

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF FLORIDA  
(MIAMI DIVISION)**

Ghada Oueiss,

Plaintiff,

v.

Mohammed Bin Salman Bin Abdulaziz Al Saud, Mohammed Bin Zayed Al Nahyan, DarkMatter, Faisal al Bannai, Saudi 24 TV, a broadcast television station owned by the Kingdom of Saudi Arabia, Al Arabiya, a broadcast television station owned by the Kingdom of Saudi Arabia, Prince Mohammed Bin Salman Abdulaziz Foundation d/b/a MiSK Foundation, Saud Al Qahtani, Bader Al-Asaker, Saudi Arabian Cultural Mission, Tarek Abou Zeinab, Turki Al-Owerde, Faisal Al Menaia, Awwad Al Otaibi, Sharon Collins, Christanne Schey, Hussam Al-Jundi, Annette Smith, John Does 1-20,

Defendants.

Case No. \_\_\_\_\_

**Complaint**

Plaintiff Ghada Oueiss (“Ms. Oueiss” or “Plaintiff”) for her complaint against Defendants Mohammed bin Salman Bin Abdulaziz Al Saud, Mohammed Bin Zayed Al Nahyan, DarkMatter, a cybersecurity company headquartered in Abu Dhabi, Faisal al Bannai, Saudi 24 TV, a broadcast television station owned by the Kingdom of Saudi Arabia, Al Arabiya, a broadcast television station owned by the Kingdom of Saudi Arabia, Prince Mohammed Bin Salman Abdulaziz Foundation d/b/a MiSK Foundation, Saud Al Qahtani, Bader Al-Asaker, Saudi Arabian Cultural Mission, Tarek Abou Zeinab, Turki Al-Owerde, Faisal Al Menaia, Awwad Al Otaibi, Sharon Collins, Christanne Schey, Hussam Al-Jundi, Annette Smith, and John Does 1-20 (together “Defendants”), alleges and states as follows:

## INTRODUCTION

1. This is a civil action arising out of the targeted unlawful hacking of Plaintiff, Ghada Oueiss, an international journalist who has a significant presence in the U.S. and abroad, both as a journalist for *Al Jazeera Media Network* (“*Al Jazeera*”) and as a frequent contributor to U.S. news agencies, such as *The Washington Post*. This unlawful hack and leak operation against Ms. Oueiss (the “Conspiracy”) was spearheaded by the crown princes of Saudi Arabia and the United Arab Emirates (“UAE”) and their co-conspirators in the U.S. and elsewhere.

2. The hack and leak operation was directed and controlled by foreign actors who created an American infrastructure comprised of various U.S. citizens that worked in concert to viciously attack Ms. Oueiss. As discussed below, all these Defendants – both foreign and domestic – worked together to carry out a multi-faceted conspiracy and attack on Ms. Oueiss.

3. Briefly put, the Conspiracy against Ms. Oueiss consists of three stages: (1) the “recruiting stage,” whereby Saudi government officials and agents of the crown princes of Saudi Arabia utilized their positions in U.S.-based entities (such as the Saudi Arabian Cultural Mission) to recruit American citizens to join a campaign to promote pro-Saudi and pro-UAE disinformation and attack any critics of the regimes, including Ms. Oueiss; (2) the “hacking stage,” whereby Defendants hacked Ms. Oueiss’ personal mobile device on several occasions; and (3) the “dissemination, amplification, and defamation stage,” whereby Defendants, in the U.S. and abroad, disseminated stolen personal images of Ms. Oueiss, with full knowledge of the hacking operation, all in an attempt to defame, disparage and intimidate Ms. Oueiss from continuing to report on the regimes’ human rights abuses.

4. Why did these wrongdoers engage in this Conspiracy against Ms. Oueiss? Obsessed with maintaining a polished standing, the de facto rulers of the UAE and Saudi regimes are determined to whitewash their public images in the eyes of the American government and its

citizens. One way to accomplish this goal is to eviscerate all critics of their regimes—no matter the veracity of the critics’ statements about the regimes.

5. Ms. Oueiss brings this action against all Defendants – domestic and foreign – responsible for the unlawful hacking and dissemination of her personal information worldwide, with key supporting acts committed in the State of Florida where two Defendants – Sharon Collins and Hussam Al-Jundi – engaged in tortious acts, including publishing the stolen information and actively participating in the Conspiracy against Ms. Oueiss. Each actor must be held responsible for their unlawful actions and Conspiracy against Ms. Oueiss, and this lawsuit marks the beginning of a journey toward justice for Ms. Oueiss.

#### **EVISCERATING CRITICS OF THE SAUDI AND UAE REGIMES**

6. On October 2, 2018, journalist Jamal Khashoggi was ambushed, asphyxiated, murdered, and then dismembered. As he lay lifeless in the building of the Saudi Embassy in Turkey, his killers chatted casually—unaware that they were being recorded.

7. “I normally put on my earphones and listen to music when I cut cadavers. In the meantime, I sip on my coffee and smoke. After I dismember it, you will wrap the parts into plastic bags, put them in suitcases and take them out [of the building].” The man who uttered those vile words is Salah Mohammed Abdah Tubaigy. He was recorded during and after the murder, discussing how he would dispose of the evidence. He is just one of more than 15 Saudi killers who participated in this state-sanctioned assassination.

8. Mr. Khashoggi was a brilliant journalist. An ardent dissident of Saudi Arabia, and a columnist for *The Washington Post*, his sole crime was his outspoken support for Saudi progressivism and his criticism of the Saudi government and its de facto leader, Crown Prince Mohammed bin Salman bin Abdulaziz Al Saud (“MBS”).

9. In the months leading up to his murder, Mr. Khashoggi was constantly attacked by an army of Twitter, Inc. (“Twitter”) trolls who were acting at the behest of the Saudi government. These Twitter trolls, assembled by the Saudi regime to attack Mr. Khashoggi on Twitter, were individuals hiding behind inauthentic accounts, commonly referred to as “bot” accounts.<sup>1</sup> These “bot” accounts consistently posted intentionally inflammatory, defamatory, or upsetting statements on Twitter to, among other things, steer the conversation off-topic.

10. As explained in Ms. Maggie Mitchell Salem’s (a friend of Mr. Khashoggi) interview with the *New York Times*, “[t]he mornings were the worst for him because he would wake up to the equivalent of sustained gunfire online[.]”<sup>2</sup> These attackers carrying out this offensive cyber effects operation were “part of a broad effort dictated by Crown Prince Mohammed bin Salman and his close advisers to silence critics both inside Saudi Arabia and abroad.” *Id.* This type of information warfare is something that Saudi Arabia has perfected, having gone so far as to infiltrate companies like Twitter. Indeed, as reported by the *New York Times*,<sup>3</sup> it was against the backdrop of this onslaught of internet attacks, orchestrated, curated and executed by the Saudi regime, that Mr. Khashoggi was eventually murdered.

11. Mr. Khashoggi’s case is tragic. But equally upsetting is that this was a murder that was carried out at the behest of a de facto ruler of a country. The Central Intelligence Agency of the United States (“CIA”) determined, after investigating this crime, that MBS ordered this murder.

---

<sup>1</sup> <https://us.norton.com/internetsecurity-emerging-threats-what-are-twitter-bots-and-how-to-spot-them.html#:~:text=Twitter%20bots%2C%20also%20known%20as,goals%20on%20a%20large%20scale>. (“Twitter bots . . . are automated Twitter accounts controlled by bot software. While they are programmed to perform tasks that resemble those of everyday Twitter users – such as liking tweets and following other users – their purpose is to tweet and retweet content for specific goals on a large scale.”).

<sup>2</sup> <https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html>

<sup>3</sup> *See id.* (“The vigorous push also appears to include the grooming-not previously reported- of a Saudi employee at Twitter whom Western intelligence officials suspected of spying on user accounts to help Saudi leadership.”).

12. Equally telling of MBS's culpability in Mr. Khashoggi's murder is MBS's own recognition and admissions through the action of his co-conspirators' acknowledgment of orchestrating the murder. As further set forth below, high standing members of the Saudi network and co-conspirators have openly threatened Ms. Oueiss in connection to her coverage or by direct reference to Mr. Khashoggi's fate. MBS's endorsement of such action, both by action and inaction, constitutes an admission of culpability and responsibility for the murder.

13. After this horrific event, *Time* named Mr. Khashoggi as the "person of the year," publishing its appreciation for his journalistic acumen and calling him a "Guardian of the Truth."

14. Mr. Khashoggi was not alone, however, in his outspoken view of the Saudi regime.

15. Saudi Arabia has been criticized by Human Rights Watch, Amnesty International, and the U.S. Department of State for unlawful killings, executions for non-violent offenses, forced renditions, forced disappearances, torture, violence and discrimination against women, censorship, and even severe restrictions of religious freedoms.

16. Thus, Plaintiff, Ms. Ghada Oueiss, a 44-year-old journalist who has published her reporting in media outlets around the world, including the U.S., is just the most recent victim of Saudi operatives using American instrumentalities to further varying objectives.

17. Ms. Oueiss earned her degree from Lebanese University of Journalism, graduating in 1999. Ms. Oueiss joined *Al Jazeera* in 2006 and has since published various articles for U.S.-based news agencies including *The Washington Post*.

18. Ms. Oueiss is the recipient of the 2013 May Chidiac Foundation Award for Journalism.

19. Like Mr. Khashoggi, Ms. Oueiss has written on topics focused on Saudi Arabia's human rights abuses, notwithstanding the risk to her life.

20. After Mr. Khashoggi was murdered for being a guardian of truth adverse to Saudi Arabia's interests, Ms. Oueiss publicly reported on the Saudi regime's involvement in the assassination.

21. And she did not relent, ever mindful of the fact that a brutal murder had been committed with total impunity. In doing so, Ms. Oueiss earned the attention of the Saudi regime. What followed was a premeditated attack, intended to destroy her reputation, personal life, and career.

22. Ms. Oueiss is one of the most recent of a list of journalists targeted by joint and coordinated efforts of Saudi and UAE leadership, which leverage multiple entities and vectors using social media harassment campaigns and targeted hacking efforts to defame, humiliate and harm dissidents and any others that report facts unaligned with the Saudi or UAE regimes.

