Mandates of the Special Rapporteur on extrajudicial, summary or arbitrary executions and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
AL SAU 2/2020

17 January 2020

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on extrajudicial, summary or arbitrary executions and Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolutions 35/15 and 34/18.

In this connection, We would like to bring to the attention of your Excellency's Government credible information we have received indicating that Mohammed bin Salman, the Crown Prince of the Kingdom of Saudi Arabia, has been personally involved in the hacking of the cell phone of Jeffrey Bezos, owner of The Washington Post and the Chief Executive Officer of Amazon.com, Inc. The information is based in part on a comprehensive expert forensic analysis of Mr. Bezos' cell phone made available to us.

The Crown Prince and Mr. Bezos exchanged phone numbers on 4 April 2018. The digital forensic analysis strongly suggests that Mr. Bezos' phone was infiltrated on 1 May 2018 through a video file transmitted to Mr. Bezos via a WhatsApp account utilized personally by the Crown Prince (the same number exchanged on 4 April). The video was encrypted, and the file was slightly larger than the video itself.

According to the information we have reviewed, within hours of receipt of the video file, a massive and unauthorized exfiltration of data from Mr. Bezos' phone began, continuing and escalating intermittently for months thereafter, though Mr. Bezos himself remained entirely unaware of the exfiltration during this period. Thereafter, in WhatsApp messages to Mr. Bezos on 8 November 2018, and on 16 February 2019, the Crown Prince reportedly revealed awareness of personal information of Mr. Bezos, not available from public sources.

Reinforcing the credibility of the allegations of hacking described above is public information reporting that Mr. Saud al-Qahtani, a close advisor of the Crown Prince, directed a massive online campaign against Mr. Bezos, including thousands of artificially-trending, coordinated and inauthentic tweets excoriating *The Washington Post* and calling for boycotts of Bezos companies.[1]

[1] See, e.g., https://www.thedailybeast.com/how-the-saudis-made-jeff-bezos-public-enemy-1; https://www.bloomberg.com/news/articles/2018-11-04/saudis-call-for-amazon-boycott-over-anger-at-washington-post

According to publicly available information, Mr. al-Qahtani also worked with an Italian company, Hacking Team, and purportedly purchased an ownership interest in that company on behalf of your Excellency's government. It is further alleged that Hacking Team had received requests from its customers to develop the capability to infect devices via a video sent by WhatsApp. This request is remarkably similar to the Pegasus spyware developed by the NSO Group in order to have the capability to infect phones via WhatsApp and other means. Pegasus has been reportedly deployed by Saudi Arabia against journalist and activist Mr. Omar Abdulaziz and other Saudi nationals.

According to the analysis received, the infiltration of Mr. Bezos' phone was likely facilitated by malicious tools procured by Mr. al-Qahtani, such as a product of NSO (e.g., Pegasus-3). Since the apparent infiltration of Mr. Bezos, Facebook has publicly confirmed the vulnerability associated with "sending a specifically crafted MP4 file to a WhatsApp user." WhatsApp has warned more than 1400 people that they may have been targeted through the use of Pegasus, and in recent months, media reports warned people who "have received a random, unexpected MP4 video file," exactly as Mr. Bezos did on 1 May [2].

We do not wish to prejudge the accuracy of these allegations. However, if true, they point to violations of Mr. Bezos' right to freedom of expression and right to privacy by your Excellency's Government. The allegations also point to possible violations of the rights of others whose personal information might have been disclosed through this infiltration, thereby potentially infringing their rights to freedom of expression, association, religious belief, and culture, their right to privacy, and possibly even their right to life.

Both Special Rapporteurs have repeatedly denounced surveillance of the type reportedly perpetrated here (see A/HRC/41/35 (2019) and A/HRC/41/CRP.1 (2019)). The General Assembly itself has "condemned unlawful or arbitrary surveillance and interception of communications as 'highly intrusive acts' that interfere with fundamental human rights" (A/HRC/41/35, para. 1, quoting UN General Assembly Resolutions General Assembly resolutions 68/167 and 71/199).

This reported surveillance of Mr. Bezos, using software developed and marketed by private companies, is a concrete example of the harm individuals suffer because of the unconstrained sale and marketing of spyware. It reinforces the need for a moratorium on the global sale and transfer of private surveillance technology, as called for by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways."

