

Pegasus Project (investigation)

The **Pegasus Project** is an international investigative journalism initiative that revealed governments' espionage on journalists, opposition politicians, activists, business people and others using the private Pegasus spyware developed by the Israeli technology and cyberarms firm NSO Group. Pegasus is ostensibly marketed for surveillance of "serious crimes and terrorism". In 2020, a target list of 50,000 phone numbers leaked to Forbidden Stories, and an analysis revealed the list contained the numbers of leading opposition politicians, human rights activists, journalists, lawyers and other political dissidents.^[1]

More than half of these phones that were inspected by Amnesty International's cybersecurity team revealed forensic evidence of the Pegasus spyware, a zero-click Trojan virus developed by NSO Group.^[1] This malware provides the attacker full access to the targeted smartphone, its data, images, photographs and conversations as well as camera, microphone and geolocation. This information was passed along to 17 media organisations under "The Pegasus Project" umbrella name. Reports started to be published by member organisations on 18 July 2021, revealing notable non-criminal targets and analysing the practice as a threat to freedom of the press, freedom of speech, dissidents and democratic opposition. On 20 July, 14 heads of state were revealed as former targets of Pegasus malware.^[2] Various parties called for further investigation of the abuses and a limitation on trading such repressive malware, among them the newsrooms involved, the Committee to Protect Journalists, the International Press Institute, and Edward Snowden.

Contents

Software

Investigation

Origins and members

Investigative methodology

Findings

Regions and targets

Heads of state and government

Azerbaijan

Hungary

India

Italy

Mexico

Morocco

Saudi Arabia

United Arab Emirates

Reactions

NSO Group's response

Vetting and licence contract

Involvement denial and deresponsibilisation

Journalists/NGOs

Companies

National governments

Algeria

France

Hungary

India

Israel

Kazakhstan

Morocco

Pakistan

Rwanda

Saudi Arabia

United Arab Emirates

Other reactions

Government investigations

See also

References

Software

The Pegasus spyware was developed by the Israeli cyberarms firm NSO Group. It can be covertly installed on mobile phones (and other devices) running most^[3] versions of iOS and Android. The spyware is named after the mythical winged horse Pegasus—it is a Trojan horse that can be sent "flying through the air" to infect phones.^[4] Usages of the Pegasus spyware have been monitored for years. Amnesty has argued that the digital invasion is correlated with real-life consequences for spied targets, via psychological or physical damages.^[5]

The NSO Group exports are overseen by the Israeli Ministry of Defense's Defense Exports Control Agency (DECA).^[6]

Investigation

Origins and members

In 2020, a list of over 50,000 phone numbers believed to belong to individuals identified as "people of interest" by clients of the Israeli cyberarms firm NSO Group was leaked to Amnesty International and Forbidden Stories, a media nonprofit organisation based in Paris, France. This information was passed along to 17 media organisations under the umbrella name "The Pegasus Project". Over several months, over 80 journalists from The Guardian (United Kingdom), Le Monde and Radio France (France), Die Zeit, Süddeutsche Zeitung, WDR and NDR (Germany), The Washington Post and Frontline (United States),^[7] Haaretz (Israel), Aristegui Noticias and Proceso (Mexico), Knack and Le Soir (Belgium), The Wire (India), Daraj (Syria),^[8] Direkt36 (Hungary),^[9] and OCCRP investigated the spying abuses.

Investigative methodology

The leaked list of targeted phone numbers provides an indication of being a "person of interest" and a first indication of possible hacking, to be confirmed via direct forensic examination of the phone. Amnesty has published *Forensic Methodology Report: How to catch NSO Group's Pegasus*.^[3] According to Amnesty, "The Citizen Lab at the University of Toronto has independently peer-reviewed a draft of the forensic methodology outlined in this report. Their review can be found [here](https://citizenlab.ca/2021/07/amnesty-peer-review/) (<https://citizenlab.ca/2021/07/amnesty-peer-review/>)."^[3] Amnesty also published various tools or data from this investigation, including a Mobile Verification Toolkit (MVT)^[3] and a GitHub repository listing indicators of NSO/Pegasus compromised devices.^{[3][10]} Some emerging unverified online services claim to be able to assess an infection by Pegasus, but their usage is discouraged as possible scams themselves.^[11] Amnesty and Forbidden Stories received numerous queries for checking devices but were not able to satisfy the demand for assistance.^[11]

Findings

The investigation suggested that Pegasus continued to be widely used by authoritarian governments to spy on human rights activists, journalists and lawyers worldwide, although NSO claims that it is only intended for use against criminals and terrorists.^{[1][12]}

A French journalist noted that "in a matter of cyber-surveillance, we observe that abuse is *de facto* the rule".^[13] Forbidden Stories argues the Pegasus software and its usages *de facto* constitute a global weapon to silence journalists.^[14]

Forensic Architecture and the Pegasus Project lead a data analysis and built a data visualisation plotting attempt hacking of dissidents together with real-life intimidations, threats or violence. They have argued that Pegasus has become a key tool for states to repress their own people.^[15]

Regions and targets

Targets include known criminals as well as human rights defenders, political opponents, lawyers, diplomats, heads of state and nearly 200 journalists from 24 countries.^[16] *The Guardian* mentioned 38 journalists in Morocco, 48 journalists in Azerbaijan, 12 journalists in the United Arab Emirates and 38 journalists in India as having been targeted.^[17] Some of the targets whose names have been revealed are listed below; the list is non-exhaustive.

Heads of state and government

According to an analysis by the German newspaper *Die Zeit* and others, the following incumbent and former heads of state and government have been targeted,^{[18][19]} implying possible full access to their mobile phones' data:

- Abdelaziz Bouteflika, former President of Algeria^[20]
- Noureddine Bedoui, former Prime Minister of Algeria
- Mostafa Madbouly, Prime Minister of Egypt
- Charles Michel, former Prime Minister of Belgium and current President of the European Council
- Emmanuel Macron, President of France
- Édouard Philippe, former Prime Minister of France
 - Édith Chabre, wife of Édouard Philippe
 - Most French ministers

- Numerous French diplomats
- Barham Salih, President of Iraq
- Bakhytzhan Sagintayev, former Prime Minister of Kazakhstan
- Saad Hariri, Prime Minister of Lebanon
- Mohammed VI, King of Morocco
- Saadeddine Othmani, Prime Minister of Morocco
- Imran Khan, Prime Minister of Pakistan
- Cyril Ramaphosa, President of South Africa
- Ruhakana Rugunda, former Prime Minister of Uganda
- Ahmed Obeid bin Daghr, former Prime Minister of Yemen

Azerbaijan

- Fatima Movlamli, an Azerbaijani civil society activist and journalist opposed to local authoritarian government. Intimate photographs of her were leaked on Facebook in 2019 when she was only 18.^[17]

Hungary

Used against opposition journalists, opposition leaders and critics.

- Szabolcs Panyi, a Hungarian investigative journalist for Direkt36, hacked in 2019.^[21] Panyi joined the Pegasus Project investigation.^[21]
- András Szabó, a Hungarian investigative journalist.^[22]
- Dávid Dercsényi, a Hungarian investigative journalist (HVG).^[9]
- György Gémesi, a right-wing opposition politician, mayor of Gödöllő and president of the Alliance of Hungarian Local-Governments.^[23]
- János Bánáti, president of the Hungarian Bar Association, and nine other lawyers.^[24]
- Zoltán Varga, a businessman and owner of Central Media Group, which publish opposition press products (24.hu).^[9]
- Attila Chikán, a former economy minister in the first cabinet of Viktor Orbán, currently a vocal critic of Orbán's politics.^[9]

India

Used against opposition leaders, union ministers, journalists, administrators such as Election Commissioner and heads of the Central Bureau of Investigation (CBI) and minority leaders.

