Surveillance Is Intimidation: Ronan Farrow Reveals Secrets of High-Tech Spyware

Amy Goodman, Juan González ⋮ 27-34 minutes ⋮ 12/4/2024

We look at the world of high-tech surveillance with Pulitzer Prize-winning journalist Ronan Farrow and filmmaker Matthew O'Neill. Their new HBO documentary *Surveilled* is now available for streaming. Farrow says he became interested in the topic after he was tracked by the Israeli private intelligence firm Black Cube during his reporting on Hollywood mogul Harvey Weinstein's sexual abuse. Although Black Cube used a "relatively low-tech approach," Farrow says the experience started him on a path to investigate more sophisticated methods of surveillance, including the powerful spyware Pegasus, which has been used against journalists and dissidents around the world. As part of the reporting for the documentary, Farrow traveled to Israel for a rare interview with a former employee of NSO Group, the Israeli software company that makes Pegasus. He warns that it's not just "repressive governments" that abuse Pegasus and other surveillance technology, but also a growing number of democratic states like Greece, Poland and Spain. U.S. law enforcement and intelligence agencies under both the Biden and Trump administrations have also considered such spyware, although the extent to which these tools have been used is not fully known. "Surveillance technology has historically always been abused. Now the technology is more advanced and more frightening than ever, and more available than ever, so abuse is more possible," says Farrow.

TRANSCRIPT

This is a rush transcript. Copy may not be in its final form.

AMY GOODMAN: This is *Democracy Now!*, democracynow.org. I'm Amy Goodman, with Juan González.

We turn now to a film that looks at the increasing use of spyware targeting journalists, human rights advocates, dissidents across Western democracies and around the world. The HBO original documentary *Surveilled*, which is airing tonight on HBO at 9 p.m., follows Pulitzer Prize-winning journalist Ronan Farrow, who uncovers how Pegasus and other surveillance programs are threatening democracy across the globe. This is the film's trailer.

> **RONAN FARROW:** Why should people around the world care about the hacking that you're documenting here?
>
> **ELIES CAMPO:** These cases affect 450 million people. It's a violation of their rights.
>
> **CLAUDIU DAN GHEORGHE:** What we ended up finding was actually the tip of the iceberg.
>
> **RONAN FARROW:** Spyware is this powerful surveillance tool. Big spyware

companies say they sell this tech only to governments. But this multibillion-dollar industry is mostly unregulated. The most advanced spyware can turn your smartphone into a spy in your pocket. It can copy everything and record you without you ever knowing, and then just disappear without a trace.

This company, NSO Group, makes Pegasus, advanced spyware reportedly deployed in at least 45 countries, with allegations it's being used to target journalists, human rights activists and political dissidents.

What's the most objectionable thing that you saw in your time at the company?

NSO GROUP WHISTLEBLOWER: One of the moral problems that I had was the journalist murder.

RONAN FARROW: Should people be concerned?

NSO GROUP WHISTLEBLOWER: Definitely, yes.

RONAN FARROW: Does NSO know that some of its customers are abusing this technology?

REP. JIM HIMES: This tool could fall into the hands of the Iranians, the North Koreans, the Chinese. We need our experts to know what is out there.

ELIES CAMPO: They targeted my family. My mom, she worked at the hospitals, so they had access to hundreds of data of patients all around the world.

RONAN FARROW: Do you think it's headed down a path of more domestic impact?

NATHANIEL FICK: These technologies, any nefarious use that we can imagine, we're probably going to see.

AMY GOODMAN: The trailer to the new HBO original film *Surveilled*, now streaming on Max, the film directed by Perri Peltz and Matthew O'Neill.

On Tuesday, *Democracy Now!*'s Juan González and I spoke with Matt O'Neill and Ronan Farrow, who produced the film. Ronan is a contributing writer at *The New Yorker*, his latest article headlined "The Technology the Trump Administration Could Use to Hack Your Phone."

I began by reading to Ronan from a recent article in *The Guardian* that notes, "In 2017, while reporting on a story on Harvey Weinstein that would, along with a *New York Times* report, kick off the #MeToo movement, the investigative journalist Ronan Farrow found himself the target of covert surveillance. The efforts to suppress investigations into Weinstein's history of sexual abuse, for which the Hollywood mogul paid the Israeli private intelligence firm Black Cube, were mostly old-school," unquote.

I asked Ronan Farrow to lay out what happened.

RONAN FARROW: Well, I got a firsthand view of the toolkit that powerful institutions and individuals can deploy when they're trying to suppress reporting.