23. On the Saudi front, Abdullatif al-Shaikh, a high standing social member of Saudi society, kicked off the social media attack against Ms. Oueiss by calling her a "prostitute" on Twitter. He then brazenly threatened Ms. Oueiss, tweeting a picture of Ms. Oueiss next to a photograph of Mr. Khashoggi's fiancée with the threat "Very soon." This was only the beginning of the onslaught against Ms. Oueiss.<sup>4</sup>

24. Abdullatif al-Shaikh would never have made such a threat without MBS's approval, tacit or otherwise. MBS has never denounced this brazen threat, another recognition of Saudi involvement.

25. Ms. Oueiss was harkened back to what her friend Mr. Khashoggi had told her about how to deal with the coordinated Saudi and UAE social media harassment. On August 31, 2018,

---

<sup>4</sup> See <https://womeninjournalism.org/cfwij-press-statements/saudi-arabia-journalist-ghada-oueiss-is-once-again-attacked-by-accounts-suspected-to-be-tied-to-the-saudi-government> (discussing the Saudi regime's involvement in disseminating the hacked photographs of Ms. Oueiss, while simultaneously "deploying and buying [Twitter] accounts to troll and attack" women journalists, such as Ms. Oueiss).

shortly before he was murdered, Mr. Khashoggi told Ms. Oueiss: “Block them and ignore and do not upset yourself. That’s what I do.” Ms. Oueiss responded: “Hello mentor, you are absolutely right, but although I am getting used to this and it doesn’t upset me anymore, I still want to shed light to their style.”



26. When Ms. Oueiss fought back instead, by retweeting her attackers' tweets with the goal of exposing them and continuing her reporting, the Saudi and UAE operatives escalated their attacks.

27. In a shocking turn, the Saudi regime, having previously relied on bots and government officials, elevated their attacks to a new instrument of Saudi warfare: the use of unregistered American agents to work for and promote foreign interests in the U.S.

28. On three separate occasions from February 2020 through June 2020, Ms. Oueiss woke up to new Saudi attacks meant to disparage and embarrass her in online public forums where she regularly operates. On the first occasion, doctored financial documents were leaked across pro-Saudi media outlets attempting to damage Ms. Oueiss' journalistic integrity. On the second and third occasions, private photographs from Ms. Oueiss' mobile device were posted on social media in escalating attempts to sully her reputation. The third and most egregious attack leaked numerous screenshots of a video from Ms. Oueiss' mobile device, which were altered in a way to falsely make her look nude. These leaked photographs were plastered across social media platforms and various "news" websites (which, as discussed below, were created at the behest of MBS and other named Defendants solely for the purpose of spreading disinformation about Ms. Oueiss).

29. A series of attacks on Ms. Oueiss' persona, womanhood, character, and personal life were being executed and amplified on social media. How did this occur? Ms. Oueiss was the target of a coordinated effort to hack her mobile device and subsequently defame her. Her mobile device was hacked by a then-unknown person or entity, and the contents of her mobile device (including personal photographs of Ms. Oueiss) were stolen. As alleged herein, forensic evidence obtained from her mobile device and other evidence reveals that the individuals and entities

responsible for the hacking of her personal mobile device acted at the behest of MBS and the Crown Prince of the UAE, acting in concert with the other named Defendants.

30. These attacks were global, including attacks focused in the U.S. where a group of Americans—recruited by and working in lockstep with members of the Saudi government—proliferated and promoted the Saudi and UAE agenda online.

31. The attacks began with offensive posts and online harassment, escalated to the posting of doctored financial documents, and then peaked with the hacking of Ms. Oueiss' personal mobile device and the posting and amplification of personal photographs that made her the subject of thousands of tweets and threatened her professionally and personally. Eventually, Ms. Oueiss even received various phone calls and text messages from unknown individuals threatening her life and career. These harassing calls and messages continue to this day.

32. Unlike the “bot” accounts discussed above, the attackers that have targeted Ms. Oueiss are real people. These agents are American citizens residing in the U.S. who, while not appearing to have any affiliation with Saudi Arabia, have been recruited by the other Defendants to accomplish Saudi goals of manipulating the American public through disinformation.

33. This case is brought to address the unlawful conduct by the de facto rulers of the Saudi and UAE regimes, their foreign agents, and their U.S. mercenaries, which has been directed at the U.S. and at Plaintiff, and for which Plaintiff seeks damages and injunctive relief.

#### **DESCRIPTION OF PARTIES AND THE “NETWORK”**

##### ***Plaintiff***

34. Plaintiff Ms. Ghada Oueiss is a principal anchor and presenter for *Al Jazeera*, which is headquartered in Doha, Qatar, and she regularly reports on human rights issues. A frequent contributor to the *Washington Post*, George Washington University, and Publications International

Press Institute (of which she is a member), she has worked for several newspapers, television channels and radio stations.

35. With a viewership of over 8,000,000 in the U.S., Ms. Oueiss derives a portion of her income from her work in the U.S. Ms. Oueiss visits the U.S. frequently for both personal and professional reasons.<sup>5</sup> In 2012, for example, she visited the U.S. to cover the Presidential election. In 2014, she visited Florida to visit family members, some of whom reside in Florida. In 2018, she returned again to the U.S. again to cover the congressional elections. Ms. Oueiss has been to the U.S. as recently as the fall of 2019.

36. Ms. Oueiss' prominence as a journalist has resulted in her obtaining millions of followers on social media. Ms. Oueiss has approximately 150,000 followers on Instagram, approximately 10,000 of which reside in the U.S. Ms. Oueiss has approximately 2 million followers on Facebook, approximately 200,000 of which reside in the U.S. Ms. Oueiss has approximately 850,000 followers on Twitter, at least 8,500 of which reside in the U.S.

37. As discussed below, Ms. Oueiss has been attacked by U.S. agents of Defendants MBS, Al Qahtani and Al-Asaker, among others. These U.S. agents have not notified the U.S. government of their agreement with Defendants to carry out this multi-faceted campaign against Ms. Oueiss, and a significant portion of this operation has been conducted by two Defendants in Florida. As shown in detail below, these U.S. agents, together with other foreign actors on Twitter, have formed a cohesive network (the "Network") on Twitter, to spread pro-Saudi and pro-UAE propaganda and ruthlessly attack anyone who dares to report on these regimes' human rights abuses.

---

<sup>5</sup> See, e.g., <https://www.hotelstrata.com/events/palo-alto/palo-alto-reach-education-fund-tour-with-ghada-oueiss-4565112>

*The American Nodes*

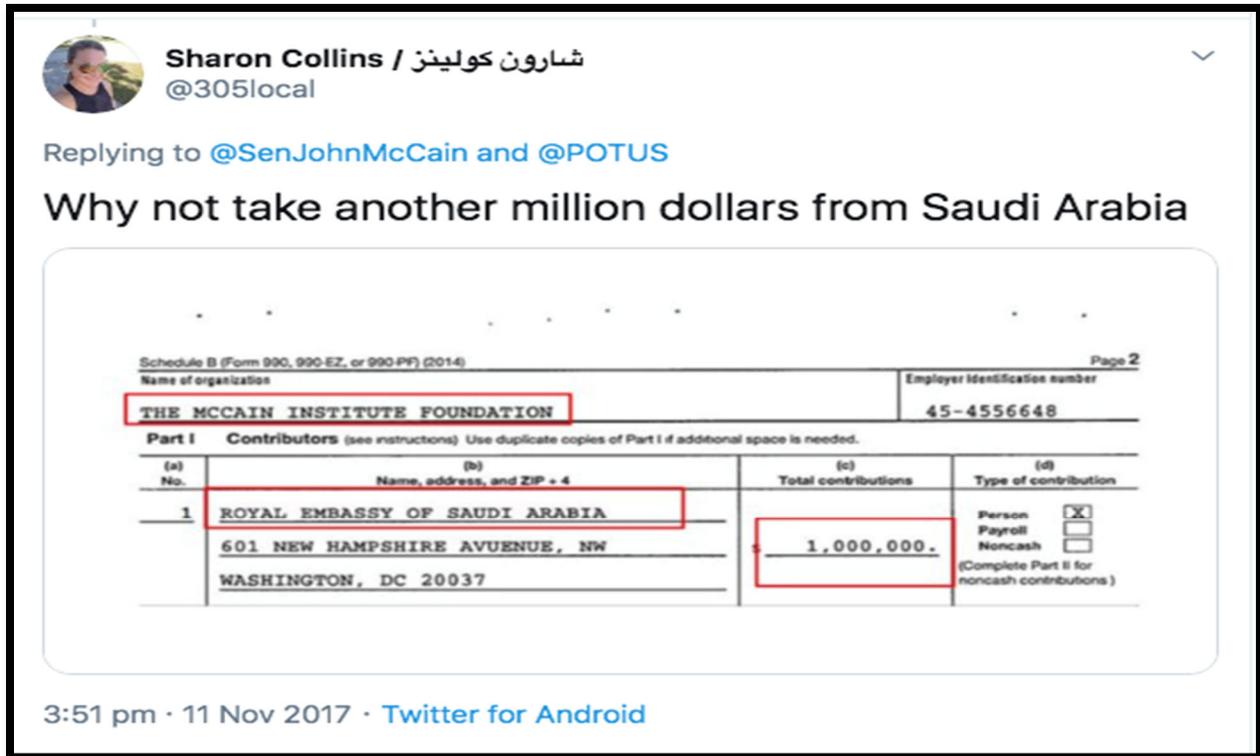
*Defendant Sharon Collins*

38. Defendant Sharon Collins is an American citizen who resides in Miami, Florida. Defendant Collins is the owner of a Florida-based automobile-related company. She is active on Twitter using the Twitter “handles” @305local, which was created in July 2011, and @305local2, which was created in November of 2017.<sup>6</sup> Through these handles, she has posted pro-Saudi disinformation and defamatory statements about Ms. Oueiss, and she knowingly disseminated doctored versions of private photographs that were stolen from Ms. Oueiss’ mobile device, all in furtherance of the Conspiracy discussed in this Complaint. She is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act.

39. Prior to 2018, Defendant Collins’ main Twitter account (@305local) did not appear to be geared toward any political agenda or propaganda effort with respect to the Middle East, and her Twitter activity did not reveal any pro-Saudi sentiment. If anything, prior to 2018, her Twitter activity was *anti*-Saudi Arabia. Indeed, in November 2017, Defendant Collins tweeted out against Senator John McCain allegedly accepting donations from the Saudi regime:

---

<sup>6</sup> A “handle” is a unique username that begins with the @ symbol and which is used to identify users on Twitter.