- Rahul Gandhi, an Indian politician and main rival of Indian Prime Minister Narendra Modi, was targeted on two of his cellphones.^[25] He would go on to claim that "all [his] phones are tapped".^[26]
 - Five close friends and other Indian National Congress party officials were in the leaked list of potential targets.^[25]

- Prashant Kishor, a political strategist and tactician, who is linked with several of Prime Minister Narendra Modi's rivals,^[27] was also targeted.^[28] Some opposition politicians such as Mamata Banerjee even claimed that Pegasus was used to keep track of the meetings between the two.^[29]
- Ashok Lavasa, an ex-Election Commissioner of India who flagged Prime Minister Narendra Modi's poll code violation in the 2019 Indian general election was targeted.^[30]
- Alok Verma, who was ousted as the head of the Central Bureau of Investigation (CBI) by Prime Minister Narendra Modi in 2018 was a target.^[31]
- Numerous Indian politicians including Deputy Chief Minister of Karnataka G. Parameshwara, as well as close aides of then Chief Minister H. D. Kumaraswamy and senior Congress leader Siddaramaiah.^{[32][33][34]}
- Abhishek Banerjee, a West Bengal politician of the All India Trinamool Congress, and the nephew of incumbent Chief Minister of West Bengal Mamata Banerjee.^[35]
- Siddharth Varadarajan, a New Delhi-based, American investigative journalist and founder of The Wire. Varadarajan joined the Pegasus Project investigation.^[21]
- Umar Khalid, a left-wing student activist and leader of the Democratic Students' Union, was added to the list in late 2018, then charged with sedition. He was arrested in September 2020 for organising the Delhi riots; the provided evidence was taken from his phone. He is currently in jail awaiting trial.^[17]
- Stan Swamy, an Indian Jesuit father and activist. Swamy died on 5 July 2021 at the age of 84 after contracting COVID-19 in prison.^[17]
 - Collaborators Hany Babu, Shoma Sen and Rona Wilson were also in the project's list of alleged targets.^[17]
- Ashwini Vaishnaw, Minister of Electronics and Information Technology who assumed office less than 3 weeks before the investigation was revealed.^[36]
- The inner circle to the 14th Dalai Lama Tenzin Gyatso, the 17th Karmapa Ogyen Trinley Dorje and other Tibetan figures, including:^[37]
 - Tempa Tsering, the Dalai Lama's envoy to Delhi^[37]
 - Tenzin Taklha, the Dalai Lama's senior aide^[37]
 - Chhimey Rigzen, the Dalai Lama's senior aide^[37]
 - Lobsang Tenzin, the 5th Samdhong Rinpoche, who is responsible for the selection of the Dalai Lama's successor^[37]
 - Lobsang Sangay, former president of the Tibetan government-in-exile^[37]
 - Penpa Tsering, president of the Tibetan government-in-exile^[38]



Stan Swamy, a Roman Catholic priest and tribal rights activist, was arrested on terrorism charges and died in prison in 2021

Italy

- Romano Prodi, former Prime Minister of Italy and former President of the European Commission, was spied on while he was working as the UN Special Envoy to Sahel.^[39]

Mexico

Used against anti-corruption journalists, opposition leaders and a judge.

- Cecilio Pineda Birto (died 2 March 2017), a Mexican investigative and anti-corruption journalist. His phone was added as a Pegasus target just weeks before his assassination.^[21]
- Eduardo Ferrer Mac-Gregor Poisot, a Mexican judge, former president of the Inter-American Court of Human Rights.^[17]
- Alejandro Solalinde, a Catholic priest and champion of migrants' rights. Believed to be targeted due to his support to opposition politicians.^[17]

Morocco

Used against opposition, Western Sahara-friendly journalists in Morocco and France, and more than 6,000 Algerian politicians, high-ranking military officials, heads of intelligence, civil servants, diplomats and activists.^[20]

- Edwy Plenel, a French journalist, co-founder and publishing editor at opposition newsroom Mediapart, hacked in 2019 by Morocco.^[40]
- Lénaïg Bredoux, a French journalist also at Mediapart, hacked in 2020 by Morocco.^[40]
- Ignacio Cembrero, a Spanish journalist specialising in the Maghreb. He reported that he was hacked by the Moroccan government after learning that in June a Moroccan newspaper "picked up two WhatsApp conversations he had had with senior officials of the Spanish administration".^{[41][42]}
- Ahmed Gaid Salah, former Chief of Staff of the Algerian People's National Armed Forces^[20]
- Ali Haddad, Algerian businessman and supporter of former President Abdelaziz Bouteflika^[20]
- Abdelkader Messahel, former Minister of Foreign Affairs of Algeria^[20]

Saudi Arabia

Used against an opposition journalist and a women's rights activist since 2018.

- Jamal Khashoggi (died 2 October 2018), a Saudi-American investigative and opposition journalist, a contributor to The Washington Post, assassinated by Saudi operatives. Khashoggi, his wife Hanan El-Atr and phones of other people close to him have been targeted before and after his assassination.^[43]
 - Hatice Cengiz, Khashoggi's partner, was infected with Pegasus with forensic evidence of the spyware found on 6, 9 and 12 October 2018, a few days after Khashoggi's assassination.^[44]
 - Khashoggi's contacts Yasin Aktay, Yahya Assiri, Hanan El-Atr, Abdullah Khashoggi, Madawi al-Rasheed, and Azzam Tamimi were also targeted.^[45]
 - İrfan Fidan, Turkey's Istanbul chief prosecutor in charge of the Khashoggi murder's investigation, who later



Loujain al-Hathloul, Saudi women's rights activist, was placed on Pegasus target's list then abducted, arrested and tortured.

charged 20 Saudi operatives, is on the list of leaked targets.^[46]

- Loujain al-Hathloul, a prominent Saudi women's rights activist, selected in 2018, likely by the United Arab Emirates (an ally of Saudi Arabia), before her abduction and return to Saudi Arabia for arrest and possibly torture. She was released from prison in February 2021, but her freedom of movement is still limited.^[17]
- Madawi al-Rasheed, a British citizen of Saudi origin and a professor of social anthropology.^[47]

United Arab Emirates

Used against human rights activists, local leaders and local nobility and Sheikh Maktoum family members. With more than 10,000 people of interest linked to Dubai, it was one of the most extensive uses of Pegasus.^{[48][49]} The targets were mainly from the UAE and Qatar, but also included people from Egypt, Lebanon, Iraq, Yemen, and Saudi Arabia.^[48] In 2020,^[50] the NSO Pegasus license was stripped from Dubai due to human rights concerns^[51] and spying on Sheikh Maktoum family members.^[50]

- Princess Haya bint Hussein, the ex-wife of Sheikh Maktoum of Dubai, self-exiled in London.^{[51][52]} The list of "people of interest" includes her phone number as well as the phone number of 8 of her closest aides, advisers and friends, including personal assistant, security staffs, one of her lawyers advising her in her custody and divorce dispute with Sheikh Maktoum.^[51]
 - Security firm Quest's staffs: Martin Smith, CEO; its director of investigations; Shimon Cohen, its communications adviser.^[51]
 - John Gosden, a British horse racing trainer and friend.^[51]
- Sheikha Latifa bint Mohammed Al Maktoum, the daughter of Sheikh Maktoum of Dubai, attempted to escape to Goa, India. From there, she hoped to travel to the United States, where she planned to seek asylum, only to be caught by Indian special forces.^{[53][50]} Her phone number had appeared on 25 February 2018, one day after her escape, but the phone was already discarded in a café bathroom and replaced with a brand-new phone with new SIM cards.^[50] Phones used by Latifa's friends and family were soon added to the system. It is suspected that UAE Pegasus surveillance of her friends' phones helped Dubai to track Latifa's escape, and abduct her back near Goa.^[50]
 - Christian Elombo, a French soldier and friend of Latifa, and his girlfriend^[50]
 - Juan Mayer, a skydiving photographer and friend^[50]
 - Lynda Bouchiki, a skydiver and friend, events manager. Latifa chatted via phone with Bouchiki while fleeing.^[50]
 - Sioned Taylor, a Briton skydiver and friend, maths teacher. Latifa chatted via phone with Taylor while fleeing.^[50]
 - David Haigh, a British national previously detained and tortured in UAE prison, human rights campaigner and lawyer campaigning to free Latifa.^{[54][55]}
- Alaa al-Siddiq (died 19 June 2021), an Emirati human rights activist, executive director of the human rights organisation ALQST and the daughter of Muhammad al-Siddiq, one of the UAE-94 pro-democracy political prisoners.^[48] She was documenting violences by Gulf governments on prisoners.^[56] Following the 2011 Arab Spring, Alaa al-Siddiq was self-exiled to Qatar then the UK since 2012.^[48] All of her family members were stripped of their UAE nationality. Following her death in a car accident in 2021 in the UK, the UAE refused her body to be taken back to the country for burial.^[48] Citizens Lab found traces of Pegasus surveillance on her phone.^[57]