[2] See, e.g., https://www.facebook.com/security/advisories/cve-2019-11931
https://www.forbes.com/sites/zakdoffman/2019/11/16/new-whatsapp-threat-confirmed-android-and-ios-users-at-risk-from-malicious-video-files/#296f91365ab8
https://thehackernews.com/2019/11/whatsapp-hacking-vulnerability.html

These allegations, if true, also reinforce the concerns expressed by the Special Rapporteur on extrajudicial, summary or arbitrary executions about the role surveillance played in the murder of Mr. Jamal Khashoggi. Importantly, they point to the potential involvement of the Crown Prince himself in the surveillance and targeting not only of his perceived opponents but also of people of strategic importance, including non-nationals.

These allegations thus are relevant in evaluating claims concerning the extent of the Crown Prince involvement in the targeting and ultimate murder of Mr. Jamal Khashoggi. Moreover, the information received concerns allegations that are remarkably similar to the kinds of surveillance conducted against associates of Mr. Khashoggi and may have been conducted against Mr. Khashoggi himself. It is further alleged that during the same period Mr. Bezos' phone was apparently infiltrated, so were the phones of at least four Saudi nationals allegedly perceived by the Crown Prince as adversaries.

In her report presented to the Human Rights Council in March 2019, "Investigation into the Unlawful Death of Mr. Jamal Khashoggi", the Special Rapporteur found that the Crown Prince "played an essential role in permitting [a] campaign against dissidents and political opponents to occur, as the forces of the State could not be used in this manner without his agreement or acquiescence" (see, A/HRC/41/CRP.1 para. 257(c)).

The report described how, as part of this campaign, the cell phone of Mr. Abdulaziz had been infected with Pegasus spyware, an infiltration attributed by the widely respected academic and forensic research institute, Citizen Lab, to your Excellency's government.[3] "Pegasus had allowed the Saudi-linked operator to access Mr. Abdulaziz's phone contacts, photos, text messages, online chat logs, emails, and other personal files. The operator also had the ability to use the phone's microphone and camera to secretly view and eavesdrop on Mr. Abdulaziz." (A/HRC/41/CRP.1, para. 68). Mr. Abdulaziz was a friend of Mr. Khashoggi, so this hacking potentially permitted your Excellency's government to spy on some of Mr. Khashoggi's communications.

Reinforcing the credibility of the allegations of Saudi online campaigns against perceived opponents, since the UN report on the execution of Mr. Khashoggi was issued, the United States has brought criminal proceedings against two Twitter employees and a Saudi national "for their respective roles in accessing private information in the accounts of certain Twitter users and providing that information to officials of the Kingdom of Saudi Arabia."[4] All three individuals are charged with being illegal agents for your Excellency's government who, according to U.S. prosecutors, engaged in the "targeting

[3] https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/ .

[4] "Two Former Twitter Employees and a Saudi National Charged as Acting as Illegal Agents of Saudi Arabia, Press Release, U.S. Department of Justice, Office of Public Affairs, November 7, 2019 https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia

and obtaining private data from dissidents and known critics, under the direction and control of the government of Saudi Arabia".[5]

The criminal complaint identifies an official of your Excellency's Government as central in "cultivating employees of Twitter in an effort to obtain private user information that he could not obtain elsewhere". This official allegedly identified the target accounts and arranged for payments to those obtaining the private data from them.[6] He is identified as being the Secretary General of a charitable organization belonging to a member of the Royal Court, identified as Royal Family Member-1.

We are informed that this foreign official may be the Secretary General of the MiSK Foundation, a charity owned by the Crown Prince, who appears to be "Royal Family Member-1" in the complaint. If these allegations are true, they again suggest the personal involvement of the Crown Prince in targeting Saudi dissidents.

These allegations are relevant to the factual background concerning the murder of Mr. Khashoggi and suggest a continuous, multi-year, direct and personal involvement of the Crown Prince in illegal efforts to target perceived opponents. They add support to the allegations, warranting further investigation, that the Crown Prince personally supervised, or at a minimum was aware of, the mission targeting Mr. Khashoggi in Istanbul, whether or not he specifically ordered his murder.