40. However, like other named Defendants, in the summer of 2018, Defendant Collins’ activity on Twitter took a drastic turn. Specifically, Defendant Collins began relentlessly and consistently pushing *pro*-Saudi propaganda through her Twitter account.

41. Evincing a further change in Defendant Collins’ behavior, Defendant Collins engaged in significant interaction and coordination with the named Defendants via Twitter— individuals with whom she had no prior connection. The interactions between Defendant Collins and the other Defendants on Twitter were openly in furtherance of the collaboration and unification amongst the Defendants to follow a *pro*-Saudi propaganda campaign. Specifically, as of September 29, 2020, Defendant Collins has had 6,189 interactions with the Defendants via Twitter. Most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while consistently attacking dissidents of the Saudi and UAE regimes:

<b>User</b>	<b>Interactions with user by @305local</b>	<b>Date of First Identifiable Mention</b>
ScheyChris (Defendant Schey)	1775	2018-06-27 13:20:44
KateStewart22 (Defendant Al Qahtani)	1691	2018-07-07 23:23:51
Orchardcitygal & Smiity646 (Defendant Smith)	1609	2018-12-06 13:20:22
TarekLebanon1 (Defendant Zeinab)	635	2018-11-21 23:54:49
Turki_AlOwerde (Defendant Al-Owerde)	479	2019-02-14 17:27:05

42. As time progressed, so did Defendant Collins' sudden and seemingly inexplicable connection to Saudi Arabia. In or around December 2019, Defendant Collins visited Riyadh, Saudi Arabia. Specifically, on December 9, 2019, Defendant Collins tweeted a photograph of the skyline in Riyadh, along with the statement that the photograph depicted her "view from dinner last night." Defendant Collins further stated that "#Saudi has welcomed me with nothing but open arms."



43. Defendant Collins took this photograph from the Globe Lounge Restaurant, located in the five-star Al Faisaliah Hotel (located in Riyadh), where she stayed from December 7, 2019 to December 15, 2019.

44. On December 9, 2019, Defendant Collins stated publicly on Twitter that she attended a dinner at Defendant Al Otaibi's home in Saudi Arabia. In the December 9, 2019 post,

she took photographs of Defendant Al Otaibi's home, and thanked Defendant Al Otaibi and his family for hosting her.

45. Upon information and belief, Defendants MBS, Saudi 24 TV, Al Arabiya, Al Qahtani, Al-Asaker and the Recruiting Defendants<sup>7</sup> funded Defendant Collins' trip to Saudi Arabia in December 2019, as part of the Conspiracy against Plaintiff and the larger pro-Saudi propaganda campaign.

*Defendant Hussam Al-Jundi*

46. Defendant Hussam Al-Jundi is an American citizen who resides in Orlando, Florida. He operates a Twitter account with the handle @SamJundi to post pro-Saudi disinformation. Notwithstanding the fact that he is the Executive Vice President of a business in Saginaw, Michigan, and relocated to the U.S. in or around 1991, Defendant Al-Jundi changed his Twitter patterns entirely beginning in May 2018. He is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act.

47. From November 2011 to early 2018, Defendant Al-Jundi's tweets were primarily in English, with little mention of Saudi Arabia or the UAE. Defendant Al-Jundi participated in an interview with Mlive.com in or around September 11, 2001, in which he discussed his experiences as an Arab immigrant to the U.S. During the interview, Defendant Al-Jundi stated that he does not discuss Middle Eastern politics with his relatives because he is "focused on America" and sees himself "as an American more than anything."

48. However, like Defendant Collins (as well as the other American nodes discussed below), Defendant Al-Jundi's political views and Twitter activity changed drastically in the summer of 2018. Specifically, from May 4, 2018 to the present, Al-Jundi began tweeting almost

---

<sup>7</sup> As discussed below, the "Recruiting Defendants" are defined as Defendants Zeinab, Al Menaia, Al-Owerde, and Al Otaibi.

exclusively in a colloquial form of the Arabic language. His Twitter account is now—similar to that of Defendant Collins and the other American nodes—increasingly devoted to praising Saudi Arabia, again using the gateway to the larger Conspiracy to defame and destroy anti-regime critics.

49. Indeed, in his Twitter biography, Defendant Al-Jundi states that his “heart is Saudi.”

50. Like the other Defendants, Defendant Al-Jundi routinely engages in interactions with the other named Defendants via Twitter, indicating collaboration among the Defendants to promote Saudi Arabian interests and policies. Specifically, as of September 29, 2020, Defendant Al-Jundi has had 1,985 interactions with the named Defendants via Twitter. Most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while consistently attacking dissidents of the Saudi and UAE regimes:

<b>User</b>	<b>Interactions with user by @SamJundi</b>	<b>Date of First Identifiable Mention</b>
ScheyChris (Defendant Schey)	707	2018-11-11 21:57:14
TarekLebanon1 (Defendant Zeinab)	556	2018-11-22 17:55:42
Orchardcitygal & Smiity646 (Defendant Smith)	190	2018-12-07 16:09:05
KateStewart22 (Defendant Al Qahtani)	186	2018-12-05 1:24:43
Turki AIOwerde (Defendant Al-Owerde)	176	2019-02-21 13:03:55
305local (Defendant Collins)	158	2018-11-03 2:50:41
Al_menaia, almenaia & Faisal_Almenaia (Defendant Al Menaia)	12	2018-12-04 1:02:23

*Defendant Annette Smith*

51. Defendant Annette Smith is an American citizen who resides in Patterson, California and is a former Patterson City Council member. She operates a Twitter account with the handle @orchardcitygal, which was used to disseminate the leaked personal photographs of Ms. Oueiss on June 10, 2020, spread other disparaging messages aimed at Ms. Oueiss, and post

messages promoting pro-Saudi disinformation. She is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act.

52. From the time that Defendant Smith's Twitter account was created in or around 2009, until September 2018, Defendant Smith's account never once mentioned or otherwise referenced Saudi Arabia or Defendant MBS.

53. However, in October 2018, Defendant Smith's Twitter activity drastically changed. Despite her California residency, and an apparent lack of connection to the Saudi regime, the vast majority of Defendant Smith's Twitter activity revolves around posting pro-Saudi propaganda.

54. Moreover, Defendant Smith began consistently pushing a pro-Saudi narrative through her Twitter account, which has consistently been the gateway to the larger Conspiracy and efforts to abuse and defame those critical of the Saudi and UAE regimes:



55. As of September 29, 2020, Defendant Smith has had 4,251 interactions with the named Defendants via Twitter. Most, if not all, of these interactions relate to praising Saudi

Arabia, UAE, MBS, or other acolytes of MBS, while consistently attacking dissidents of the Saudi and UAE regimes:

User	Interactions with user by @orchardcitygal	Date of First Identifiable Mention
305local (Defendant Collins)	1521	2018-10-22 19:55:48
KateStewart22 (Defendant Al Qahtani)	1339	2018-10-29 15:31:04
ScheyChris (Defendant Schey)	796	2018-10-22 19:55:48
Turki_AlOwerde (Defendant Al-Owerde)	386	2019-02-14 17:12:12
TarekLebanon1 (Defendant Zeinab)	105	2018-11-24 4:30:56
SamJundi (Defendant Al-Jundi)	104	2019-02-04 2:33:11

Defendant Christanne Schey

56. Defendant Christanne Schey is an American citizen who resides in Houston, Texas, and is a former employee of broadband company Frontier Communications. She maintains a Twitter account with the @ScheyChris handle, posting pro-Saudi disinformation. Defendant Schey is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act.

57. From 2010 to 2013, Defendant Schey operated one Twitter account: @chris\_schey. Using this Twitter account, Defendant Schey posted approximately 100 tweets in three and a half years. During this timeframe, Defendant Schey never mentioned the Middle East.

58. In March 2016, Defendant Schey created her second Twitter handle, @ScheyChris. Like Defendants Collins and Smith, Defendant Schey's Twitter account was bereft of any mention of Middle Eastern politics until approximately 2018—the same year that Defendants Collins, Al-Jundi and Smith began to drastically shift their activity on Twitter towards pro-Saudi propaganda and policies. Using the Twitter handle @ScheyChris, Defendant Schey has tweeted over 240,000 times and has a Tweet frequency of approximately 340 tweets per day. Since April 2018,

Defendant Schey's Twitter account has been fervently pro-Saudi, while Schey routinely attacks perceived foes of the regime.

59. Like other Defendants, Defendant Schey routinely interacts and collaborates with the named Defendants via Twitter to promote pro-Saudi propaganda, again the gateway to the subsequent onslaught of social media assault and defamation against Saudi and UAE critics. Specifically, as of September 29, 2020, Defendant Schey has had 33,108 interactions with the members of the Network. Most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while consistently attacking dissidents of the Saudi and UAE regimes:

User	Interactions with user by @ScheyChris	Date of First Identifiable Mention
KateStewart22 (Defendant Al Qahtani)	10395	2018-06-30 13:48:34
Turki_AlOwerde (Defendant Al-Owerde)	9607	2019-02-14 16:26:59
Orchardcitygal & Smiity646 (Defendant Smith)	5448	2018-12-08 1:43:41
305local (Defendant Collins)	5279	2018-06-27 18:09:10
SamJundi (Defendant Al-Jundi)	1894	2018-08-28 13:39:32
TarekLebanon1 (Defendant Zeinab)	326	2018-11-22 1:18:27
Al_menaia, almenaia & Faisal_Almenaia (Defendant Al Menaia)	159	2018-06-13 2:15:41

#### ***Other Americans in the Network***

60. While not named Defendants in this lawsuit, several other members of the Network are U.S. citizens who were, upon information and belief, recruited by the Recruiting Defendants to join the Network to promote pro-Saudi disinformation and attack the Saudi regime's perceived enemies. These individuals include Shay Marie Evans (@shayevasatchel), Sarah Whalen (@SarahWhalen7), and South Florida resident Pamela Steinhauser (@Spencer\_Diana24).

61. These other American Nodes had no apparent connection to Saudi Arabia, any of the Network members, or the Middle East for that matter, until the summer of 2018. Then, like the other members of the Network discussed above, these American citizens began promoting pro-Saudi disinformation on Twitter and heavily interacting with the foreign and American nodes in the Network.