- Ahmed Mansoor, an Emirati human rights and reformist blogger, confirmed hacked by Pegasus.^[48] Arrested in 2011, pardoned, then arrested again in 2017 with 10 years sentences. Detained in dire conditions.
- Over 3,000 Qataris.^[48]
- European, Asian human rights activists supporting rights in the Gulf countries.^[48]

Reactions

NSO Group's response

Vetting and licence contract

NSO Group did not deny the presence of its spyware, responding to the report by stating they rigorously vetted its customers' human rights records before allowing them to use its spy tools.^[1] It says military-grade Pegasus is only supposed to be used to prevent serious crime and terrorism. NSO stated its purchasing client governments are bidden by a signed contract and licence, agreeing to terms of uses, and contractually limited to legitimate criminal or terrorist targets.^[51] Once sold, NSO Group says it does not know nor can see how its client governments use its spyware.^[51]

Involvement denial and deresponsibilisation

NSO Group stated: *"NSO does not operate the systems that it sells to vetted government customers, and does not have access to the data of its customers' targets. NSO does not operate its technology, does not collect, nor possesses, nor has any access to any kind of data of its customers. Due to contractual and national security considerations, NSO cannot confirm or deny the identity of our government customers, as well as the identity of customers of which we have shut down systems."*^[58]

The CEO of NSO Group categorically claimed that the list in question is unrelated to them, the source of the allegations can not be verified as a reliable one. "This is an attempt to build something based on a crazy lack of information... There is something fundamentally wrong with this investigation."^[59] The owner of the company that developed the Pegasus spyware categorically refutes all allegations, stating that the list of the phone numbers in question has nothing to do with the Pegasus spyware.^[59] NSO denied "false claims" about its clients' activities, but said it would "continue to investigate all credible claims of misuse and take appropriate action".^[1]

Journalists/NGOs

Journalists around the world have expressed outrage at the use of anti-criminality tools against non-criminals, journalists, opposition representatives, and other civilians. Edward Snowden has called for governments to impose a global moratorium on the international spyware trade in order to avoid ubiquitous violation of privacy and associated abuses.^[60]

Haaretz argued such invasive monitoring technology is the weapon of choice for autocratic governments, allowing continuous monitoring of opponents, preventing protests from the beginning before they are organised, and discouraging sources to share information with journalists.^[61] This technology should, therefore, be shared only with countries with independent and solid rule of law.^[61]

The Committee to Protect Journalists called for a critical reform of the surveillance software industry and market.^[62]

The International Press Institute, an international press freedom network, denounced the abuse of spying on journalists, calling formal investigations and accountability.^[63]

Tamer Almisshal, an investigative journalist for Al Jazeera Arabic, said, "[The hacking of the Al Jazeera staffers' and journalists' phones is] a crime against journalism. Based on this spyware, journalists have been arrested, disappeared, or even killed. Khashoggi is just one example".^[64]

In a statement, the National Association of Hungarian Journalists said they were "shocked" by the revelations and also stated: "If this is the case, it is unacceptable, outrageous and illegal, full information must be disclosed to the public immediately".^[65]

In a tweet, the Press Club of India (PCI) issued a statement:

This is the first time in the history of this country that all pillars of our democracy — judiciary, Parliamentarians, media, executives & ministers — have been spied upon. This is unprecedented and the PCI condemns unequivocally. The snooping has been done for ulterior motives. What is disturbing is that a foreign agency, which has nothing to do with the national interest of the country, was engaged to spy on its citizens. This breeds distrust and will invite anarchy. The Govt should come out clean on this front and clarify.^[66]

Similarly, the Editor's Guild of India also released a statement directed against the alleged spying made by the Indian government, saying:

This act of snooping essentially conveys that journalism and political dissent are now equated with 'terror'. How can a constitutional democracy survive if governments do not make an effort to protect freedom of speech and allows surveillance with such impunity?

It asked for a Supreme Court monitored enquiry into the matter, and further demanded that the inquiry committee should include people of impeccable credibility from different walks of life—including journalists and civil society—so that it can independently investigate the facts around the extent and intent of snooping using the services of Pegasus.^{[67][68]}

Companies

Amazon's cloud computing subsidiary AWS stated they had terminated "relevant infrastructure and accounts" linked to NSO Group, following an investigation by Amnesty International that discovered Amazon CloudFront was being used to infect targets with the Pegasus malware.^[69]

The CEO of WhatsApp, Will Cathcart, called for a global moratorium on the use of unaccountable surveillance technology and defended the use of end-to-end encryption following the reports.^{[70][71]}

National governments

Algeria

In a statement released, Algeria's public prosecutor has ordered an investigation into the reports that the country may have been a target of the Pegasus spyware.^[72]

France

After the revelations of the Pegasus Project investigation, in which it was revealed that the French president Emmanuel Macron was targeted,^[19] France launched an investigation into the matter.^[73] In the aftermath of these revelations, Macron changed his telephone number and replaced his phone. Furthermore, he ordered an overhaul in security procedures.^[74]

Macron reportedly contacted Israel's prime minister Naftali Bennett to discuss Israel's internal investigation and express concern that his data appeared on the list of potential targets and urged Bennett to conduct an inquiry.^[75]

French intelligence (ANSSI) confirmed that Pegasus spyware had been found on the phones of three journalists, including a journalist of France 24, in what was the first time an independent and official authority corroborated the findings of the investigation.^[76]

Hungary

A statement from the office of Viktor Orbán in Hungary stated that they were not aware of any alleged data collection.^[77] On 22 July, the Prosecution Service of Hungary announced that it would open an investigation to determine whether there was an illegal data collection.^{[78][79]}

India

The government has not denied the usage of Pegasus spyware in their response so far.^{[80][81]} The government has also denied the request for investigation or an independent Supreme Court inquiry by the opposition into the matter.^{[82][83][84]}

The official response of the Government of India to The Washington Post stated that "[t]he allegations regarding government surveillance on specific people has no concrete basis or truth associated with it whatsoever" and that such news reports were an attempt to "malign the Indian democracy and its institutions". They further stated that each case of interception, monitoring and decryption is approved by the Union Home Secretary and that there exists an oversight mechanism in the form of a review committee headed by the Union Cabinet Secretary and that any such interceptions have been done under the due process of law.^[77]

The former IT minister of India Ravi Shankar Prasad asked, "If more than 45 nations are using Pegasus as NSO has said, why is only India being targeted?"^[85]

The Indian IT Minister Ashwini Vaishnaw in a statement in parliament stated that the reports were "highly sensational" and that they had "no factual basis". He further stated that NSO themselves had rubbished the claims. He stated that the existence of numbers in a list was not sufficient evidence to indicate that the spyware was used and said that the report itself stated the same and without the physical examination of the phone such claims cannot be corroborated.^[86]