In connection with the above alleged facts and concerns, please refer to the **Annex on Reference to international human rights law** attached to this letter which cites international human rights instruments and standards relevant to these allegations.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all cases brought to our attention, we would be grateful for your observations on the following matters:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.

2. Who, other than the Crown Prince himself, had and has access to the WhatsApp account used by the Crown Prince to communicate with Mr. Bezos?

3. What standards does your Excellency's Government use to ensure that the deployment of surveillance software or "spyware" against private individuals is solely undertaken for lawful purposes under international human rights law? What, if any, laws or regulations are in place to regulate

[5] Id., https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia
[6] Criminal Complaint, November 5, 2019, para. 25, https://www.justice.gov/opa/press-release/file/1215836/download

the use by State officials of spywares against individuals? What public authorities have the power to authorize their use against private individuals?

4. Please provide detailed information about your Excellency Government's contracts with private surveillance companies, such as NSO Group and Hacking Team that include the provision of software and services to conduct intrusive surveillance.

5. Has your Excellency's government ever taken corrective action after any inappropriate or unlawful use of spyware by state officials? What kind of oversight has your Excellency's Government developed to preclude unlawful uses of spyware by officials?

6. What actions has your Excellency's Government taken in response to the US federal criminal charges, referred to above, relating to Twitter? Has it taken any action with respect to the Saudi citizen charged with criminal violations under United States law?

7. In the investigation undertaken by your Excellency's Government of Mr. Khashoggi's murder, was there any effort to determine the extent to which there was official surveillance of Mr. Khashoggi and of any of his acquaintances? If so, what was the investigation and what were its results?

8. Has there been any investigation of Mr. Saud al-Qahtani's use of spyware against potential political opponents or dissidents?

9. What actions does your Excellency's Government plan in response to the allegations with respect to the infiltration of Mr. Bezos' phone?

This communication and any response received from your Excellency's Government will be made public via the communications reporting website within 60 days. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

While awaiting a reply, we urge that all necessary interim measures be taken to halt the alleged violations and prevent their re-occurrence and in the event that the investigations support or suggest the allegations to be correct, to ensure the accountability of any person(s) responsible for the alleged violations.

We may publicly express our concerns in the near future as, in our view, the information upon which the press release will be based is sufficiently reliable to indicate a matter warranting immediate attention. We also believe that the wider public should be alerted to the potential implications of the above-mentioned allegations. The press release will indicate that we have been in contact with your Excellency's Government's to clarify the issue/s in question.

Please accept, Excellency, the assurances of our highest consideration.

Agnes Callamard
Special Rapporteur on extrajudicial, summary or arbitrary executions

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Annex One
Reference to international human rights law

In connection with the above alleged facts and concerns, we would like to refer Your Excellency's Government to Article 3 of the Universal Declaration of Human Rights which states that "Everyone has the right to life, liberty and security of person".

The right to life is a foundational and universally recognized right, applicable at all times and in all circumstances, including during armed conflict or other public emergency. This right to life is a norm of *jus cogens*, and is protected by international and regional treaties, customary international law and domestic legal systems. The obligation to respect the right to life also applies extraterritorially. The right to life has two components. The first and material component is that every person has a right to be free from the arbitrary deprivation of life. The second and more procedural component is the requirement of proper investigation and accountability where there is reason to believe that an arbitrary deprivation of life may have taken place. States are required to respect and to protect the right to life "by law": "Deprivation of life is, as a rule, arbitrary if it is inconsistent with international law or domestic law." The "notion of 'arbitrariness' is not to be fully equated with 'against the law', but must be interpreted more broadly to include elements of inappropriateness, injustice, lack of predictability, and due process of law as well as elements of reasonableness, necessity, and proportionality." Arbitrary deprivation of life includes the intentional and often premeditated use of lethal State force outside of the judicial process – killings often referred to as extra-judicial executions. Abuse of state power to bring about a politically sanctioned arbitrary killing against a specific group or individual ignores state obligations to ensure due process, and constitutes a violation of the fundamental right to life as well as a violation of the rule of law. Moreover, the wider impact that an intentional targeted killing has on society is an element that may distinguish these acts from other violations of the right to life. As a result of this abhorrent abuse of power and blatant disregard for the rule of law, extrajudicial killings have been considered, by the International Commission of Jurists, as a "grave human rights violation". This categorization does not limit the scope of what falls under grave human rights violations but merely serves as an effort to describe the severity of extrajudicial killings (A/HRC/41/CRP.1).