And I saw it on a miniature scale, where one mogul did this, frankly, insane maneuver of retaining a private intelligence company that literally hired actors, former military and intelligence people from Israel, to play roles and insinuate themselves into individuals' lives who were around the story. That included sources that I was working with, women who, as it turns out, had allegations of assault against Weinstein. It included journalists working on the story, including me.

And so, there was a two-pronged approach. There were people posing as people who wanted to talk to us, wanted to get close to us, and then there were also subcontractors who were hired to just do the traditional gumshoe work of staking people like me out. I had two guys outside of my apartment. And eventually I was able to get the contracts and all the signatures of the lawyers and prove that this operation was happening, and get sources inside this company, Black Cube, to describe what they were doing. And actually, one of the subcontractors that was following me around all the time, sometimes using some high-tech approaches, too — pinging my phone, getting my geolocation data so they could follow me to meetings — one of them became a source in the end. So, I wrote a book about this, *Catch and Kill*, and there's a documentary series on that, if people are interested in more.

But I did, through that experience, through this relatively low-tech approach to surveillance, get a little picture of how personally devastating it can be to have your private interactions monitored in that way. In this case, there were real stakes, because I was talking to whistleblowers around this story who were risking everything and couldn't be uncovered, if I wanted the story to go forward. And I also saw how unsafe it makes you feel. Surveillance of journalists — and, you know, this goes for surveillance of dissidents, it goes for surveillance of political opposition members that we see in the film and in the world now so often — is not just information gathering. Surveillance of this type is intimidation, and it shrinks the space for all kinds of expression in democracies.

JUAN GONZÁLEZ: Yeah, Ronan, from that relatively low-tech type of surveillance to what we're confronting today and in recent years, how did then you decide to cover this aspect of the high-tech surveillance?

RONAN FARROW: Well, through that reporting, I developed sources in the Israeli private intelligence world. And I spent some time in Tel Aviv. I spent some years getting close to people in this industry, in this world. And I clocked, through my own experiences, just how pivotal a challenge this is.

For anyone who cares about maintaining people's basic rights and maintaining the free flow of information in democracies in order to protect those rights, surveillance, I realized, was a linchpin. It wasn't some sidebar issue. It was one of the tools that people use to try to suppress democracy, to suppress the free flow of information. It is part of the authoritarian playbook that we see historically again and again, that police states emerge where there are oversteps into privacy violations.

And I realized, as I was looking at this issue and experiencing these dynamics as a journalist myself, that the bleeding edge of this kind of surveillance, and the

thing that was transforming it and making it more available and more intrusive and scarier, was this modern spyware that can take control of phones, at a time when we're more and more enmeshed with our phones. And I realized that this was one of the foremost challenges confronting journalists around the world, and also one of the challenges that anyone, even if you don't think of yourself as being in a vulnerable category — you're not an activist, you're not a dissident — should care about and should understand, because phones are increasingly not private spaces.

I dealt with, in addition to being followed around, dynamics where personal information was leaked around stories. I worked on stories about Trump's collaboration with the *National Enquirer* that ultimately helped catalyze that indictment around Trump and the hush payments. And during that reporting, I also had intimate texts leaked. There were all sorts of efforts to use private information as a lever. So, I was just seeing how, again and again, if you want to expose the truth, if you want to be a voice of opposition to power, you're inevitably dealing with this kind of surveillance. And I was seeing how the highest-tech version of it was the scariest, was the most secretive, was the most poorly understood.

AMY GOODMAN: So, tell us about Pegasus. And this amazing film, *Surveilled*, takes us to Israel, takes us to your investigation of the company and who the company is selling to.

RONAN FARROW: So, the biggest players in the spyware market, which is now a multibillion-dollar industry — and it mostly is comprised of companies that want to stay secretive. So, there's not a lot of reporting on this. There's not a ton of public-facing websites. Companies that do have a kind of public-facing presence, they don't actually talk about what they do or who their clients are. This is one reason why the reporting was necessary.

Now, in this multibillion-dollar industry, the big players claim, in a bid for legitimacy, that they only sell to government offices, mostly government intelligence agencies, government defense offices. But the technology that's privately available for purchase by those offices is now cheaper, more efficient, more intrusive. So what you're seeing is two categories of change. You're seeing governments that previously didn't have the size and the resources to have a CIA-style high-tech surveillance operation just buy a kind of CIA in a box. You know, we talk in the film to officials in small Western democracies who love this technology — and, by the way, I should point out, small Western democracies where the populations of those countries don't yet know that this technology is being used against them. And we hear from those officials how they think it's great that they can, ostensibly, in some of these cases with warrants, but much more freely and cheaply, just hack into people's phones as needed in law enforcement operations.