The Minister of Home and Internal Security Amit Shah in a statement on his blog insinuated that this was an attempt to disrupt the monsoon session of the parliament and that the opposition parties were "jumping on a bandwagon" and were trying to "derail anything progressive that comes up in Parliament". He stated that the report was an attempt to "derail India's development trajectory through their conspiracies".^{[80][87]}

Replying to allegations from the opposition, Minister of State in Ministry of Home Affairs Ajay Kumar Mishra said that there is no reason for a probe and the people who made the allegations are "political failures".^[26]

Israel

The Israeli government denied having access to the information gathered by NSO's clients.^[88]

In the aftermath of the revelations by the investigations of the Pegasus Project, the head of the Israeli parliament's Foreign Affairs and Defence Committee announced a commission to investigate the allegations of misuse of Pegasus for surveillance and hacking.^[89]

Kazakhstan

In the revelations made by the investigation, it came to light that the Kazakhstan's former Prime Minister, Bakhytzhhan Sagintayev, could have been targeted.^[19] Furthermore, it has been reported that Kassym-Jomart Tokayev, the president of Kazakhstan, was also targeted.^[90]

However, top officials have claimed that these reports and allegations of the president being spied on were "without evidence". Furthermore, the deputy head of Kazakhstan's presidential administration Dauren Abaev said the list of targets was "rather intriguing information without any evidence".^[90]

Morocco

The Moroccan government denied claims of acquiring and using Pegasus, and has said it "categorically rejects and condemns these unfounded and false allegations, as it has done with previous similar allegations by Amnesty International".^[77] The Moroccan ambassador to France, Chakib Benmoussa, also denied reports that his country's authorities had spied on French President Emmanuel Macron.^[91]

In an interview given to Jeune Afrique, Moroccan Foreign Minister Nasser Bourita stated it was "important to shed light on the facts, far from controversy and slander", and claimed that certain titles unionised within the journalist consortium "serve agendas well known for their primary hostility towards Morocco and are ulcerated by its successes under the leadership of His Majesty King Mohammed VI."^[92]

Morocco later sued Amnesty International and Forbidden Stories for defamation, with lawyer Olivier Baratelli saying that the Moroccan state "wants all possible light cast on these false allegations".^[93] It also issued defamation citations against *Le Monde*, Mediapart and Radio France on 28 July, and filed an injunction request against the German newspaper *Süddeutsche Zeitung* on 2 August.^[94]

Pakistan

The Prime Minister of Pakistan, Imran Khan, whose name was revealed to be in the list,^[19] has called on the United Nations for an investigation on the Indian use of Pegasus.^{[95][96]}

Rwanda

Rwanda, through a statement by Vincent Biruta, Minister of Foreign Affairs and International Cooperation, denied using Pegasus and claimed that accusations of the country using Pegasus are part of an ongoing campaign to cause tensions between Rwanda and other countries, and to promote disinformation about Rwanda domestically and internationally.^[77]

Saudi Arabia

Saudi Arabia's official Saudi Press Agency has denied all allegations of its use of Pegasus spyware on journalists and human rights activists as "baseless". The allegations were dismissed as "untrue".^{[97][98]}

United Arab Emirates

A statement released by the UAE's foreign minister stated that the allegations of use of the Pegasus spyware by the UAE on journalists and individuals were "categorically false" and that such allegations had no evidentiary basis and they denied all allegations.^{[72][98]} This despite ample material evidences of UAE dissidents being targeted.

Other reactions

In India the Indian National Congress accused Prime Minister Narendra Modi of "treason" and compromising national security following the release of the reports and called for the removal of Minister of Home and Internal Security Amit Shah and an investigation of the role of Prime Minister Narendra Modi into the affair.^{[99][100]}

The Indian IT minister made a statement that similar claims were made in the past regarding Pegasus for WhatsApp which had no factual basis and was even denied by the Supreme Court of India.^[101] However, many of the statements made by the Indian IT minister were verified by the Internet Freedom Foundation and were not found to be accurate.^[102]

West Bengal Chief Minister Mamata Banerjee alleged that the central government intends to "turn India into a surveillance state" where "democracy is in danger".^{[103][104]} On July 26th, 2021 The West Bengal Chief Minister announced a commission of inquiry into the alleged surveillance of phones using the Pegasus spyware developed by the Israeli cyber-intelligence company NSO Group. Retired Supreme Court judge Justice Madan B Lokur, and former Chief Justice of Calcutta High Court, Justice (ret'd) Jyotirmay Bhattacharya, have been appointed as members of the commission.^[105]

In India, some news articles were released making claims that Amnesty never claimed that the leaked phone numbers were of NSO's Pegasus spyware list.^[106] However, these reports were later proven to be false, and Amnesty issued a statement stating that it categorically stands by the findings of the investigation and that the data is irrefutably linked to potential targets of NSO Group's Pegasus spyware.^[107]

Government investigations

On 20 July 2021, it was reported that French prosecutors would investigate allegations that Moroccan intelligence services used Pegasus to spy on French journalists.^[108]

France's national agency for information systems security (ANSSI) identified digital traces of NSO Group's hacking spyware on three journalists' phones and relayed its findings to the Paris public prosecutor's office, which is overseeing the investigation into possible hacking.^[109]

See also

- NSO Group
- DarkMatter (Emirati company)
- SCL Group

- WhatsApp snooping scandal
- Facebook–Cambridge Analytica data scandal
- Facebook abuses campaigns by governments
- Edward Snowden
- Pegasus Project revelations in India

References

1. Kirchgaessner, Stephanie; Lewis, Paul; Pegg, David; Cutler, Sam; Lakhani, Nina; Safi, Michael (18 July 2021). "Revealed: leak uncovers global abuse of cyber-surveillance weapon" (<https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>). *The Guardian*. Retrieved 20 July 2021.
2. Mitra, Devirupa (21 July 2021). "Pegasus Project: 14 World Leaders in Leaked Database" (<https://thewire.in/world/pegasus-project-14-world-leaders-macron-ramaphosa-michel-imran>). *The Wire*. Retrieved 21 July 2021.
3. Forensic Methodology Report: How to catch NSO Group's Pegasus (<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>) (Report). Amnesty International. 18 July 2021. Retrieved 19 July 2021.
4. Bouquet, Jonathan (19 May 2019). "May I have a word about... Pegasus spyware" (<https://www.theguardian.com/theobserver/commentisfree/2019/may/19/may-i-have-a-word-about-pegasus-spyware>). *The Guardian*. Retrieved 20 July 2021.
5. "New investigation shows global human rights harm of NSO Group's spyware" (<https://www.amnesty.org/en/latest/news/2021/07/investigation-maps-human-rights-harm-of-nso-group-spyware/>). *Amnesty International*. 3 July 2021. Retrieved 19 July 2021.
6. Williams, Dan (22 July 2021). "Israeli lawmaker sees possible export review on NSO spyware scandal" (<https://www.reuters.com/article/israel-cyber-nso-idAFL8N2OY1NT>). *Reuters*. Retrieved 28 July 2021.
7. "About The Pegasus Project" (<https://forbiddenstories.org/about-the-pegasus-project/>). *Forbidden Stories*. Retrieved 19 July 2021.
8. "Israel Helped Over Ten Countries Tap Over 50,000 Phones" (<https://daraj.com/en/76189/>). *Daraj*. 18 July 2021. Retrieved 20 July 2021.
9. Panyi, Szabolcs; Pethő, András (19 July 2021). "Hungarian journalists and critics of Orbán were targeted with Pegasus, a powerful Israeli cyberweapon" (<https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsgirokat-is-celba-vettek-vele/>). *Direkt36*. Retrieved 19 July 2021.
10. "AmnestyTech/investigations" (<https://github.com/AmnestyTech/investigations>). *GitHub*. 19 July 2021. Retrieved 19 July 2021.
11. Six, Nicolas (20 July 2021). " " Projet Pegasus " : comment savoir si l'on a été infecté par le logiciel de surveillance ?" (https://www.lemonde.fr/pixels/article/2021/07/20/projet-pegasus-comment-savoir-si-l-on-a-ete-infecte-par-le-logiciel-de-surveillance_6088919_4408996.html). *Le Monde* (in French). Retrieved 20 July 2021.
12. Priest, Dana; Timberg, Craig; Mekhennet, Souad (18 July 2021). "Private Israeli spyware used to hack cellphones of journalists, activists worldwide" (https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_3). *The Washington Post*. Retrieved 20 July 2021.
13. Fenoglio, Jérôme (19 July 2021). " " Projet Pegasus " : quand la dérive devient la norme" (https://www.lemonde.fr/idees/article/2021/07/19/projet-pegasus-quand-la-derive-devient-la-norme_6088737_3232.html). *Le Monde* (in French). Retrieved 20 July 2021.