Saudi Arabia is subject to this peremptory and customary norm and is obligated to respect the right to life. The Arab Charter on Human Rights, which Saudi Arabia has ratified, recognizes that "[e]very human being has the inherent right to life", that the "right shall be protected by law", and that "[n]o one shall be arbitrarily deprived of his life." In making this declaration of rights, the Arab Charter "reaffirms the principles of the Charter of the United Nations, the Universal Declaration of Human Rights and the provisions of the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights.". In addition, Saudi Arabia has also ratified the Convention against Torture.

Furthermore, we would like to note that the UDHR protect everyone's rights to privacy, opinion and expression. In particular, Article 12 of the UDHR states that "No

one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

We also wish to stress that the ICCPR, to date ratified by 173 States, provides in Article 17 that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks".

In his report on Surveillance and human rights (A/HRC/41/35), the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted that Governments deploying surveillance tools must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. Surveillance should only be authorized in law for the most serious criminal offences. To be compliant with those standards, national laws must:

(a) Emphasize that everyone enjoys the right not to be subjected to unlawful or arbitrary interference with his or her privacy;

(b) Require that any legislation governing surveillance be contained in precise and publicly accessible laws and only be applied when necessary and proportionate to achieve one of the legitimate objectives enumerated in article 19 (3) of the International Covenant on Civil and Political Rights;

(c) Ensure that a surveillance operation be approved for use against a specific person only in accordance with international human rights law and when authorized by a competent, independent and impartial judicial body, with all appropriate limitations on time, manner, place and scope of the surveillance;

(d) Require, given the extreme risks of abuse associated with targeted surveillance technologies, that authorized uses be subjected to detailed record-keeping requirements. Surveillance requests should only be permitted in accordance with regular, documented legal processes and the issuance of warrants for such use. Surveillance subjects should be notified of the decision to authorize their surveillance as soon as such a notification would not seriously jeopardize the purpose of the surveillance.

We would also like to recall that the Special Rapporteur on extrajudicial, arbitrary or summary executions recommended States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools to Saudi Arabia and other States until a human rights-compliant safeguards regime is in place; any allegations that such equipment may have been misused should be the object of independent and transparent investigations by the relevant authorities; and implement other measures recommended by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his report A/HRC/41/36.

Annex Two

Analysis of the Evidence of Surveillance of Mr. Bezos' personal phone
- Key Technical Elements -

To complement the preliminary substantive findings and associated expressions of concern by the Special Rapporteurs to the Saudi authorities regarding their alleged surveillance of Mr. Bezos, the following annex summarises the technical methodologies deployed to establish grounds for a reasonable belief (a "medium to high confidence" to use the precise wording of the technical experts involved) that Mr. Bezos was subjected to intrusive surveillance via hacking of his phone as a result of actions attributable to the WhatsApp account used by Crown Prince Mohammed bin Salman.

An in-depth, forensic level examination of Mr. Bezos' phone – including full forensic imaging and analysis - was undertaken by a team of digital forensic experts. According to the expert team, this forensic study was undertaken in a protected environment specifically created to enable thorough investigation of the phone without risk of contamination. A full report of the expert findings was made available to the Special Rapporteurs.

The phone in question underwent the following tests:

Test undertaken	Tool used	Finding/result
Logical mobile acquisition	Cellebrite UFED 4PC	Acquisition successful
Network package collection while device was locked, unlocked, idle and while simulating activity	Wireshark, Fiddler	Collection of network traffic successful
Presence of malware	Cellebrite Physical Analyser	No known malware detected
Presence of conventional or typical malicious software	Cellebrite Physical Analyser; use of a sandboxed network to simulate an active internet connection	Vetted 350,579 unique hashes but no known malicious software detected
Presence of suspect indicators of compromise (IOCs) from the network capture logs	Cellebrite reports and captured network logs	Identified 1,290 URLs and 378 unique domain names and identified 192 potentially suspect IOCs
In-depth audit of 192 suspect IOCs	Manual review by experts	No evidence found that any of the identified domain names or URLs were related to malicious traffic.