There are legitimate arguments for the use of this technology, like with any surveillance technology. And theoretically, in those Western democracies where there's a process to get a warrant, this is something that shouldn't have to be scary. But what we see over and over again is that it just gets abused — I would argue, inevitably. Surveillance technology has historically always been abused. Now the technology is more advanced and more frightening than ever, and more

available than ever, so abuse is more possible and more ready than ever.

What we've seen in the last few years is not only that repressive regimes with a poor human rights record are using this technology against journalists and against dissidents, against political opposition members, and sometimes, by the way, with dangerous and even deadly results. There have been studies that have linked hundreds of cases of violence to spyware technology. A lot of the players involved, including NSO Group, deny this, but NSO Group's flagship technology, Pegasus, was allegedly found on the phone of at least one associate close to Jamal Khashoggi in the time frame when he was murdered by the Saudi regime. We see this over and over again. Javier Valdez in Mexico, great reporter who was working on cartel stories, was killed. People around him had had Pegasus on their phones. So, that's the pattern under repressive regimes.

But we're seeing not only that, but also one Western democracy with an ostensible commitment to human rights after another see scandals in which this technology is purchased and then overused. We've seen it in Greece. We've seen it in Poland, where just this week a former spy chief in that country was actually arrested as part of inquiries into a massive spyware dragnet that happened under the previous administration there. And we've seen it in Spain, where some of this film is set, and where we helped document this massive cluster of hacks where the Spanish government, which you wouldn't think would be a player that would be responsible for this kind of a breach, they just hacked one civil society member after another associated with a separatist movement, but a peaceful one, in Catalonia.

JUAN GONZÁLEZ: And, Matthew O'Neill, you're the director of the film. And specifically the focus of the film on Spain and the independence movement in Catalonia, what most surprised you in doing that work in Spain?

MATTHEW O'NEILL: Well, I think when Perri Peltz and I first sat down with Ronan — and Perri's the other director of the film — when he started talking about the way his reporting was leading to Spain. We had heard of Pegasus. We think it's a really important subject, this cyberespionage. We associate it with autocracies, Saudi Arabia, the — imagine the capabilities of a Russia or a China. But that this was happening in Spain, and that Ronan was sitting on the cusp of exposing what at that point was the largest cluster of Pegasus infections inside any one place, in one group — I think it started with 67, now it's in the hundreds — our eyes were opened, because it felt like this story, what was unfolding in a democracy, in a U.S. ally, was something that people needed to know about.

And our idea, as we talked about how to tell this story, because Ronan's reporting was already so extensive, was: What could we do to give the audience access to Ronan's process and see the reporting and the discoveries unfold? And that's part of what makes *Surveilled*, I think, really interesting. Perri and I have been longtime admirers of Ronan as a journalist and a reporter, and this gave not only us, but all of you at home, the opportunity to ride along shotgun with him.

AMY GOODMAN: So, this is a clip from the HBO documentary *Surveilled*, in which our guest, Ronan Farrow, speaks with the Citizen Lab's Elies Campo in Catalonia.

RONAN FARROW: Why should people around the world care about the hacking that you're documenting here in Catalonia?

ELIES CAMPO: This is going to be one of the first cases where there is such a large and vast number of affected people and from a vast and different type of categories of society. So, we've had the Parliament of Catalonia targeted. We've had the government of Catalonia targeted. We've had lawyers targeted. We've had civil leaders of cultural organizations of Catalonia targeted.

RONAN FARROW: This is not some future Orwellian scenario. It really — it happened here. It's happening here.

ELIES CAMPO: It's happening here.

AMY GOODMAN: And this is another clip of the HBO documentary *Surveilled*, featuring Jordi Solé, a Catalan politician, former member of the European Parliament.

ELIES CAMPO: [translated] The iPhone will generate a diagnostic file which won't include personal data. We just received confirmation that your phone was hacked twice: once on the 11th of June and then again on the 27th of June.

JORDI SOLÉ: 2020?

ELIES CAMPO: 2020.

RONAN FARROW: When does it look like you were infected?

JORDI SOLÉ: I have to check its date, but around the day I was appointed member of the European Parliament.

RONAN FARROW: How do you feel, knowing that you may have been compromised in this way?

JORDI SOLÉ: Well, I feel surprised and angry at the same — at the same time.