14. Rueckert, Phineas (18 July 2021). "Pegasus: The new global weapon for silencing journalists" (<https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/>). *Forbidden Stories*. Retrieved 22 July 2021.
15. "Digital Violence: How the NSO Group Enables State Terror" (<https://digitalviolence.org/>). *Digital Violence*. Retrieved 25 July 2021.
16. Richard, Laurent; Rigaud, Sandrine (18 July 2021). "The Pegasus Project: A Worldwide Collaboration to Counter a Global Crime" (<https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/>). *Forbidden Stories*. Retrieved 19 July 2021.
17. Walker, Shaun; Kirchgaessner, Stephanie; Lakhani, Nina; Safi, Michael (19 July 2021). "Pegasus project: spyware leak suggests lawyers and activists at risk across globe" (<https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe>). *The Guardian*. Retrieved 19 July 2021.
18. Randow, Gero von (20 July 2021). "Überwachungsskandal Pegasus: Frankreichs Präsident Macron im Visier der Spione" (<https://www.zeit.de/politik/ausland/2021-07/spionage-frankreich-marokko-emmanuel-macron-handy-pegasus-cyberwaffe-ueberwachung>). *Die Zeit* (in German). Retrieved 20 July 2021.
19. Timberg, Craig; Birnbaum, Michael; Harwell, Drew; Sabbagh, Dan (20 July 2021). "On the list: Ten prime ministers, three presidents and a king" (<https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/>). *The Washington Post*. Retrieved 20 July 2021.
20. "Pegasus: From its own king to Algeria, the infinite reach of Morocco's intelligence services" (<http://www.middleeasteye.net/news/pegasus-morocco-king-macron-targeted-intelligence-reach>). *Middle East Eye*. Retrieved 18 September 2021.
21. Lakhani, Nina (18 July 2021). "Revealed: murdered journalist's number selected by Mexican NSO client" (<https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto>). *The Guardian*. Retrieved 19 July 2021.
22. "Pegasus: Spyware sold to governments 'targets activists'" (<https://www.bbc.com/news/technology-57881364>). *BBC News*. 19 July 2021. Retrieved 19 July 2021.
23. Panyi, Szabolcs (24 July 2021). "Orbán ellen fordult, azóta érzi úgy, zaklatják és megfigyelik. Most kiderült, hogy Gémesi Györgyöt is megcélozták a kémfegyverrel" (<https://www.direkt36.hu/orban-ellen-fordult-azota-erzi-ugy-zaklatjak-es-megfigyelik-most-kiderult-hogy-gemesi-gyorgyot-is-megceloztak-a-kemfegyverrel>). *Direkt36* (in Hungarian). Retrieved 25 July 2021.
24. Panyi, Szabolcs; Pethő, András (20 July 2021). "President of the Hungarian Bar Association and several other lawyers targeted with Israeli spyware Pegasus" (<https://telex.hu/direkt36/2021/07/20/pegasus-nso-surveillance-hungary-lawyers-bar-association-janos-banati>). *Direkt36*. Retrieved 20 July 2021.
25. Safi, Michael (19 July 2021). "Key Modi rival Rahul Gandhi among potential Indian targets of NSO client" (<https://www.theguardian.com/news/2021/jul/19/key-modi-rival-rahul-gandhi-among-indian-targets-of-nso-client>). *The Guardian*. Retrieved 19 July 2021.
26. Prabhu, Sunil (23 July 2021). Ghosh, Deepshikha (ed.). "'My Phone Is Definitely Tapped, I'm Not 'Potential Target'": Rahul Gandhi" (<https://www.ndtv.com/india-news/rahul-gandhi-on-pegasus-scandal-my-phone-is-clearly-tapped-im-not-potential-target-2492906>). *NDTV*. Retrieved 23 July 2021.
27. Venkataramakrishnan, Rohan (19 July 2021). "The Political Fix: What can Prashant Kishor bring to the Congress – or the anti-Modi Opposition?" (<https://scroll.in/article/1000493/the-political-fix-what-can-prashant-kishor-bring-to-the-congress-or-the-anti-modi-opposition>). *Scroll.in*. Retrieved 23 July 2021.

28. "Pegasus Spyware: Two Union ministers, Rahul Gandhi, Prashant Kishor on Pegasus list: Report" (<https://timesofindia.indiatimes.com/india/two-union-ministers-rahul-gandhi-prashant-kishor-on-pegasus-list-report/articleshow/84568453.cms>). *The Times of India*. Times News Network. 20 July 2021. Retrieved 20 July 2021.
29. Mishra, Anupam (22 July 2021). "Govt snooped on my meetings with Prashant Kishor using Pegasus spyware: Mamata Banerjee" (<https://www.indiatoday.in/india/story/mamata-banerjee-on-pegasus-spyware-row-modi-govt-prashant-kishor-1831284-2021-07-22>). *India Today*. Retrieved 23 July 2021.
30. Agarwal, Kabir (19 July 2021). "Ashok Lavasa Placed on Snoop List as EC After Flagging Modi's 2019 Poll Code Violations" (<https://thewire.in/government/pegasus-project-ashok-lavasa-narendra-modi-amit-shah-model-code-of-conduct>). *The Wire*. Retrieved 20 July 2021.
31. "Ousted CBI chief Verma's number on Pegasus list" (<https://www.thehindu.com/news/national/hours-after-ouster-as-cbi-chief-alok-vermas-phone-numbers-made-it-to-pegasus-list-report/article35477226.ece>). *The Hindu*. 22 July 2021. Retrieved 23 July 2021.
32. Ashirwad Mahaprashasta, Ajoy (19 July 2021). "BJP Ministers Ashwini Vaishnaw, Prahlad Patel Find Place in List of Potential Pegasus Targets" (<https://thewire.in/politics/bjp-ministers-ashwini-vaishnaw-prahlad-patel-pegasus-spyware>). *The Wire*. Retrieved 19 July 2021.
33. "Pegasus Spyware: फॉरेंसिक टेस्ट में हुई पेगासस द्वारा जासूसी की पुष्टि, निशाने पर थे कई भारतीय पत्रकार" (<https://bastikhabar.online/pegasus-spyware-forensic-test-confirms-spying-by-pegasus-many-in-dian-journalists-were-on-target>). *Basti Khabar* (in Hindi). 18 July 2021. Retrieved 20 July 2021.
34. "Kumaraswamy, Siddaramaiah Secretaries Were Pegasus 'Targets' During 2019 Karnataka Political Turmoil" (<https://www.outlookindia.com/website/story/india-news-kumaraswamy-siddaramaiah-secretaries-were-pegasus-targets-during-2019-karnataka-political-turmoil/388834>). *Outlook*. 20 July 2021. Retrieved 21 July 2021.
35. Agarwal, Kabir; Ashirwad Mahaprashasta, Ajoy; Varadarajan, Siddharth (19 July 2021). "Prashant Kishor Hacked by Pegasus, Mamata's Nephew Also Selected as Potential Snoop Target" (<https://thewire.in/government/prashant-kishor-mamata-banerjee-nephew-pegasus-spyware>). *The Wire*. Retrieved 21 July 2021.
36. "Pegasus Project: 136 Names Revealed By The Wire On Snoop List So Far" (<https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance>). *The Wire*. 23 July 2021. Retrieved 25 July 2021.
37. Safi, Michael (22 July 2021). "Dalai Lama's inner circle listed in Pegasus project data" (<https://www.theguardian.com/news/2021/jul/22/dalai-lama-inner-circle-listed-pegasus-project-data>). *The Guardian*. Retrieved 25 July 2021.
38. "Members of Dalai Lama's inner circle on Pegasus list" (<https://www.hindustantimes.com/india-news/members-of-dalai-lama-s-inner-circle-on-pegasus-list-101626969360453.html>). *Hindustan Times*. 22 July 2021. Retrieved 26 July 2021.
39. "Pegasus Project, "spiato anche Romano Prodi quando era inviato speciale Onu per il Sahel" " (<https://www.ilfattoquotidiano.it/2021/07/21/pegasus-project-spiato-anche-romano-prodi-quando-era-inviato-speciale-dellonu-per-il-sahel/6268710/>). *il Fatto Quotidiano* (in Italian). 21 July 2021. Retrieved 21 July 2021.
40. "How Morocco spied on Mediapart journalists using Pegasus spyware" (<https://www.mediapart.fr/en/journal/france/190721/how-morocco-spied-mediapart-journalists-using-pegasus-spyware>). *Mediapart*. 19 July 2021. Retrieved 19 July 2021.
41. "Ignacio Cembrero, tras ser víctima de ciberespionaje con Pegasus: "Hay otros españoles que todavía no han salido a la luz" " (https://www.lasexta.com/noticias/internacional/ignacio-cembrero-ser-victima-ciberespionaje-pegasus-hay-otros-espanoles-que-todavia-han-salido-luz_2021071960f5dc4fc7f1ec00013dd29a.html). *La Sexta* (in Spanish). 19 July 2020. Retrieved 20 July 2021.

