Opinion **NSO Group Technologies**

# We need a new global standard to curb intrusive spyware

When tech companies can freely undermine national security, democracies are at risk

**MARIETJE SCHAAKE**

Pegasus software has allegedly been used to spy on journalists and politicians © Joel Saget/AFP/Getty

**Marietje Schaake** NOVEMBER 10 2021

*The writer is international policy director at Stanford University's Cyber Policy Center*

After more than a decade, democratic governments are finally waking up to the hazards of commercial spyware. Recent media coverage has exposed how authoritarian regimes are using NSO Group's Pegasus software to spy on journalists and politicians. The EU has now tightened its rules on the export of surveillance technology, and the US Department of Commerce last week determined that Israel-based NSO Group and three other hacking companies were "engaging in activities that are contrary to the national security or foreign policy interests of the United States". However, these modest steps do not go far enough: what's needed is a global standard to reign in technologies that violate the rights to privacy, free assembly as well as free expression.

From crippling ransomware to questionable neural algorithms which use AI to identify suspicious non-verbal activity, to face and emotion-detecting technologies, there is a proliferation of software applications which conflict with liberal democratic values.

Traditionally, export controls are imposed on products that threaten national security, such as those that could boost the manufacture of nuclear weapons. The EU has recently extended its export regime to include spyware technologies, and added human rights violations as a criterion for potential harm. But since the NSO Group is based outside the EU, it lies outside Brussels' jurisdiction. Without a wider international agreement, options for curbing these companies are limited.

While restricting exports may help prevent the flow of intrusive technologies from democracies to dictatorships, imports and domestic uses remain unaddressed. The Pegasus Project revealed how, in the heart of the EU, Hungarian prime minister Viktor Orban has deployed commercial surveillance systems to target the few remaining independent media outlets within his own country.

Even some democratic states, such as the Netherlands, are guilty of procuring hacking and surveillance systems, but do not disclose which ones. Undoubtedly, they will claim these are only ever used to track down the most serious criminal and terror suspects. Yet this lends credibility and capital to an exceedingly harmful industry. If democracies are serious about curbing surveillance, they should exercise greater transparency and lead by example.

More than ad hoc measures or restrictions applied to individual companies, the US should partner with the EU and other willing countries to set a new international standard for the use of, and trade in, spyware. This would be a tangible outcome for President Biden's upcoming Summit for Democracy, a US-led virtual meeting in early December aimed at preventing authoritarianism, fighting corruption, and promoting human rights.

Beyond spyware, a variety of other technologies deserve greater scrutiny and regulation. Illegitimate mass surveillance systems, facial recognition software and tools used for illegal cyber operations are traded across borders to facilitate repression, conflict, and instability. Poor cyber security is now a source of systematic risk which threatens national resilience. Greater co-ordination is necessary to ensure that technologies which are currently legal do not provide the means for widespread rights violations.

Moreover, an international agreement between democratic states against malicious uses of technology will help set multilateral norms. UN human rights experts this week raised the alarm once more about how tech companies serve as modern-day "mercenaries". "Private actors provide a wide range of military and security services in cyber space, including data collection, intelligence and surveillance," they warned.

In the future, a licensing requirement should be the default for tech companies that contravene the human rights standard of democratic states. This would ensure better controls of end use and exports. Regulation would also allow for mapping of how software is being deployed, and enable greater transparency.