AMY GOODMAN: So, that's the Catalan politician, former member of the European Parliament, Jordi Solé, and, before that, Elies Campo, who is the investor. He lives in Barcelona. His sister and parents were also — their phones were infected with Pegasus. Ronan Farrow, if you can talk about the significance of this? And it goes to the whole issue of you've got a spy in your pocket. Exactly what are the authorities, those who are paying for this, the information they're getting from your phone?

RONAN FARROW: Well, everything, potentially. People have to start realizing that their phones are now public spaces in so many ways, even if you're just a person using your phone in a run-of-the-mill way and you don't think you're in one of these vulnerable categories. Anyone with the resources can hack your phone if they want to. Any country, even places where there are supposed protections of

privacy rights, are now battlegrounds over this technology, where we are seeing people like the sister and parents of Elies Campo, who you mentioned, who are apolitical, getting caught up in surveillance dragnets.

I've been, in my ongoing reporting in recent weeks, talking to privacy law experts who really stress at this point that one should know about this and care about this and exercise good digital hygiene and get the protections that you can, maybe even get your phone tested, whether you are, again, in a vulnerable category or not. And so, in this case in Spain, you saw people like Elies's parents, who are just doctors, have all of their patients' sensitive records and photos and scans just divulged to whoever wants to use them. All they know is the government now potentially has all of this information.

AMY GOODMAN: And the phone becomes a microphone?

RONAN FARROW: Pegasus and other similar competing technologies can turn on your microphone without you knowing, can turn on your camera and record video without you knowing, and send all of that information back to whoever has purchased and is working with NSO, or whatever the spyware company is, to operate the technology.

JUAN GONZÁLEZ: And, Ronan, if a person did want to disinfect their phone if they suspected that they were being surveilled, is there a new industry arising now to basically check phones? And are we seeing sort of an arms race between the surveillance folks and the anti-surveillance folks in terms of these smartphones, that almost virtually everyone has in their pocket?

RONAN FARROW: Well, when I talk about the world now being a battlefield over this technology, one of the fights, one of the fronts in that battle, is between the technology companies, the platform holders that operate your operating system on your phone, like Apple, that operate your messaging applications, like WhatsApp, and on the other side of the battlefield, the spyware companies.

So, in the film and in my print reporting, I talked to both the programmers at, for instance, WhatsApp, who every day there's a team within that company, within Meta — now owns it — looking at: What are the attempts to intrude on this technology? What are these, at times, astonishingly creative technical solutions that allow this technology to worm its way into your phone through little vulnerabilities in the code? And then I also talked to the programmers at, for instance, NSO Group, who are really proud of that daily fight where they find creative solutions to get into the phones, and who have to exercise a lot of rationalization, frankly, is my view, in the face of all this evidence that those efforts are being misused and abused to target vulnerable people.

AMY GOODMAN: So, in the film *Surveilled*, you interview a whistleblower — right? — at NSO. Ronan Farrow interviews an NSO whistleblower who's asked for anonymity.

> **RONAN FARROW:** So, you're hacking these phones. What kinds of reactions did you get?

NSO GROUP WHISTLEBLOWER: It's jaw-dropping. It's very impressive the first time that you see it.

RONAN FARROW: What was the pitch that you were offering these governments?

NSO GROUP WHISTLEBLOWER: Usually, we had like one iPhone, one Android device, we used to demonstrate how we can exfiltrate the data from those devices, actively take snapshots of the screen or pictures from the camera, actively record through the microphones.

RONAN FARROW: What should the average citizen in any country in the world know about this company and this technology?

NSO GROUP WHISTLEBLOWER: It's very powerful. It's very intrusive.

RONAN FARROW: Should people be concerned?

NSO GROUP WHISTLEBLOWER: Yeah, yeah.

AMY GOODMAN: "We're telling these governments how to exfiltrate the data," he says, and his voice is disguised as you talk to him, an NSO Group whistleblower. And they make Pegasus. So, if you can talk about the U.S. buying this technology, from Trump to Biden?

RONAN FARROW: Under multiple administrations of both parties, we have seen overreaches of surveillance technology. Under the first Trump administration — *The New York Times* has reported extensively on this — there was actually a purchase of this very technology, Pegasus, which, again, can seize control of a phone, turn it into a listening device, disgorge all of your private data, by the FBI. So, the FBI purchased — later, Christopher Wray, the FBI director, told Congress — just for testing purposes, a Pegasus account. And they did it through a subcontractor. Later, *The New York Times* sued for more information, that showed pretty clearly that this was not clearly delineated just for testing purposes. There was a whole conversation within the FBI where they wanted to deploy this, potentially on American soil, in an operational, very real way. Now, as far as we know, that didn't happen. That stopped.