42. Bassets, Marc (19 July 2021). "Una filtración revela el espionaje de Gobiernos a periodistas y opositores con el programa Pegasus" (<https://elpais.com/internacional/2021-07-19/una-filtracion-revela-el-espionaje-de-gobiernos-a-periodistas-y-opositores-con-el-programa-pegasus.html>). *El País* (in Spanish). Retrieved 20 July 2021.
43. Bouvart, Arthur; Priest, Dana (18 July 2021). "Affaire Khashoggi : deux femmes proches du journaliste assassiné ont été surveillées par Pegasus" (https://www.lemonde.fr/projet-pegasus/article/2021/07/18/affaire-khashoggi-deux-femmes-proches-du-journaliste-assassine-ont-ete-surveillees-par-pegasus_6088655_6088648.html). *Le Monde* (in French). Retrieved 19 July 2021.
44. "VIDEO: How NSO Group's Pegasus Spyware Was Found on Jamal Khashoggi's Fiancée's Phone" (<https://www.pbs.org/wgbh/frontline/article/how-nso-group-pegasus-spyware-found-jamal-khashoggi-fiancee-phone/>). *Frontline*. 18 July 2021. Retrieved 19 July 2021.
45. *Pegasus: the spyware technology that threatens democracy* (<https://www.youtube.com/watch?v=G7H9uo3j5FQ>). *The Guardian*. 19 July 2021. Retrieved 19 July 2021 – via YouTube.
46. Kirchgaessner, Stephanie (18 July 2021). "Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests" (<https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>). *The Guardian*. Retrieved 19 July 2021.
47. Pegasus Project: Why I was targeted by Israeli spyware (<https://www.middleeasteye.net/opinion/pegasus-israel-saudi-arabia-why-targeted-spyware>), Madawi al-Rasheed], 20 July 2021, Middle East Eye
48. Moukalled, Diana (18 July 2021). "UAE: Israel's (Pegasus) Spyware in the Service of Autocracy" (<https://daraj.com/en/76524/>). *Daraj*. Retrieved 21 July 2021.
49. Barthe, Benjamin (21 July 2021). "' ' Projet Pegasus ' : de la répression domestique à l'espionnage géopolitique aux Emirats" (https://www.lemonde.fr/projet-pegasus/article/2021/07/21/aux-emirats-de-la-repression-domestique-a-l-espionnage-geopolitique_6089088_6088648.html). *Le Monde* (in French). Retrieved 22 July 2021.
50. Sabbagh, Dan (21 July 2021). "Data leak raises new questions over capture of Princess Latifa" (<https://www.theguardian.com/world/2021/jul/21/data-leak-raises-new-questions-over-capture-of-princess-latifa>). *The Guardian*. Retrieved 22 July 2021.
51. Pegg, David; Lewis, Paul (21 July 2021). "Dubai suspected after Princess Haya listed in leaked Pegasus project data" (<https://www.theguardian.com/world/2021/jul/21/dubai-suspected-after-princess-haya-listed-in-leaked-pegasus-project-data>). *The Guardian*. Retrieved 21 July 2021.
52. "Dubai ruler hacked ex-wife using NSO Pegasus spyware, high court judge finds" (<https://www.theguardian.com/world/2021/oct/06/dubai-ruler-hacked-ex-wife-using-nso-pegasus-spyware-high-court-judge-finds-sheikh-mohammed-princess-haya>). *the Guardian*. 6 October 2021. Retrieved 6 October 2021.
53. Mitra, Devirupa (21 July 2021). "Before Indian Soldiers Captured Dubai Princess on High Seas, UAE Zeroed in on Her Friends' Numbers" (<https://thewire.in/world/dubai-princess-sheikh-latifa-pegasus-list>). *The Wire*. Retrieved 22 July 2021.
54. Harwell, Drew; Sabbagh, Dan (2 August 2021). "Human rights activist and close ally of detained Dubai princess had phone hacked by NSO spyware, forensic test finds" (<https://web.archive.org/web/20210802170739/https://www.washingtonpost.com/technology/2021/08/02/activist-dubai-princess-pegasus-surveillance/>). *Washington Post*. ISSN 0190-8286 (<https://www.worldcat.org/issn/0190-8286>). Archived from the original (<https://www.washingtonpost.com/technology/2021/08/02/activist-dubai-princess-pegasus-surveillance/>) on 2 August 2021. Retrieved 2 August 2021.