Test undertaken	Tool used	Finding/result
Presence of jail-breaking tools and known iOS exploits tools	In-depth investigation of logical file system - auditing 274,515 directories, sub-directories and filenames	No evidence found of jail-breaking tools or known iOS exploits being present.
Analysis of suspect video file (sent to Mr. Bezos on WhatsApp from the Crown Prince's account as provided by to Mr. Bezos by the Crown Prince)	Analysis of the WhatsApp artifacts from Cellebrite reports	Initial results did not identify the presence of any embedded malicious code, but further analysis revealed that the suspect video had been delivered via an encrypted downloader host on WhatsApp's media server.
Analysis of the contents of the downloader	Attempted decryption	Due to WhatsApp's end-to-end encryption, the contents of the downloader cannot be practically determined.
Comparative analysis of cellular data egress with past usage of Mr. Bezos' phone	Analysis of the forensic artifacts from the Cellebrite reports	Records showed that within hours of receipt of the video from the Crown Prince's WhatsApp account, there was an anomalous and extreme change in phone behavior, with cellular data originating from the phone (data egress) increasing by 29,156 per cent. Data spiking then continued over the following months at rates as much as 106,031,045 per cent higher than the pre-video data egress base line.
Comparative analysis of cellular data egress with devices similar to the Bezos phone	Expert analysis of five other similar devices	Up until the day the suspect video file was received, data egress patterns were found to be similar – and explicable by nature of activity undertaken – across all five devices and Mr. Bezos' phone. Following receipt of the suspect video file, a stark contrast was found in the magnitude of data egress from Mr. Bezos' phone as compared to the five other phones.

Test undertaken	Tool used	Finding/result
Assessment of possible use of mobile spyware – cyber weapons	Expert analysis of likelihood of cyber weapons as methods for anomalous stimulation and capture of data egress	Experts advised that the most likely explanation for the anomalous data egress was use of mobile spyware such as NSO Group's Pegasus or, less likely, Hacking Team's Galileo, that can hook into legitimate applications to bypass detection and obfuscate activity. For example, following the initial spike of exfiltration after receipt of the suspect video file, more than 6GB of egress data was observed using exfiltration vectors.

Annex Three

Brief Timeline of Key Events

KEY DATE	EVENT
December 2016	At a Washington-based think-tank, Jamal Khashoggi makes critical remarks about Donald Trump's ascent to the US presidency. Soon after, the Saudi regime cancelled Mr. Khashoggi's column in the al-Hayat newspaper, and ultimately banned him from writing, appearing on television, and attending conferences. A Saudi official explained that Mr. Khashoggi's statements "do not represent the government of Saudi Arabia or its positions at any level, and his opinions only represent his personal views, not that of the Kingdom of Saudi Arabia." Mr. Khashoggi's subsequent exile from Saudi Arabia was self-imposed, based upon his belief that for his own safety and freedom he had no other choice but to leave.
September 2017	The Washington Post publishes Mr. Khashoggi's first column: "*Saudi Arabia wasn't always this repressive. Now it's unbearable.*"
November 2017	Pegasus-3 spyware is acquired from NSO Group by the Saudi regime, specifically the Saudi Royal Guard.
February 7, 2018	Washington Post publishes a column by Mr. Khashoggi entitled: "*Saudi Arabia's crown prince already controlled the nation's media. Now he's squeezing it even further*."
February 28, 2018	Washington Post publishes a column by Mr. Khashoggi in which he writes: "…maybe [the Crown Prince] should learn from the British royal house that has earned true stature, respect and success by trying a little humility himself."
March 21, 2018	Washington Post owner, Mr. Bezos, is invited to attend a small dinner with the Crown Prince in Los Angeles.
April 3, 2018	Washington Post publishes a column by Mr. Khashoggi while the Crown Prince is in the U.S. in which Mr. Khashoggi writes: "…replacing old tactics of intolerance with new ways of repression is not the answer."
April 4, 2018	Mr. Bezos attends dinner with the Crown Prince, in the course of which they exchange phone numbers that correspond to their WhatsApp accounts.
May 1, 2018	A message from the Crown Prince account is sent to Mr. Bezos through WhatsApp. The message is an encrypted video file. It is later established, with reasonable certainty, that the video's downloader infects Mr. Bezos' phone with malicious code.
May, 2018	The phone of Saudi human rights activist Yahya Assiri is infected with