62. The acts of each Defendant named above contributed, in part, to the Conspiracy to harm Plaintiff personally and professionally for her critical reporting of the Saudi and UAE regimes, and Defendant MBS's involvement in the murder of Mr. Khashoggi and others.

***The Leaders of the Conspiracy***

*Defendant MBS*

63. Defendant Mohammed bin Salman bin Abdulaziz Al Saud is the current Crown Prince of the Kingdom of Saudi Arabia. MBS resides in Riyadh, Saudi Arabia, and has effectively been in a position of power since he pushed aside all rivals in 2017 through a brutal crackdown on family members and business leaders. Defendant MBS is not the head of state for the Saudi regime, nor is Defendant MBS the head of the Saudi regime's government. The current head of state for the Saudi regime (as well as the current Prime Minister of Saudi Arabia) is King Salman bin Abdulaziz Al Saud—Defendant MBS's father.

64. Defendant MBS is known for his brute authoritarian governing, his extrajudicial murder of Mr. Khashoggi, and his use of violence to extinguish free speech, contrary views, and dissidence, inside and outside of his kingdom. Defendant MBS has been the driver for the bombing of Yemen in which war-induced famine has resulted in the starvation of 13 million civilians. Defendant MBS coordinates, directs, and supervises the Saudi regime's actions in silencing its critics and brutally attacking its enemies.

65. The CIA has concluded that Defendant MBS ordered the assassination of Mr. Jamal Khashoggi.<sup>8</sup>

66. Defendant MBS is also behind the orchestration of several hacking operations against perceived enemies, including prominent American citizens<sup>9</sup> and others, as set forth in the Complaint, as well as other attempted murders.<sup>10</sup>

67. As discussed in detail in this Complaint, Defendant MBS (along with assistance from his agents) has built a network of dozens of individuals—including real-life American citizens—who together have tweeted more than 1.1 million times, reaching over 435,000 Twitter accounts, attacking perceived enemies stateside and abroad, including Plaintiff.

Defendant MBZ

68. Defendant Mohammed bin Zayed Al Nahyan (“Defendant MBZ”) is the current Crown Prince of the UAE and Deputy Supreme Commander of its Armed Forces. Defendant MBZ resides in Abu Dhabi. In 2019, the *New York Times* named Defendant MBZ the most powerful Arab ruler. However, Defendant MBZ is neither the head of state for the UAE, nor is he the head of the UAE’s government. The current President and head of state for the UAE is Sheikh Khalifa bin Zayed, who was named as the President by the UAE Federal Council in November 2004.

69. Defendant MBZ supported Defendant MBS prior to Defendant MBS’s rise to power in June 2017. According to numerous sources, Defendant MBZ has served as a mentor to,

---

<sup>8</sup> See <https://abcnews.go.com/Politics/blindingly-obvious-saudi-crown-prince-ordered-khashoggi-murder/story?id=59305430> (noting that a State Department official stated it was “blindingly obvious” based on the CIA’s assessment that Defendant MBS orchestrated the murder of Mr. Jamal Khashoggi).

<sup>9</sup> See <https://www.theverge.com/2020/1/21/21075968/amazon-jeff-bezos-hacked-saudi-arabia-crown-prince-whatsapp-message> (noting that Defendant MBS “targeted and successfully hacked” Jeff Bezos’ mobile device through a WhatsApp message).

<sup>10</sup> See <https://www.cnn.com/2020/08/06/politics/saudi-assassination-plot-allegations/index.html> (noting that a lawsuit has been filed against Defendant MBS in the District of Columbia for Defendant MBS’s role in hiring a group of hitmen known as the “Tiger Squad” to assassinate a former top aide of the Saudi regime).

and has influenced the decision making of, Defendant MBS. Defendant MBZ has also been the mastermind behind policies that both he and Defendant MBS have jointly aligned with, specifically on issues of foreign policy.<sup>11</sup>

70. Under Defendant MBZ's influence, the UAE has matured its offensive cyber effects operations capabilities and its intelligence services through the Signals Intelligence Agency, which is the UAE's equivalent of the CIA. The Signals Intelligence Agency and Defendant DarkMatter are headquartered in the same building in Abu Dhabi.<sup>12</sup>

*Defendant DarkMatter*

71. Defendant DarkMatter is an Emirati cybersecurity company founded in or around 2014 or 2015. DarkMatter supports the UAE's cybersecurity development, controls the sophisticated hacking group known as "Project Raven," and partners with the Signals Intelligence Agency to conduct offensive cyber effects operations against targets of the UAE regime. For example, DarkMatter, through Project Raven, was responsible for the targeted hacking of the chairman of *Al Jazeera* in June 2017 in the immediate aftermath of the onset of the blockade of Qatar, led by Saudi Arabia and the UAE.

*Defendant al Bannai*

72. Defendant al Bannai is a citizen of the United Arab Emirates and currently the Secretary General of the Advanced Technology Research Council (ATRC) and the CEO and Managing Director of EDGE GROUP, a state-owned defense conglomerate that include more than two dozen defense subsidiaries. Al Bannai is likewise a founder of DarkMatter and maintained an

---

<sup>11</sup> See, e.g., <https://www.middleeasteye.net/opinion/will-mbs-bring-end-saudi-dynasty>

<sup>12</sup> See <https://theintercept.com/2019/06/12/darkmatter-uae-hack-intercept/>

ownership interest in DarkMatter during the period when DarkMatter hacked Plaintiff's mobile device.

*Defendant Al Qahtani*

73. Defendant Saud Al Qahtani is a Saudi Arabian citizen and former royal court advisor to Defendant MBS. Prior to his dismissal in 2018, he was Defendant MBS's media consultant, as General Supervisor of the Center for Studies and Media Affairs. His role in supervising Mr. Khashoggi's murder is well known, as the U.S. Department of Treasury has specifically noted that he was "part of the planning and execution of the operation that led to the killing of Mr. Khashoggi."<sup>13</sup> Defendant Al Qahtani has admitted working for and conspiring with Defendant MBS on Twitter: "Do you think I'm acting on my own whim? I am a civil servant and a faithful executioner of the orders of the King and the Crown Prince."<sup>14</sup> Defendant MBS enlisted Defendant Al Qahtani to act on his behalf, and Defendant Al Qahtani has publicly accepted his role as an agent acting on behalf of Defendant MBS. As a "civil servant and faithful executioner" of Defendant MBS, Defendant Al Qahtani was (and continues to be) knowingly controlled by Defendant MBS.

74. Defendant Al Qahtani is no stranger to the creation of bot networks to push Saudi disinformation while attacking political opponents, or the use of unlawful hacking efforts and techniques to attack the Saudi regime's political opponents and critics.

75. Investigative journalists have noted Defendant Al Qahtani's supervisory role in "social media and surveillance operations for the Royal Court," and have noted that he was

---

<sup>13</sup> See <https://home.treasury.gov/news/press-releases/sm547>

<sup>14</sup> See <https://www.pbs.org/wgbh/frontline/film/the-crown-prince-of-saudi-arabia/transcript/>

nicknamed “Lord of the Flies” for his extensive use of bots (which have also been referred to as “flies”) in trying to control the narrative on Twitter.<sup>15</sup>

76. Defendant Al Qahtani has made statements on various hacking platforms, including popular hacking site *Hack Forums*, implicating himself in the Saudi regime’s intrusion and spying methods. Indeed, on the site *Hack Forums*, he has tried to hire hackers to manage his botnet campaigns for \$500 per month, has purchased 525 accounts on YouTube in furtherance of a social media influence operation, and has hired hundreds of individuals in Saudi Arabia to staff his troll farms on Twitter.<sup>16</sup>

77. As recently as June 2019, Defendant Al Qahtani was linked to an attempted hack of *The Guardian*, which reported that it was targeted by a Saudi hacking team at the order of Defendant Al Qahtani. Indeed, on June 19, 2019, *The Guardian* published an article describing how a source from inside the Saudi regime provided them with a “confidential internal order” from within the Saudi government. This confidential order, signed by Defendant Al Qahtani,<sup>17</sup> instructed a tech-savvy team of hackers to carry out the “penetration” of *The Guardian’s* computer servers “in complete secrecy.”<sup>18</sup>

78. It is no surprise then that Twitter suspended Defendant Al Qahtani’s Twitter account last year. *The Wall Street Journal* described Defendant Al Qahtani as “an architect of a Saudi government crackdown on dissidents in recent years that included the murder of journalist Jamal Khashoggi in Istanbul in 2018[.]” *The Wall Street Journal* also reported that, despite Defendant Al Qahtani being formally stripped of his title after it was revealed that he was involved

---

<sup>15</sup> See [https://www.bellingcat.com/app/uploads/2019/06/Lord-of-the-Flies\\_Redacted\\_6-25-19.pdf](https://www.bellingcat.com/app/uploads/2019/06/Lord-of-the-Flies_Redacted_6-25-19.pdf)

<sup>16</sup> See *id.*

<sup>17</sup> See *id.*

<sup>18</sup> See <https://www.theguardian.com/world/2019/jun/19/guardian-told-it-was-target-of-saudi-hacking-unit-after-khashoggi-killing>

in the murder of Jamal Khashoggi, he has “continued to play an important role in the kingdom as an informal advisor to [Defendant MBS].”<sup>19</sup>

79. Consistent with his role as a trusted advisor to Defendant MBS, Defendant Al Qahtani spearheaded the Conspiracy against Ms. Oueiss. That is, not only did he lead the creation and subsequent management of large botnets on Twitter to continuously ridicule Ms. Oueiss, but through his position as a board member of the MiSK Foundation, he also led the recruitment and establishment of the Network which was organized at the behest of Defendant MBS—with the objectives of promoting Saudi disinformation and attacking critics of the Saudi regime, such as Ms. Oueiss. Additionally, aside from organizing the creation of the Network, Defendant Al Qahtani also led one of the (successful) campaigns to unlawfully hack Ms. Oueiss’ mobile device, and then subsequently disseminate the private photographs of Ms. Oueiss via Twitter.

