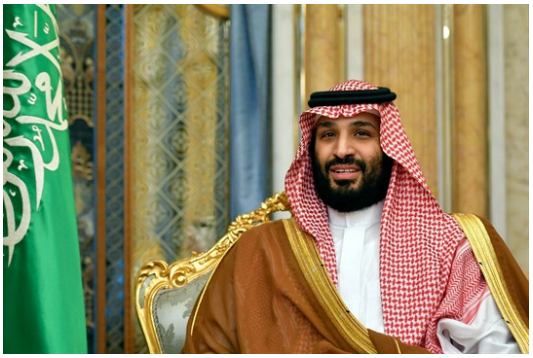
WPR
WORLD POLITICS REVIEW®

The Bezos Hack and the Dangers of Spyware in the Hands of Autocrats

Candace Rondeaux | Friday, Jan. 24, 2020



Crown Prince Mohammed bin Salman at a meeting in Jeddah, Saudi Arabia, Sept. 18, 2019 (Pool photo by Mandel Ngan via AP).

The stunning allegation this week that Saudi Crown Prince Mohammed bin Salman hacked the phone of Amazon's Jeff Bezos (https://www.washingtonpost.com/politics/un-ties-alleged-phone-hacking-to-posts-coverage-of-saudi-arabia/2020/01/22/a0bc63ba-3d1f-11ea-b90d-5652806c3b3a_story.html), according to a report by United Nations investigators (https://www.docdroid.net/E8DLBGR/united-nations-bezos-statement.pdf#page=5), may come as a shock to some. But for most people tracking the rise of Saudi Arabia's de facto ruler over the past five years, it's business as usual. From his disastrous proxy war in Yemen to the killing of Washington Post journalist Jamal Khashoggi (https://www.theguardian.com/world/2019/jun/19/jamal-khashoggi-killing-saudi-crown-prince-mohammed-bin-salman-evidence-un-report) in the Saudi consulate in Istanbul in 2018, the young crown prince, known as MBS, has demonstrated time and again his hubristic belief that there are no limits to his power.

What is more shocking is that anyone truly believes that another investigation into Saudi malfeasance will curb the use of spyware by autocratic governments against their perceived critics at home and abroad. To be sure, for the sake of accountability, the FBI should heed the call by U.N. experts Agnes Callamard and David Kaye to open an investigation into how the heir to the Saudi kingdom apparently used Israeli-made spyware to breach the personal phone of the world's richest man, who owns a leading American newspaper and runs one of the world's most valuable publicly traded companies. But in the grand scheme of things, investigating the hack of Bezos' phone might not make all that much difference in preventing these kinds of abuses.

Instead, the best defense against dangerous surveillance technology is to treat the spyware that MBS deployed against Bezos the same way that the U.N., the United States and others deal with weapons of mass destruction: regulate it as much as possible and insist on more global oversight.

Since rising to power in 2015, first as Saudi Arabia's defense minister and soon after as crown prince, MBS has worked assiduously to burnish his strongman credentials by waging an aggressive information war against his critics and perceived adversaries inside and outside the kingdom. Yet President Donald Trump's White House

has repeatedly bent over backward to shield MBS from censure (https://www.middleeasteye.net/news/blank-check-five-times-trump-stood-saudi-government-2019) despite multiple instances of his involvement in well-documented human rights abuses, most notoriously Khashoggi's murder.

Of course, such deference to Saudi Arabia predates Trump in Washington, which will no doubt remain in thrall to the false god of foreign policy expedience that rewards the likes of MBS with sweetheart defense deals and White House visits, all in the name of stability and security in the Middle East. While Congress has taken the rare step of criticizing MBS and trying to punish Saudi Arabia's behavior, both over Khashoggi's killing and the war in Yemen, it has shown little to no capacity or will to rein in tech firms whose spyware MBS has used to stifle dissent.

Firms like the NSO Group, the maker of the Pegasus spyware that MBS reportedly deployed against Bezos and Saudi dissidents, already profit handsomely from the insatiable appetite of autocrats, oligarchs and powerful tycoons to target their critics and perceived adversaries. This devil's bargain extends around the world (https://www.worldpoliticsreview.com/articles/28337/how-spyware-like-nso-pegasus-is-making-dissent-more-dangerous). In 2018, it was revealed that Black Cube, the same Israeli private security firm that disgraced Hollywood mogul Harvey Weinstein hired to intimidate and harass his #MeToo accusers, tried to target Obama administration officials (https://www.newyorker.com/news/news-desk/israeli-operatives-who-aided-harvey-weinstein-collected-information-on-former-obama-administration-officials) in a phishing campaign designed to discredit them and the Iran nuclear deal.

> ***The best defense against dangerous surveillance technology is to treat it like weapons of mass destruction: regulate it as much as possible and insist on more global oversight.***

Yet no serious action has been taken by legislators in Washington to constrain firms like the NSO Group and Black Cube from targeting U.S. citizens, residents and firms that otherwise enjoy privacy protections under U.S. law. Congress has remained all but silent, in fact, about the role of Israel and Saudi Arabia—America's two most important Middle Eastern allies—in deploying tech to stifle the media, target critics and snuff out honest democratic debate.