55. Dan, Sabbagh (2 August 2021). "Princess Latifa campaigner had 'phone compromised by Pegasus spyware'" (<https://www.theguardian.com/world/2021/aug/02/princess-latifa-campaigner-david-haigh-phone-compromised-pegasus-spyware>). *the Guardian*. Archived (<https://web.archive.org/web/20210802201730/https://www.theguardian.com/world/2021/aug/02/princess-latifa-campaigner-david-haigh-phone-compromised-pegasus-spyware>) from the original on 2 August 2021. Retrieved 2 August 2021.
56. "New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq" (<https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq>). *the Guardian*. 24 September 2021. Retrieved 24 September 2021.
57. "New evidence suggests spyware used to surveil Emirati activist Alaa Al-Siddiq" (<https://www.theguardian.com/world/2021/sep/24/new-evidence-suggests-spyware-used-to-surveil-emirati-activist-alaa-al-siddiq>). *the Guardian*. 24 September 2021. Retrieved 24 September 2021.
58. "Response from NSO and governments" (<https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments>). *The Guardian*. 18 July 2021. Retrieved 20 July 2021.
59. Kabir, Omer; Ravet, Hagar (20 July 2021). "NSO CEO exclusively responds to allegations: 'The list of 50,000 phone numbers has nothing to do with us'" (<https://www.calcalistech.com/tech/articles/0,7340,L-3912882,00.html>). *CTech by Calcalist*. Retrieved 21 July 2021.
60. Pegg, David; Lewis, Paul (19 July 2021). "Edward Snowden calls for spyware trade ban amid Pegasus revelations" (<https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations>). *The Guardian*. Retrieved 19 July 2021.
61. Ziv, Amitai (18 July 2021). "The Pegasus Project | How Israeli Spy-tech Became Dictators' Weapon of Choice" (<https://www.haaretz.com/israel-news/tech-news/.premium-how-israeli-spy-tech-became-dictators-weapon-of-choice-1.10010738>). *Haaretz*. Retrieved 19 July 2021.
62. "Spyware reform critical as at least 180 journalists revealed as potential Pegasus targets" (<https://cpj.org/2021/07/spyware-reform-critical-180-journalists-potential-pegasus-targets/>). *Committee to Protect Journalists*. 19 July 2021. Retrieved 20 July 2021.
63. "Pegasus Project: Full investigation needed after 180 journalists targeted by spyware" (<https://ipi.media/pegasus-project-full-investigation-needed-after-180-journalists-targeted-by-spyware/>). *International Press Institute*. 19 July 2021. Retrieved 20 July 2021.
64. "Al Jazeera journalists hacked using Israeli firm's spyware" (<https://www.aljazeera.com/news/2020/12/21/al-jazeera-journalists-hacked-by-spyware-sold-by-israeli-firm>). *Al Jazeera*. 21 December 2020. Retrieved 20 July 2021.
65. "Morocco and Hungary deny reports that they infiltrated phones with Pegasus spyware" (<https://www.france24.com/en/technology/20210719-morocco-and-hungary-deny-reports-that-they-infiltrated-phones-with-pegasus-spyware>). *France 24*. 19 July 2021. Retrieved 21 July 2021.
66. Press Club of India [@PCITweets] (19 July 2021). "This is the first time in the history of this country that all pillars of our democracy — judiciary, Parliamentarians, media, executives & ministers — have been spied upon. This is unprecedented and the PCI condemns unequivocally. The snooping has been done for interior [sic] motives" (<https://twitter.com/PCITweets/status/1417013381563699201>) (Tweet). Retrieved 21 July 2021 – via [Twitter](#).
67. "Editors Guild Joins Call for SC-Monitored Probe Into Pegasus Snooping Allegations" (<https://thewire.in/media/pegasus-project-editors-guild-supreme-court-probe>). *The Wire*. 21 July 2021. Retrieved 21 July 2021.
68. "Editors Guild of India seeks Supreme Court-monitored probe into Pegasus case" (<https://www.telegraphindia.com/india/editors-guild-of-india-seeks-supreme-court-monitored-probe-into-pegasus-case/cid/1823347>). *The Telegraph*. 21 July 2021. Retrieved 21 July 2021.
69. Cox, Joseph (19 July 2021). "Amazon Shuts Down NSO Group Infrastructure" (<https://www.vice.com/en/article/xgx5bw/amazon-aws-shuts-down-nso-group-infrastructure>). *Motherboard*. Vice Media. Retrieved 20 July 2021.

70. Banerjee, Prasad (19 July 2021). "WhatsApp CEO calls on governments, companies to take Pegasus makers to task" (<https://www.livemint.com/technology/tech-news/whatsapp-ceo-calls-on-governments-companies-to-take-pegasus-makers-to-task-11626701471086.html>). *Mint*. Retrieved 20 July 2021.
71. Sharma, Mihir (20 July 2021). "Pegasus Scandal Should Be a Wake-Up Call for U.S." (<https://www.bloomberg.com/opinion/articles/2021-07-19/pegasus-spyware-scandal-should-prompt-new-u-s-controls>) *Bloomberg.com*. Retrieved 20 July 2021.
72. "Algeria launches probe of NSO spyware claim; Saudi Arabia, UAE deny allegations" (<https://www.timesofisrael.com/algeria-launches-probe-of-nso-spyware-claim-saudi-arabia-uae-deny-allegations/>). *The Times of Israel*. Agence France-Presse. 23 July 2021. Retrieved 26 July 2021.
73. Desai, Shweta (22 July 2021). "France launches investigation into Pegasus spyware" (<https://www.aa.com.tr/en/world/france-launches-investigation-into-pegasus-spyware/2311661>). *Anadolu Agency*. Retrieved 25 July 2021.
74. Ott, Haley (23 July 2021). "French President Emmanuel Macron changes phone after reports of wide-scale Pegasus hack" (<https://www.cbsnews.com/news/pegasus-french-president-macron-changes-phone-after-wide-scale-hack-report/>). *CBS News*. Retrieved 25 July 2021.
75. McKernan, Bethan (25 July 2021). "Emmanuel Macron 'pushes for Israeli inquiry' into NSO spyware concerns" (<https://www.theguardian.com/world/2021/jul/25/emmanuel-macron-pushes-for-israeli-inquiry-into-nso-spyware-concerns>). *The Guardian*. Retrieved 25 July 2021.
76. "Pegasus spyware found on journalists' phones, French intelligence confirms" (<https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms>). *the Guardian*. 2 August 2021.
77. "Responses from countries to the Pegasus Project" (<https://www.washingtonpost.com/investigations/2021/07/18/responses-countries-pegasus-project/>). *The Washington Post*. 19 July 2021. Retrieved 20 July 2021.
78. "Pegasus-ügy: nyomozást rendelt el az ügyészség" (https://m.hvg.hu/itthon/20210722_pegasus_ugy_nyomozas_ugyeszseg). *Heti Világgazdaság* (in Hungarian). 22 July 2021. Retrieved 22 July 2021.
79. "Hungary Prosecutors Probe Pegasus Spying Claims" (<https://www.barrons.com/articles/hungary-prosecutors-probe-pegasus-spying-claims-01626963607>). *Barron's*. Agence France-Presse. 22 July 2021. Retrieved 22 July 2021.
80. Venkataramakrishnan, Rohan (21 July 2021). "Across official denials and BJP responses, one phrase missing: 'India did not use Pegasus spyware'" (<https://scroll.in/article/1000605/a-cross-official-denials-and-bjp-responses-one-phrase-missing-india-did-not-use-pegasus-spyware>). *Scroll.in*. Retrieved 21 July 2021.
81. "Verma, Asthana, Anil Ambani in Pegasus list: Report" (<https://www.hindustantimes.com/india-news/verma-asthana-anil-ambani-in-pegasus-list-report-101626979200830.html>). *Hindustan Times*. 23 July 2021. Retrieved 23 July 2021.
82. "Centre Rejects Demand for Probe Into Snooping Allegations, IT Minister Calls Reports 'Over the Top'" (<https://thewire.in/government/ashwini-vaishnaw-parliament-pegasus-snooping-allegations>). *The Wire*. 22 July 2021. Retrieved 24 July 2021.
83. "France Orders Probe Into Spyware Targeting, Israel Sets Up Crisis Group, India Remains in Denial" (<https://thewire.in/world/france-israel-probe-pegasus-spyware-surveillance-india-denial>). *The Wire*. 22 July 2021. Retrieved 24 July 2021.
84. Mishra, Himanshu Shekhar (23 July 2021). Ghosh, Deepshikha (ed.). "Centre Rejects Rahul Gandhi's Call For Pegasus Court Inquiry: 10 Points" (<https://www.ndtv.com/india-news/pegasus-government-rejects-rahul-gandhis-call-for-court-inquiry-2492996>). *NDTV*. Retrieved 24 July 2021.