80. Defendant Al Qahtani created and manages one of the masked Twitter accounts at issue in this lawsuit: The Twitter handle @KateStewart22. With tweets in English and Arabic, @KateStewart22, upon information and belief, is a masked Twitter Account created and operated by at least two individuals: Defendant Al Qahtani and an unidentified person based in England. It is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act. It has verified its identity with Twitter and discovery will reveal the true identity of the user(s) of this account, along with Defendant Al Qahtani’s instrumental role in creating and managing the account and its secondary user(s).

*Defendant Al-Asaker*

81. Defendant Bader Al-Asaker is a Saudi Arabian citizen who serves as the head of the Private Office for Defendant MBS with the rank of Minister since he was appointed by a royal

---

<sup>19</sup> See <https://www.wsj.com/articles/twitter-suspends-former-saudi-official-linked-to-crackdown-khashoggi-killing-11568999068>

decree in July 2017. He has also served as “Secretary General” of Defendant MiSK Foundation as recently as May 20, 2020.

82. Similar to Defendant Al Qahtani, Defendant Al-Asaker is no stranger to using unlawful techniques to promote pro-Saudi disinformation while simultaneously attacking critics of the Saudi regime. In November 2019, the U.S. Department of Justice charged two former Twitter employees with spying for Saudi Arabia.<sup>20</sup> Specifically, two former Twitter employees had allegedly been paid by the Saudi regime to unlawfully access the personal information of more than 6,000 Twitter accounts in 2015.<sup>21</sup> The two former Twitter employees charged with spying at the behest of the Saudi regime reported directly to Defendant Al-Asaker.<sup>22</sup>

83. Defendant Bader Al-Asaker, acting in his capacity as Secretary General of Defendant MiSK Foundation and as agent of Defendant MBS, has had an integral role in cultivating the network of foreign and domestic citizens to carry out the Conspiracy against Ms. Oueiss. In his role as Secretary General for the MiSK Foundation, Al-Asaker has traveled to the U.S. on numerous occasions since 2014, including but not limited to, March, April and September of 2018—the time period during which the American Nodes were being recruited to join this Conspiracy against Ms. Oueiss.

84. Upon information and belief, Defendant Al-Asaker, acting at the behest, and under the control, of Defendant MBS and in his official capacity as CEO of Defendant MiSK, led the (successful) campaign (with Defendant Al Qahtani) to unlawfully hack Ms. Oueiss’ mobile device, and then subsequently disseminate the private photographs of Ms. Oueiss via Twitter. Defendant

---

<sup>20</sup> See <https://thehill.com/policy/international/middle-east-north-africa/469332-former-twitter-employees-charged-with-spying>

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

Al-Asaker's conduct in furthering the Conspiracy against Ms. Oueiss was not performed in his official capacity as a public minister or agent of the Saudi regime.

Defendant Al Arabiya

85. Defendant Al Arabiya is a broadcast and internet news network with offices in Saudi Arabia and the U.S., with broadcast and internet posts circulating in the U.S. and across the world. Al Arabiya operates a studio in Washington, D.C. with reporters assigned to the White House press pool. Al Arabiya is owned and controlled by Defendant MBS and functions as a mere instrumentality of Defendant MBS. Al Arabiya is an instrumentality of Defendant MBS and is dominated and controlled by Defendant MBS such that there is no independent existence between Al Arabiya and Defendant MBS. Al Arabiya, at the behest of Defendant MBS, posted false and doctored payment documents from *Al Jazeera*, intending to defame and disparage Ms. Oueiss.

86. Al Arabiya regularly broadcasts state propaganda and is currently the subject of a defamation lawsuit in the District of Columbia filed by Mr. Khaled Saffuri—a friend of the late Mr. Khashoggi.<sup>23</sup>

Defendant Saudi 24 TV

87. Defendant Saudi 24 TV is a broadcast and internet news network with offices in Saudi Arabia and the U.S., with broadcast and internet posts circulating in the U.S. and across the world. Saudi 24 TV operates a studio in Washington, D.C., with reporters assigned to the White House press pool. Saudi 24 TV is owned by the Saudi Ministry of Communications, which in turn, is a mere instrumentality of, and is dominated and controlled by, Defendant MBS.

88. Upon information and belief, Defendant Zeinab, discussed below, in his capacity as a Saudi 24 TV employee, and at the instruction of Defendant MBS and other high-ranking

---

<sup>23</sup> See *Khaled Saffuri v. Al Arabiya, et al.*, No. 1:19-cv-03005-EGS, ECF No. 1 (D.D.C. Oct. 7, 2019).

officers of Saudi 24 TV who are dominated and controlled by Defendant MBS, recruited various American citizens (including the named Defendants in this Complaint) to join a propaganda campaign intended to promote Saudi Arabian interests and attack the Saudi regime's critics, including Ms. Oueiss.

*Defendant MiSK Foundation*

89. Defendant Prince Mohammed Bin Salman bin Abdulaziz Foundation, also known as the MiSK Foundation ("MiSK"), was founded by Defendant MBS in his personal capacity and holds itself out as a non-profit foundation.

90. Until as recently as May 2020, Defendant Al-Asaker was the Secretary-General of Defendant MiSK. Previously, Defendant Al Qahtani was a board member of Defendant MiSK. Upon information and belief, MiSK serves as a front for Defendants MBS, Al Qahtani, and Al-Asaker's objectives in creating a network of foreign and domestic agents willing to carry out unlawful discrete operations here in the U.S., including the Conspiracy against Ms. Oueiss.

91. MiSK has significant contacts with the U.S. It regularly transacts business and hosts events throughout the country.<sup>24</sup>

*Defendant SACM*

92. Defendant Saudi Arabian Cultural Mission ("SACM") is a Virginia-based entity that holds itself out as an agency created by the Saudi government to "meet the educational and cultural needs of Saudis studying in the United States." However, upon information and belief,

---

<sup>24</sup> See, e.g., [https://www.yahoo.com/news/saudi-prince-mohammed-bin-salman-064827849.html?guccounter=1&guce\\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce\\_referrer\\_sig=AQAAANbktYtzMFDs\\_0VXE8bGOVBfaobEq1KEBYhXCaDvoVR9a73CZV2HqEMmmryDVqrSjoRv8C3oqdJNX-Vnoq15a6kuMjEau7hFxIP0X3t3URFxfj8iFY86UHscbleNEJMHdNSBsRQevWcTFb3cSMCqDzyh8YTB4GyldYH OeHXRfrsb](https://www.yahoo.com/news/saudi-prince-mohammed-bin-salman-064827849.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANbktYtzMFDs_0VXE8bGOVBfaobEq1KEBYhXCaDvoVR9a73CZV2HqEMmmryDVqrSjoRv8C3oqdJNX-Vnoq15a6kuMjEau7hFxIP0X3t3URFxfj8iFY86UHscbleNEJMHdNSBsRQevWcTFb3cSMCqDzyh8YTB4GyldYH OeHXRfrsb) (noting that Defendant MBS hosted an event for MiSK in California in 2018); see also <https://www.pri.org/stories/2019-09-25/saudi-youth-forum-new-york-public-library-cancelled-after-activists-outcry> (noting that MiSK held an event in New York City in 2019).

Defendant SACM is under the control and domination of Defendants MBS, Al Qahtani and Al-Asaker who have used SACM as a front to recruit and establish a network of individuals who will carry out unlawful discrete operations, including the Conspiracy against Ms. Oueiss. Defendant Al Menaia, a member of the Conspiracy, founded the SACM Chapter for Western Oregon University. Defendant SACM is a mere instrumentality of Defendant MBS.

93. The Saudi regime closely monitors students when they leave Saudi Arabia to study in the U.S. and utilizes SACM to achieve that objective. For example, a student (speaking on the basis of anonymity due to fear of reprisal from the Saudi regime) that attended an unnamed Midwestern college stated that, at a school event in 2017, they and another person were present for the explicit purpose to record their findings and report back to the Saudi embassy what they had experienced at the event.<sup>25</sup>

94. Upon information and belief, Defendant SACM's representatives and objectives directly overlap with those of Defendant MiSK, and the Saudi regime. Indeed, as noted above, two former employees of Twitter, originally from Saudi Arabia, were groomed by Defendant Al-Asaker through MiSK to become operatives of the Saudi regime and use their positions on the inside of Twitter to unlawfully spy on Saudi dissidents.<sup>26</sup> Defendant MiSK relies on the student outreach capabilities of SACM to engage individuals to undertake its initiatives, such as the MiSK Future Path Career Essentials program.<sup>27</sup>

---

<sup>25</sup> See <https://www.pbs.org/newshour/world/saudi-students-in-u-s-say-their-government-watches-their-every-move>

<sup>26</sup> See <https://www.nytimes.com/2019/11/06/technology/twitter-saudi-arabia-spies.html>

<sup>27</sup> See <https://misk.org.sa/hcd/services/misk-future-path/>

***The Foreign Nodes (“Recruiting Defendants”)***

***Defendant Zeinab***

95. Defendant Tarek Abou Zeinab is a Lebanese radio and TV broadcaster who works out of Lebanon for Defendant Saudi 24 TV, a television broadcast channel owned by the Saudi Arabian government, and which is an instrumentality of, and is controlled and dominated by Defendant MBS. He operates the Twitter handle @tareklebanon1, which was created in April 2011. With approximately 24,600 Twitter followers, he primarily tweets in English and works in concert with his co-conspirators to create pro-Saudi propaganda and engage U.S. citizens to populate the content on their accounts. He is not registered with the Department of Justice pursuant to the Foreign Agents Registration Act.

96. Defendant Zeinab is a well-connected Lebanese political operative who has traditionally focused on, and been involved with, Lebanese-based political interests and organizations. However, beginning in 2017, Defendant Zeinab shifted his political activities in a more explicit pro-Saudi direction.

97. Upon information and belief, Defendant Zeinab began his employment with Defendant Saudi 24 TV in 2018. He has since used his Twitter accounts to personally attack and defame Ms. Oueiss in response to Ms. Oueiss’ criticism of the Saudi regime:



98. On November 25, 2018, Defendant Zeinab expressly acknowledged the establishment of a media initiative aimed at amplifying pro-Saudi and pro-Defendant MBS content, involving direct attacks on the coverage of the Saudi regime and Defendant MBS by media outlets including *Al Jazeera*, CNN, and *The Washington Post*—all in the wake of the murder of Mr. Khashoggi. As noted above, the Network of Twitter users is comprised of real-life foreign and domestic citizens.