In Israel, defense tech exports are generally governed by a 2007 national law designed to prevent the sale of weapons to governments implicated in committing atrocities and under U.N. arms embargo. But application of the law seems selective at best, to put it charitably, and the country has a long history of selling military hardware to regimes with questionable human rights records—although Israel is by no means unique in that regard. Meanwhile, Saudi Arabia has recently become one of the world's leading importers of arms and military technology, according to the Stockholm International Peace Research Institute.

Given the impact on global security, what can be done about these state-sponsored attacks on private citizens and companies? In a novel bid, Amnesty International has tried to push Israeli courts to revoke the export control license for NSO Group's spyware. Meanwhile, a separate lawsuit brought by Facebook against the Israeli tech firm hint at how legal tactics might pave the way for more strategic restrictions on dual-use technology that aids in deploying weaponized narratives (https://weaponizednarrative.asu.edu/). In August 2018, Amnesty International released a 20-page report detailing how the Saudi government used NSO Group's Pegasus spyware (https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/) to tap into the WhatsApp account of an Amnesty staffer working to track human rights developments in Saudi Arabia. A little less than a year later, Amnesty's Israeli chapter filed a lawsuit calling for the Israeli government to bar NSO Group from selling Pegasus outside Israel. Soon after, WhatsApp and its parent company, Facebook, filed a lawsuit that alleged the NSO Group helped foreign governments (https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/whatsapp-sues-israels-nso-for-allegedly-helping-spies-hack-phones-around-the-world-idUSKBN1X82BE) hack and monitor around 1,400 WhatsApp users in 20 different countries, among them journalists, diplomats, dissidents and human rights activists. The NSO Group, which was founded by veteran Israeli intelligence agents, has denied the charges and has vowed to vigorously defend its interests in court.

It remains to be seen whether U.S. federal anti-hacking laws are sufficient to the task of constraining and deterring other spyware companies in the future. In an ideal world, the legal action against the NSO Group would at a minimum encourage the company's leadership to rethink its international sales and marketing strategy. The lawsuits might also serve as a warning to other tech firms hoping to cash in from autocrats like MBS.

At the more strategic level, though, what is really needed is upgrading existing international protocols in a way that prevents the likes of MBS from deploying surveillance tech against ordinary citizens, the media and human rights defenders. Dozens of countries signed on to such an approach in 2013. when they added new surveillance and intelligence-gathering tools, as well as IP network surveillance systems and equipment, to the category of restricted dual-use goods that fall under the oversight regime of the Wassenaar Arrangement (https://www.wassenaar.org/), a non-binding multilateral set of guidelines that calls for export controls on conventional arms and new technologies.

But even those steps may not be enough, as the University of Toronto's Citizen Lab (https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf) has also pointed out. The United States, the European Union and other governments interested in defending democracy are going have to move aggressively in the next few years to pass legislation that gives citizens, firms and organizations targeted by state-sponsored information warfare a path to legal redress for breaches of privacy and defamation. The failure to legislate solutions leaves any protections to the whim of the tech industry.

Ironically, better oversight could be good news for white hat tech firms looking to expand their market share and edge out Facebook by enhancing the public's ability to even the playing field against malign actors. Tech firms like Facebook that are already struggling to convince their shareholders and the public that they can act

with integrity ought to take more serious steps to show more leadership against interlopers like MBS. Otherwise, big tech should be prepared for the day when the public backlash against spyware-wielding autocrats becomes too costly for their shareholders to bear and market reality ultimately bites.

Candace Rondeaux is a senior fellow and professor of practice at the Center on the Future of War, a joint initiative of New America and Arizona State University. Her WPR column (https://www.worldpoliticsreview.com/authors/2516/candace-rondeaux) appears every Friday.

MORE WORLD POLITICS REVIEW

Saudi Arabia's Oil Industry Faces Unprecedented Risk and Uncertainty
(https://www.worldpoliticsreview.com/articles/28278/saudi-arabia-s-oil-industry-faces-unprecedented-risk-and-uncertainty)

Are Saudi Arabia and Its Gulf Neighbors Close to Ending the Qatar Boyc…
(https://www.worldpoliticsreview.com/articles/28443/are-saudi-arabia-and-its-gulf-neighbors-close-to-ending-the-qatar-boycott)

How Spyware Like NSO Pegasus Is Making Dissent More Dangerous
(https://www.worldpoliticsreview.com/articles/28337/how-spyware-like-nso-pegasus-is-making-dissent-more-dangerous)

Can U.N. Diplomacy Head Off Conflict Between the U.S. and Iran?
(https://www.worldpoliticsreview.com/articles/28203/can-u-n-diplomacy-head-off-conflict-between-the-u-s-and-iran)

How the U.N. Human Rights Council's Rebuke of Saudi Arabia Could Rever…

(https://www.worldpoliticsreview.com/articles/27685/how-the-u-n-human-rights-council-s-rebuke-of-saudi-arabia-could-reverberate)

What Jamal Khashoggi's Murder Means for Mohammed Bin Salman's Reform V…

(https://www.worldpoliticsreview.com/insights/26487/what-jamal-khashoggi-s-murder-means-for-mohammed-bin-salman-s-reform-vision)