85. Sanyal, Anindita, ed. (19 July 2021). "["If Over 45 Countries Use Pegasus, Why Target Just India?" Says BJP](https://www.ndtv.com/india-news/bjp-on-pegasus-ravi-shankar-prasad-says-over-45-countries-using-pegasus-why-just-target-india-2490023)" (<https://www.ndtv.com/india-news/bjp-on-pegasus-ravi-shankar-prasad-says-over-45-countries-using-pegasus-why-just-target-india-2490023>). *NDTV*. Retrieved 21 July 2021.
86. "IT Minister Shri Ashwini Vaishnaw's Statement in Parliament on "Alleged use of spyware Pegasus to compromise phone data of some persons as reported in Media on 18th July 2021" " (<http://pib.gov.in/Pressreleaseshare.aspx?PRID=1736803>). Press Information Bureau. 19 July 2021. Retrieved 21 July 2021.
87. "Disruptors and obstructers will not be able to derail India's development trajectory through their conspiracies" (<http://amitshah.co.in/disruptors-and-obstructers-will-not-be-able-to-derail-indias-development-trajectory-through-their-conspiracies/>). *Amit Shah Official*. 19 July 2021. Retrieved 21 July 2021.
88. Gross, Judah Ari (19 July 2021). "Israel: If NSO Group violated export permits, 'appropriate action' will be taken" (<https://www.timesofisrael.com/israel-if-nso-group-violated-export-permits-appropriate-action-will-be-taken/>). *The Times of Israel*. Retrieved 22 July 2021. "It is important to note that the State of Israel does not have access to the information collected by the NSO Group's customers"
89. "Israel launches commission to probe Pegasus spyware: Legislator" (<https://www.aljazeera.com/news/2021/7/22/israel-launches-commission-to-probe-pegasus-spyware-legislator>). *Al Jazeera*. 22 July 2021. Retrieved 25 July 2021.
90. "Intriguing Information Without Evidence": Kazakhstan On Pegasus Spy Claims" (<https://www.ndtv.com/world-news/pegasus-report-intriguing-information-without-evidence-kazakhstan-on-pegasus-spy-claims-2493135>). *NDTV*. Agence France-Presse. 23 July 2021. Retrieved 26 July 2021.
91. "Morocco: ambassador insists that kingdom did not spy on Macron" (<https://www.middleeastmonitor.com/20210726-morocco-ambassador-insists-that-kingdom-did-not-spy-on-macron/>). *Middle East Monitor*. 26 July 2021. Retrieved 26 July 2021.
92. "Affaire Pegasus – Nasser Bourita : « Qui a intérêt à ostraciser le Maroc ? C'est là la vraie question » – Jeune Afrique" (<https://www.jeuneafrique.com/1207055/politique/affaire-pegasus-nasser-bourita-qui-a-interet-a-ostraciser-le-maroc-cest-la-la-vraie-question/>). *JeuneAfrique.com* (in French). 22 July 2021. Retrieved 9 August 2021.
93. "Pegasus Affair: Morocco sues Amnesty International, French NGO for defamation" (<https://www.france24.com/en/africa/20210722-morocco-files-libel-suit-in-france-against-ngos-alleging-it-used-pegasus-spyware>). *France 24*. 22 July 2021. Retrieved 23 July 2021.
94. "Affaire Pegasus: le Maroc porte plainte en Allemagne" (<https://leseco.ma/maroc/affaire-pegasus-le-maroc-porte-plainte-en-allemande.html>). *LesEco.ma* (in French). 4 August 2021. Retrieved 9 August 2021.
95. Shahzad, Asif (23 July 2021). "Pakistan seeks U.N. probe of India's use of Pegasus spyware" (<https://www.reuters.com/technology/pakistan-seeks-un-probe-indias-use-pegasus-spyware-2021-07-23/>). *Reuters*. Retrieved 24 July 2021.
96. "Pegasus list: Pakistan seeks UN probe into reports of PM Imran Khan's name" (<https://www.hindustantimes.com/india-news/pak-for-probe-by-un-agencies-into-reports-of-pm-imran-khan-s-name-on-pegasus-list-101627027807942.html>). *Hindustan Times*. 23 July 2021. Retrieved 24 July 2021.
97. "Saudi Arabia denies allegations of using Pegasus spyware on journalists, activists" (<https://www.dawn.com/news/1636424>). *Dawn*. Agence France-Presse. 22 July 2021. Retrieved 26 July 2021.
98. "Saudi Arabia and UAE deny Pegasus spyware allegations" (<https://www.expatica.com/sa/uncategorized/saudi-arabia-and-uae-deny-pegasus-spyware-allegations-75513/>). *Expatica*. 22 July 2021. Retrieved 26 July 2021.

99. Kuchay, Bilal (20 July 2021). "India's PM Modi accused of 'treason' over Pegasus spyware scandal" (<https://www.aljazeera.com/news/2021/7/20/pegasus-project-india-modi-treason-spyware-snooping-scandal>). *Al Jazeera*. Retrieved 20 July 2021.
100. "Pegasus Spyware India: Congress-JD(S) leaders in Karnataka were potential Pegasus spyware targets in 2019" (<https://timesofindia.indiatimes.com/india/congress-jds-leaders-in-karnataka-were-potential-pegasus-spyware-targets-in-2019-report/articleshow/84583890.cms>). *The Times of India*. 20 July 2021. Retrieved 20 July 2021.
101. "'Attempt to defame India': Government pushes back as fresh allegations of snooping emerge" (<https://timesofindia.indiatimes.com/india/attempt-to-defame-india-government-pushes-back-as-fresh-allegations-of-snooping-emerge/articleshow/84570013.cms>). *The Times of India*. Times News Network. 20 July 2021. Retrieved 21 July 2021.
102. Internet Freedom Foundation (20 July 2021). "IFF Verifies Claims Made by IT Min Ashwini Vaishnaw on Pegasus Project" (<https://www.thequint.com/cyber/policy/iff-verifies-claims-made-by-it-minister-on-the-pegasus-project-revelations>). *The Quint*. Retrieved 21 July 2021.
103. Nag, Jayatri; Bhattacharya, DP (21 July 2021). "Modi government wants 'surveillance state', says Mamata Banerjee, calls for opposition unity" (https://m.economictimes.com/news/politics-and-nation/bjp-intends-to-turn-india-into-a-surveillance-state-tmc-chief-mamata-banerjee/amp_articleshow/84612980.cms). *The Economic Times*. Retrieved 21 July 2021.
104. Mitra, Atri (21 July 2021). "Pegasus row: Govt trying to turn country into a surveillance state, says Mamata Banerjee" (<https://indianexpress.com/article/india/mamata-banerjee-tmc-pegasus-martyrs-day-kolkata-7415378/>). *The Indian Express*. Retrieved 21 July 2021.
105. "Mamata Banerjee: Panel with Justice Lokur, ex-SC Judge, to probe Pegasus row" (<https://indianexpress.com/article/india/bengal-govt-sets-up-inquiry-panel-to-probe-pegasus-snooping-row-7422996/>). *The Indian Express*. 27 July 2021. Retrieved 5 August 2021.
106. Shrivastava, Rahul; Mishra, Himanshu (22 July 2021). "Amnesty says never claimed leaked phone numbers were of NSO Pegasus Spyware list" (<https://www.indiatoday.in/india/story/amnesty-leaked-phone-numbers-nso-pegasus-spyware-list-1831119-2021-07-22>). *India Today*. Retrieved 23 July 2021.
107. Mathew, Liz; Ghose, Dipankar (23 July 2021). "Amnesty International rebuts claim by BJP, says it 'stands by' Pegasus reports" (<https://indianexpress.com/article/india/project-pegasus-false-rumours-unlawful-targeting-amnesty-7416993/>). *The Indian Express*. Retrieved 23 July 2021.
108. "French prosecutors open probe into alleged use of Pegasus malware to spy on journalists" (<https://www.france24.com/en/europe/20210720-french-prosecutors-open-probe-into-alleged-use-of-pegasus-malware-to-spy-on-journalists>). *France 24*. 20 July 2021. Retrieved 20 July 2021.
109. "Pegasus spyware found on journalists' phones, French intelligence confirms" (<https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms>). *the Guardian*. 2 August 2021.

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Pegasus_Project_\(investigation\)&oldid=1048766981](https://en.wikipedia.org/w/index.php?title=Pegasus_Project_(investigation)&oldid=1048766981)"

This page was last edited on 7 October 2021, at 20:58 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.