99. Furthermore, on December 30, 2018, shortly after Defendant Zeinab expressly acknowledged the development of the Network, Defendant Zeinab, remarkably, acknowledged creating the Network in coordination with the conspiratorial objectives set forth by Defendant Al Qahtani:

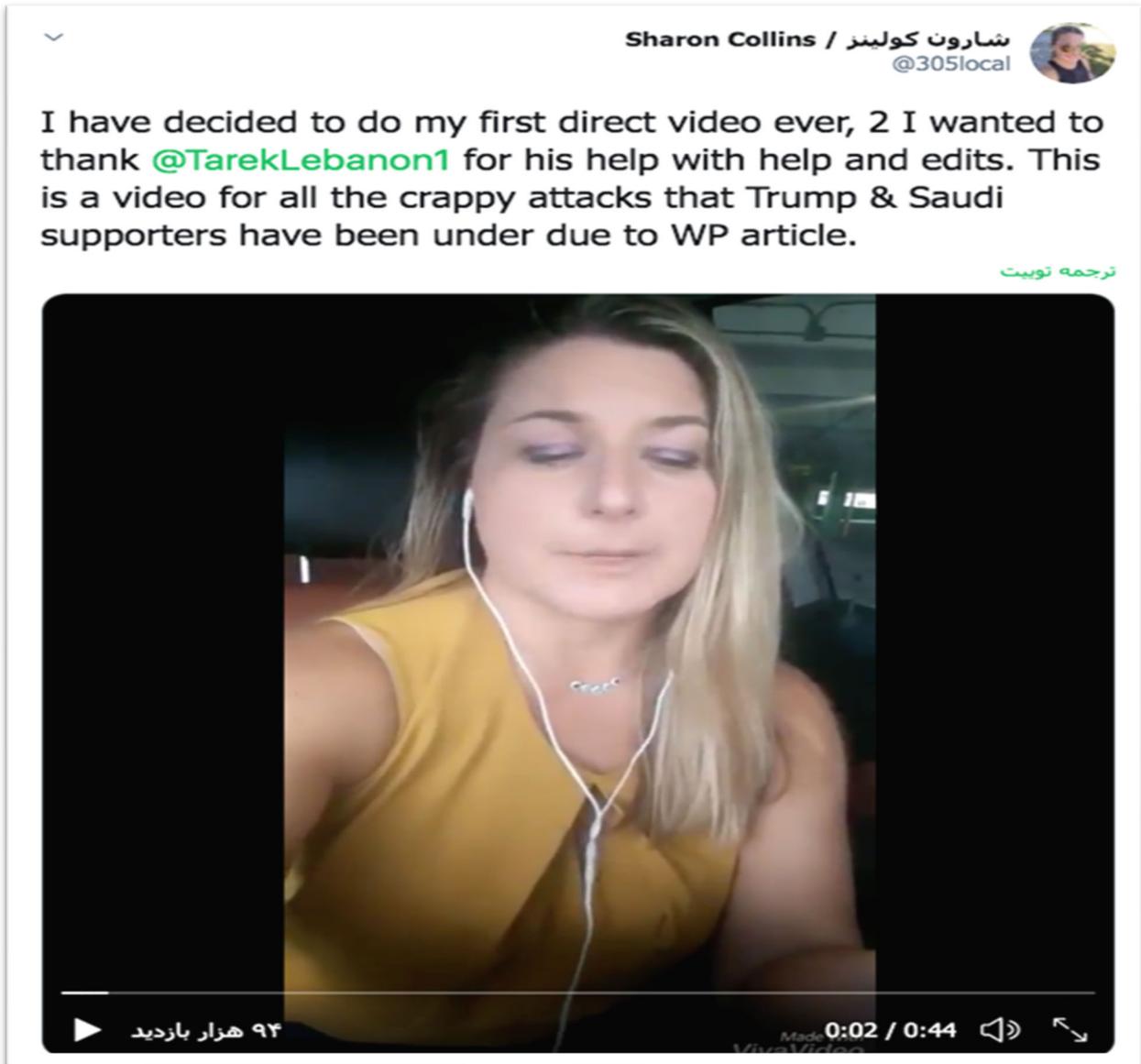


100. This brazen admission is significant evidence of Defendant Zeinab’s relationship and coordination with the named-Defendants in this Complaint via Twitter. As an agent of Defendant Saudi 24 TV (the alter ego of Defendant MBS), Defendant Zeinab instructed, influenced, and otherwise directed the American Nodes to post pro-Saudi disinformation, and to attack Defendant MBS’s perceived enemies, including Ms. Oueiss.

101. For example, as of September 29, 2020, Defendant Zeinab has had at least 2,438 interactions via Twitter with Defendants. It is noteworthy that most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while the remainder of the interactions involve attacks on Saudi and UAE critics:

<b>User</b>	<b>Interactions with user by @Tareklebanon1</b>	<b>Date of First Identifiable Mention</b>
305local (Defendant Collins)	944	2018-10-22 15:20:13
SamJundi (Defendant Al-Jundi)	745	2018-08-27 9:07:46
ScheyChris (Defendant Schey)	390	2018-10-13 19:45:31
KateStewart22 (Defendant Al Qahtani)	273	2018-11-17 2:27:36
Orchardcitygal & Smiity646 (Defendant Smith)	86	2018-12-06 13:18:15

102. Indeed, Defendant Zeinab has (publicly and privately) instructed numerous members in the Network to post pro-Saudi propaganda videos. He also assists members of the Network, such as Defendant Collins, in editing such videos:



103. Defendant Zeinab knowingly acted at the direction of, and under the control, of Defendants MBS, Al Qahtani, Al-Asaker, as well as high-ranking officers of Defendant Saudi 24 TV, in recruiting American (as well as foreign) citizens into the Network.

Defendant Al Menaia

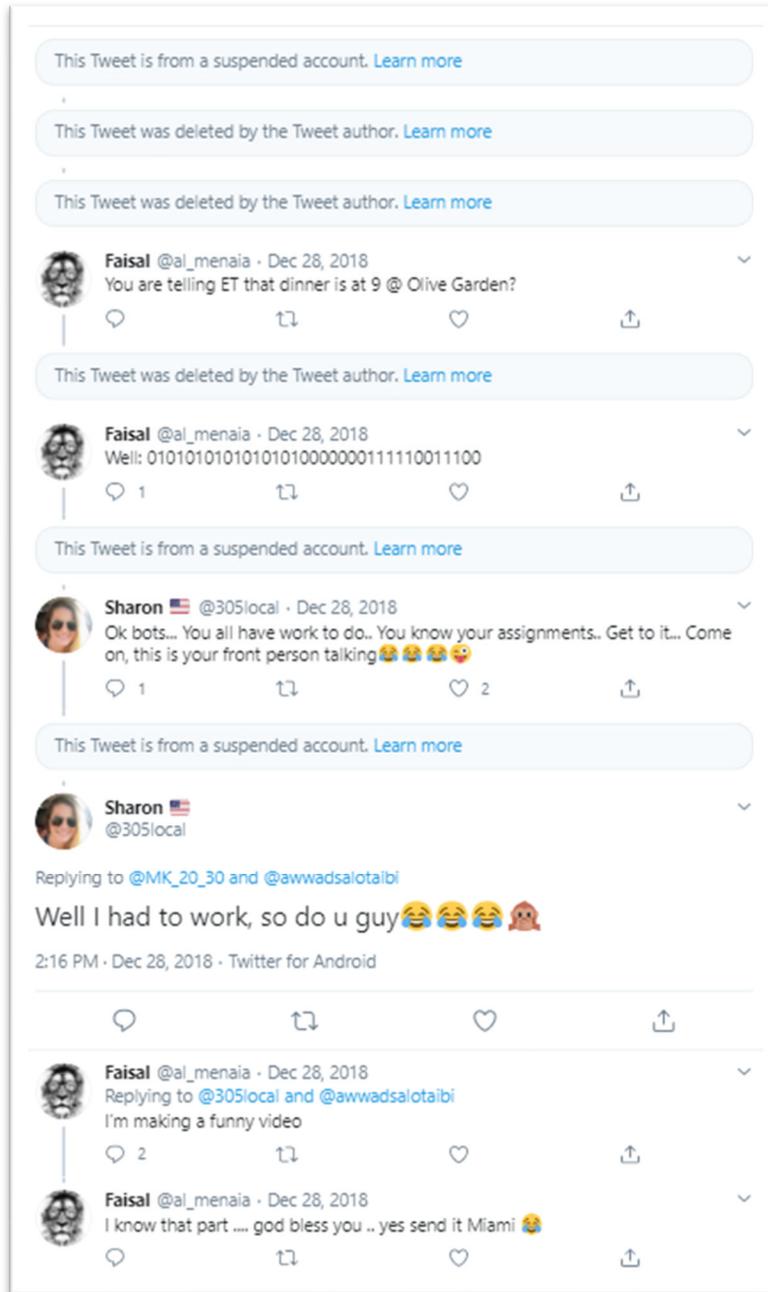
104. Defendant Faisal Al Menaia is a Saudi citizen who studied in the U.S. and the United Kingdom and previously worked for Defendant SACM while in the U.S. Defendant Al Menaia is also the founder of the SACM Chapter for Western Oregon University. In concert with

Defendant Zeinab (and their larger conspiracy to promote pro-Saudi disinformation, while attacking critics of the Saudi regime), Defendant Al Menaia has instructed several of the U.S.-based Defendants named in this Complaint to spread disinformation about other countries in a video on Twitter and also assisted in the production of videos posted on Twitter by the same U.S.-based Defendants named in this Complaint.