And under the Biden administration, there have been halting efforts, at least of a limited quality, to curtail the use of this technology. There's often dissensus and tension across the government on this. I know of cases that have not yet been made public, where Department of Justice offices, where Department of Defense offices have purchased foreign private spyware technology to help in their efforts, because not all of these offices have the resources of the CIA. Now, the Biden administration, in response to my reporting calls, did announce — and we disclosed this for the first time publicly in one of my *New Yorker* stories — an executive order where they essentially said foreign spyware that has a record of being abused can't be, shouldn't be purchased by the U.S. government. But the standards for what meets that criterion are really amorphous. And what we've seen since then is that the U.S. government has gone right on purchasing more

spyware.

Just this past fall, we saw the Department of Homeland Security — and there's been reporting that this is specifically ICE, the immigration office under the Department of Homeland Security — purchase another really powerful Israeli spyware technology called — it's a company called Paragon, and the technology is called Graphite. And, you know, I have sources within that company. They do bill themselves as a more ethically clean alternative. And one of the things that they promised the U.S. government in the vetting process that led up to this multimillion-dollar contract was that they would put restraints on how other clients, other foreign governments that use their technology, can use it to hack American citizens. But we don't know how exact those restraints are. And more to the point, there are no restraints on hacking people in America, including Americans, by ICE itself, by the Department of Homeland Security itself. And privacy law experts have been in a state of high alarm about this, partly because they point out that the Department of Homeland Security is often the U.S. government office that purchases ethically and legally questionable technology and is able to circumvent a lot of scrutiny by arguing that they have a law enforcement, national security basis for using it.

So, you now have a perfect storm, Amy, of technology of this type, that's really powerful and really easily abused, in the hands of the U.S. government, again, under the Biden administration. The Biden administration has, in response to reporting on this, just recently, paused that contract. They say they're reviewing it. But the thing is, right around the corner, the Trump administration is coming in. And we can talk about this, but obviously the Trump administration is bringing in a raft of officials, and Trump himself, who have made explicit threats against the groups that, again and again in Western democracies, have been most vulnerable to this kind of espionage.

AMY GOODMAN: That's Pulitzer Prize-winning journalist Ronan Farrow and Matthew O'Neill talking about their new documentary *Surveilled*. It airs tonight at 9:00 on HBO, is streaming at Max. We'll link to Ronan's *New Yorker* article, "The Technology the Trump Administration Could Use to Hack Your Phone." We'll talk more about that with him tomorrow. I'm Amy Goodman, with Juan González. Thanks so much for joining us.

Journalism is a linchpin of that movement. **Even as we are reeling, we're summoning up all the energy we can to face down what's coming, because we know that one of the sharpest weapons against fascism is publishing the truth.**

There are many terrifying planks to the Trump agenda, and we plan to devote ourselves to reporting thoroughly on each one and, crucially, covering the movements resisting them. We also recognize that Trump is a dire threat to journalism itself, and that we must take this seriously from the outset.

After the election, the four of us sat down to have some hard but necessary conversations about *Truthout* under a Trump presidency. How would we defend our publication from an avalanche of far right lawsuits that seek to bankrupt us? How would we keep our reporters safe if they need to cover outbreaks of political violence, or if they are targeted by authorities? How will we urgently produce the practical analysis, tools and movement coverage that you need right now — breaking through our normal routines to meet a terrifying moment in ways that best serve you?

It will be a tough, scary four years to produce social justice-driven journalism. **We need to deliver news, strategy, liberatory ideas, tools and movement-sparking solutions with a force that we never have had to before.** And at the same time, we desperately need to protect our ability to do so.

We know this is such a painful moment and donations may understandably be the last thing on your mind. But we must ask for your support, which is needed in a new and urgent way.

We promise we will kick into an even higher gear to give you truthful news that cuts against the disinformation and vitriol and hate and violence. We promise to publish analyses that will serve the needs of the movements we all rely on to survive the next four years, and even build for the future. We promise to be responsive, to recognize you as members of our community with a vital stake and voice in this work.

Please dig deep if you can, but a donation of any amount will be a truly meaningful and tangible action in this cataclysmic historical moment.

We're with you. Let's do all we can to move forward together.

With love, rage, and solidarity,

Maya, Negin, Saima, and Ziggy