	malicious code. Yahya Assiri was in frequent communication with Mr. Khashoggi.
June, 2018	The phone of Saudi political activist Omar Abdulaziz is infected with malicious code, via a texted link on Whats App. Omar Abdulaziz was in frequent communication with Mr. Khashoggi.
June, 2018	The phone of an Amnesty International official working in Saudi Arabia is targeted for infection via a WhatsApp link that it is determined leads to an NSO Group-controlled website.
June 23, 2018	The phone of Saudi dissident Ghanem al-Dosari is targeted via a text link leading to NSO infrastructure.
June 23, 2018	A second phone of Saudi dissident Ghanem al-Dosari is targeted via a text link leading to NSO infrastructure.
October 2, 2018	Mr. Khashoggi is killed by Saudi government officials. The Washington Post begins reporting on the murder, publishing ever-expanding revelations about the role of the Saudi government and of the Crown Prince personally.
October 15, 2018	Massive online campaign against Mr. Bezos begins, targeting and identifying him principally as the owner of The Washington Post. In November, the top-trending hashtag in Saudi Twitter is "Boycott Amazon." The online campaign against Mr. Bezos escalates and continues for months.
November 8, 2018	A single photograph is texted to Mr. Bezos from the Crown Prince's WhatsApp account, along with a sardonic caption. It is an image of a woman resembling the woman with whom Bezos is having an affair, months before the Bezos affair was known publicly.
February 25, 2019	The Daily Beast runs an op-ed by Iyad el Baghdadi entitled "How the Saudis Made Jeff Bezos Public Enemy No. 1."
March 31, 2019	Hundreds of major news outlets around the world report on the allegation that Saudi Arabia had access to Mr. Bezos' phone and had obtained private data. The allegation was first published in a Daily Beast op-ed by Gavin de Becker, and subsequently reported by the NY Times, CNN, al Jazeera, BBC, Bloomberg, Reuters, and others.
April 1, 2019	The entire Saudi online campaign against Mr. Bezos stops abruptly, strongly indicating inauthentic and coordinated hashtags and tweets.
April 25, 2019	Intelligence officials in Norway advise Iyad el Baghdadi of a CIA warning that he is being targeted by the Saudis and move him from his home. Intelligence sources believe the threats are connected to Mr. Baghdadi's work on Jeff Bezos.
May 1, 2019	Mr. el Baghdadi is advised by a source in Saudi Arabia that the Saudis have successfully targeted his phone.
September 20, 2019	Twitter suspends 5000 accounts for "inauthentic behavior," including

that of an advisor to the Crown Prince, Saud al Qahtani.

October 1, 2019 Mr. Bezos attends the memorial for Mr. Khashoggi held outside the Saudi Consulate in Istanbul where Mr. Khashoggi was murdered.

October 2, 2019 The Saudi online campaign against Mr. Bezos resumes after being dormant for months, specifically citing Mr. Bezos' attendance of the memorial event, and again calling for boycott of Amazon. CNN Arabia reports on the new campaign.

October 29, 2019 Facebook sues the NSO Group in U.S. federal court for trying to compromise the devices of up to 1,400 WhatsApp users' in just two weeks.

November 5, 2019 The US Department of Justice charges three people with serving as Saudi spies inside Twitter. One of the three had left Twitter and gone to work at Amazon.

November 14, 2019 Facebook confirms that "sending a specifically crafted MP4 [video] file to a WhatsApp user," is a method for installing malicious spyware; exactly as was sent to Mr. Bezos.

November 15, 2019 Several news outlets report on a WhatsApp vulnerability, and warn those who "have received a random, unexpected MP4 video file," exactly as Bezos did, to beware.

December 20, 2019 Twitter suspends 88,000 accounts linked to Saudi spying case, saying that the accounts were associated with "a significant state-backed information operation" originating in Saudi Arabia.