105. As of September 29, 2020, Defendant Al Menaia has had 1,174 interactions with the Defendants via Twitter. It is noteworthy that most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while the remainder of the interactions involve attacks on Saudi and UAE critics:

<b>User</b>	<b>Interactions with user by @Al Menaia</b>	<b>Date of First Identifiable Mention</b>
305local (Defendant Collins)	346	2018-11-25 20:08:26
TarekLebanon1 (Defendant Zeinab)	253	2018-11-25 19:45:50
ScheyChris (Defendant Schey)	208	2018-06-13 2:14:35
KateStewart22 (Defendant Al Qahtani)	205	2018-11-25 10:56:41
Turki_AlOwerde (Defendant Al-Owerde)	101	2019-02-15 15:17:09
SamJundi (Defendant Al-Jundi)	61	2018-11-26 23:55:06

106. Tweets between Defendant Al Menaia and Defendant Collins in December 2018 indicate that various members of the Network, including Defendants Al Menaia and Collins, have planned to meet for dinner at stateside restaurants, such as the Olive Garden:



107. Defendant Al Menaia has also targeted defamatory tweets at, and harassed, Ms. Oueiss, mentioning Ms. Oueiss' Twitter account in 11 tweets between October 8, 2018 and, most recently, January 25, 2020. In a January 25, 2020 tweet mentioning Ms. Oueiss, Defendant Al Menaia (@al\_menaia) referred to Ms. Oueiss as a "dog" and threatened that "we will surround

you” in response to Ms. Oueiss’ coverage of Defendant MBS’s orchestration of the hack of Jeff Bezos’ mobile device.

108. Defendant Al Menaia would never have made such a threat to Ms. Oueiss without MBS and other co-conspirators’ approval, tacit or otherwise. MBS has never denounced this co-conspirator’s brazen threat and recognition of Saudi involvement in the killing of Mr. Khashoggi. Essentially, these circumstances are effective admissions on MBS’s part.

*Defendant Al-Owerde*

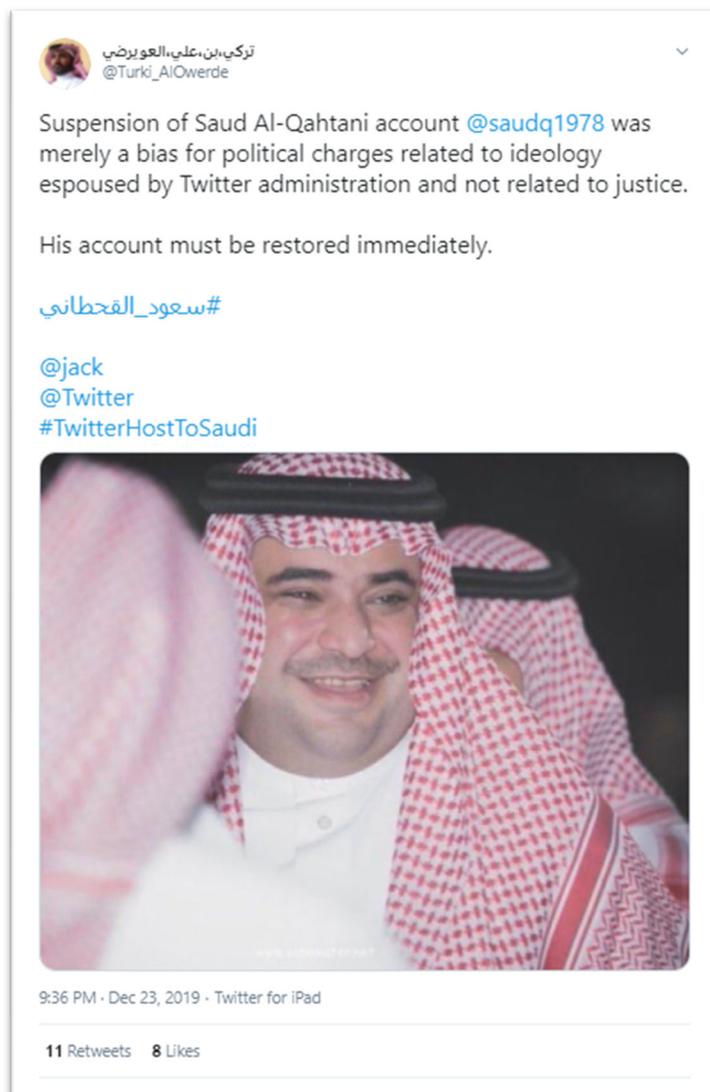
109. Defendant Turki Al-Owerde is a Saudi national and Editor-in-Chief of *The Herald Report*—a news agency based in the UAE. Defendant Al-Owerde uses his platform, including as a contributor to *The Milli Chronicle*, to spread pro-Saudi disinformation and has influenced the shifts in content posted on social media by the U.S.-based Defendants in this Complaint.

110. Defendant Al-Owerde maintains a leadership role in the Network. He engaged the U.S.-based Defendants throughout the fall of 2018, indoctrinating them by challenging their religious beliefs and influencing them over time.

111. As of September 29, 2020, Defendant Al-Owerde has had 11,602 combined interactions with the Defendants on Twitter. It is noteworthy that most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while the remainder of the interactions involve attacks on Saudi and UAE critics:

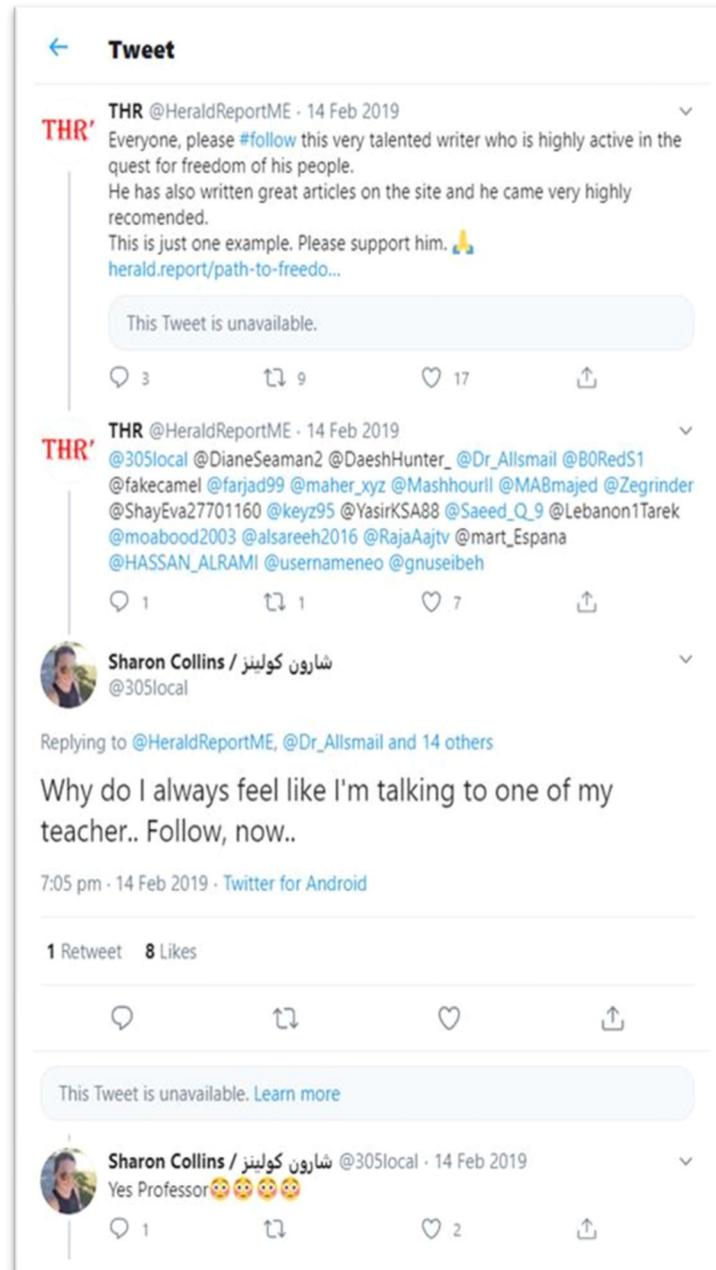
<b>User</b>	<b>Mentions of @Turki AlOwerde</b>
ScheyChris (Defendant Schey)	9607
KateStewart22 (Defendant Al Qahtani)	838
305local (Defendant Collins)	479
Orchardcitygal (Defendant Smith)	386
SamJundi (Defendant Al-Jundi)	176
Al Menaia (Defendant Al Menaia)	101
TarekLebanon1 (Defendant Zeinab)	15

112. Defendant Al-Owerde is loyal to Defendant Al Qahtani. For example, on December 23, 2019, Defendant Al-Owerde publicly appealed Twitter’s suspension of Defendant Al Qahtani’s Twitter account, calling Twitter’s actions “merely a bias for political charges related to ideology espoused by Twitter administration and not related to justice.” He called for Defendant Al Qahtani’s account to “be restored immediately.”



113. Defendant Al-Owerde has taken part in directing members of the Network to promote pro-Saudi propaganda and to defame Ms. Oueiss. Additionally, *The Herald Report's*

Twitter account which, upon information and belief, is operated by Defendant Al-Owerde, has instructed members of the Network, including Defendant Collins, to follow certain Twitter users:



114. Defendant Al-Owerde also engages in defamatory activity toward Ms. Oueiss. On October 12, 2018, he mocked Ms. Oueiss on Twitter in response to her reporting of Saudi involvement in the killing of Mr. Khashoggi. Defendant Al-Owerde further insulted Ms. Oueiss

on June 9, 2020 after the release of the hacked and stolen photographs of Ms. Oueiss, referring to Ms. Oueiss as a “clown” and referring to Ms. Oueiss’ employer as a “platform of terrorism.”

Defendant Al Otaibi

115. Defendant Awwad Al Otaibi is a Saudi Arabian citizen and works in the Information Technology and Security field. A 2017 Idaho State University College of Business graduate in the U.S., he was recruited by Defendants MBS and Al-Asaker through the MiSK Foundation to take part in leading the cultivation of the Network and, ultimately, the Conspiracy against Ms. Oueiss.

116. Since graduating from college in 2017, Defendant Al Otaibi has spent time in both the U.S. and Saudi Arabia. He has been present in the U.S. on numerous occasions, including but not limited to, from December 2017 through February 2018.

117. On June 2, 2018, Defendant Al Otaibi received a certification from Defendant MiSK for completing an “Interview Skills Program with Distinction.” Upon information and belief, Defendant MBS used the MiSK Foundation as a front to develop and coordinate relationships with networks of agents willing to carry out discrete and unlawful operations.



