboration between Access Now and Front Line Defenders.

CONTACT INFO

Marwa Fatafta
MENA Policy Manager
marwa@accessnow.org

Mohammed Al-Maskati
Digital Protection Coordinator, Middle East and North Africa
mohammed@frontlinedefenders.org