118. Since receiving his certificate from MiSK, Defendant Al Otaibi has maintained a leadership role in the Network. He regularly interacts with members of the Network, including the U.S.-based Defendants. Although he deactivated and then reactivated his Twitter account in June 2020, historical tweets by members of the Network show a close connection between him and the named Defendants. Specifically, as of September 29, 2020, he has had at least 4,495 interactions with members of the Network via Twitter. It is noteworthy that most, if not all, of these interactions relate to praising Saudi Arabia, UAE, MBS, or other acolytes of MBS, while the remainder of the interactions involve attacks on Saudi and UAE critics:

<b>User</b>	<b>Mentions of @awwadsalotaibi</b>
ScheyChris (Defendant Schey)	1832
KateStewart22 (Defendant Al Qahtani)	1063
305local (Defendant Collins)	728
Orchardcitygal (Defendant Smith)	486
TarekLebanon1 (Defendant Zeinab)	179
Al_Menaia (Defendant Al Menaia)	127
Tarek1975leb (Defendant Zeinab)	73
SamJundi (Defendant Al-Jundi)	7

119. Defendant Al Otaibi has hosted members of the Network at his home in Saudi Arabia. Indeed, on December 9, 2019, Defendant Collins—a Florida resident, with no apparent connections to Saudi Arabia prior to the creation of the Network—attended Al Otaibi’s home and posted a photograph of their dinner on Twitter:



120. Furthermore, Defendant Al Otaibi has had multiple instances of direct interaction with Prince Sattam bin Khalid bin Nasser Al Saud, indicating that Defendant Al Otaibi is a close ally of the Saudi regime and royal family.

John Doe Defendants

121. John Does 1-20 are entities or individuals who, upon information and belief, are otherwise subject to the jurisdiction of this Court. The specific identities of the various Does are unknown to Plaintiff at this time, but Plaintiff is informed and believes, and thereon alleges, that each of the Does is responsible in some manner for the occurrences alleged in this Complaint, including hacking Plaintiff's mobile device and anonymously posting false statements on various

social media platforms and websites to harm Plaintiff, and that the Defendants each were the agents, alter egos, and employees of each other, acting within the course and scope of said agency and employment of each of the other defendants, participated with, conspired with and aided and abetted each of the other defendants, and in doing the things herein alleged, were acting within the scope of such partnership, agency, representation or employment with the knowledge, authorization, consent and ratification of the other defendants. Plaintiff will seek leave to amend this Complaint to insert the true names and capacities of each Doe when the same are ascertained.

## **I. JURISDICTION AND VENUE**

### **A. Subject Matter Jurisdiction**

122. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1331 because this case arises under the Alien Tort Statute ("ATS"), 28 U.S.C. § 1350, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Stored Communications Act, 18 U.S.C. §§ 2701-12. This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

123. Exercising subject matter jurisdiction over Plaintiff's ATS claim is consistent with the requirements and policies underlying the ATS. Specifically, Plaintiff's claim under the ATS is predicated on conduct that touches and concerns the U.S. As demonstrated throughout this Complaint, Defendants MBS, MBZ, Al Qahtani, and Al-Asaker spearheaded a conspiracy involving considerable conduct in the U.S. This conduct includes recruiting U.S. citizens to spread stolen and doctored photographs of Plaintiff with the goal of defaming and destroying Plaintiff's credibility and intimidating Plaintiff from reporting on Saudi Arabia's and UAE's human rights abuses in efforts to maintain and polish these regimes' public image in the U.S.

124. As detailed herein, Defendants MBS and MBZ, working in concert with Defendant DarkMatter and other Defendants, expressly targeted Plaintiff in various locations, including the

U.S., to hack Plaintiff's personal information contained in her personal mobile device using spyware known as Pegasus for the express purpose of violating her privacy and manipulating that information to cause Plaintiff harm. Defendants MBS and MBZ further recruited American nodes, residing in the U.S., to join them in the Conspiracy to disseminate pro-Saudi disinformation and the stolen photographs of Plaintiff in the United States and elsewhere.

**B. In Personam Jurisdiction**

125. Exercising personal jurisdiction over Defendants MBS, MBZ, DarkMatter, al Bannai, Al Arabiya, Saudi 24 TV, Al Qahtani, Al-Asaker, MiSK, Zeinab, Al-Owerde, and Al Otaibi is proper in this case, consistent with Fed. R. Civ. P. 4(k)(2)(B), the U.S. Constitution and laws. As discussed throughout this Complaint, Defendants MBS, MBZ, Al Arabiya, Saudi 24 TV, Al Qahtani, Bader Al-Asaker, DarkMatter, al Bannai, MiSK, Al-Owerde, and Al Otaibi engaged in intentional tortious conduct which was directed at and occurred in the U.S.

126. Specifically, Defendant DarkMatter, under the direction of Defendants MBS, MBZ, and with assistance from Defendants al Bannai, Al Qahtani and Bader Al-Asaker, among others, hacked Plaintiff's mobile device and unlawfully extracted personal and confidential photographs and content from Plaintiff's mobile device. These Defendants then instructed the U.S. Defendants, among others, to disseminate this stolen content, with the intent of disparaging and intimidating Plaintiff—an internationally renowned journalist—in an attempt to dissuade Plaintiff from reporting on Saudi Arabia's and the UAE's human rights abuses.

127. Defendants MBS, Al Qahtani, and Al-Asaker through their roles at MiSK and SACM recruited several of the named U.S. Defendants in this Complaint, with the goal of establishing a network of U.S. citizens who would improve Saudi Arabia's public image, while simultaneously working in a cohesive fashion to destroy, disparage and defame any critic of the Saudi regime, with the hopes of improving MBS's and his regime's public image and relationship

with the U.S. government. Indeed, since Defendant MBS’s involvement in the murder of Mr. Khashoggi was made public, Defendant MBS has spent billions of dollars in “efforts to whitewash [Saudi Arabia’s] dismal [human] rights record.”<sup>28</sup>

128. This conduct carried out by Defendant MBS—including the establishment of a network of U.S. citizens to disseminate stolen information from Plaintiff’s mobile device—was in violation of the law of nations and treaties of the U.S. Specifically, the Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, which the U.S. ratified in 2006, addresses cybercrime (such as the hacking of Plaintiff’s mobile device) with the goal of harmonizing national laws and increasing cooperation amongst various nations to prevent the ever-increasing acts of offensive cyber effects operations. The Convention on Cybercrime’s main objective is “to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.”<sup>29</sup>

129. The Convention on Cybercrime has been signed or ratified by at least 65 countries, including the U.S.<sup>30</sup> MBS and MBZ’s actions in using DarkMatter to hack Plaintiff’s mobile device with the goal of obtaining Plaintiff’s confidential information to intimidate her from reporting on Saudi and UAE’s human rights abuses violates universally agreed upon legal principles. Specifically, Defendants MBS and MBZ’s actions of directing the hacking of Plaintiff’s mobile device and obtaining personal and confidential information regarding Plaintiff was in violation of several provisions and objectives of the Convention on Cybercrime.<sup>31</sup>

---

<sup>28</sup> See <https://www.hrw.org/news/2020/10/02/saudi-arabia-image-laundering-conceals-abuses>

<sup>29</sup> See <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

<sup>30</sup> See <https://www.coe.int/en/web/cybercrime/parties-observers>

<sup>31</sup> See <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ccc5b>

130. This Court also has personal jurisdiction over all Defendants pursuant to Florida's long-arm statute, Fla. Stat. Ann. § 48.193 (West 2016), because Defendants, either personally, through an agent, and as a result of their participation in the Conspiracy described herein, committed a tortious act within this state and entered into the Conspiracy to commit tortious acts while present in this state. Specifically, Defendants Collins and Al-Jundi, while present in Florida, acted at the behest of Defendants MBS, Al Qahtani and Bader Al-Asaker (among others) in posting stolen photographs of, and defamatory narratives about, Plaintiff on Twitter.

131. This Court also has personal jurisdiction over Defendants Collins and Al-Jundi because both Defendants reside in Florida.

**C. Venue**

132. Venue in this judicial district is proper pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this county. Confidential information stolen from Plaintiff's personal mobile device was accessed and otherwise distributed via social media by at least one Defendant who resides in this district. Additionally, the Conspiracy at issue in this Complaint was entered into in this district.

133. Venue in this district is also proper pursuant to 28 U.S.C. § 1391(b)(3) because there is no judicial district in a State in which all non-foreign defendants are residents, and Defendants Collins and Al-Jundi are subject to personal jurisdiction in Florida.

**D. Alter Ego Allegations**

134. As noted above, Defendants Al Arabiya, Saudi 24 TV, MiSK, and SACM are dominated and controlled by Defendant MBS and are mere instrumentalities of MBS.

135. Al Arabiya is a propaganda arm of the Saudi government and, more specifically, Defendant MBS. While Al Arabiya is listed as a wholly-owned subsidiary of Dubai-based Middle East News, FZ-LLC, Defendant MBS extorted a majority share of ownership in Al Arabiya

(approximately 60%) from Al Arabiya's former majority owner, Waleed Al Ibrahim (the founder of the Middle East Broadcasting Center).<sup>32</sup> As a result, Defendant Al Arabiya is a mere instrumentality of, and is dominated and controlled by, Defendant MBS.

136. As a result of Defendant MBS's majority ownership in Al Arabiya, Al Arabiya has been rated as a "questionable" news source "due to excessive government censorship that results in the publication of pro-state propaganda."<sup>33</sup>

137. Saudi 24 TV is also a propaganda arm of the Saudi government and Defendant MBS. Saudi 24 TV is part of Riyadh-based 24 Media Group. According to 24 Media Group, its partners include the Saudi Ministry of Media, General Entertainment Authority, Ministry of Education and the Interior Ministry. Upon information and belief, Defendant MBS directs and controls the commercial activities and employees of Defendant Saudi 24 TV, which is a mere instrumentality of, and is dominated and controlled by, Defendant MBS.

138. A U.S.-based program created by the Saudi Arabian government in 1951, SACM is a "part of the Saudi Embassy in Washington, D.C.," and is "responsible to the Saudi Arabian Ministry of Higher Education."<sup>34</sup> Thus, similar to Defendant Saudi 24 TV, SACM has close ties to and involvement with the Saudi Ministry of Education.<sup>35</sup> Upon information and belief, the

---

<sup>32</sup> See <https://mediabiasfactcheck.com/al-arabiya/>

<sup>33</sup> See *id.*

<sup>34</sup> See

[https://www.sacm.org/AboutSACM/History.aspx?\\_cf\\_chl\\_jschl\\_tk\\_=446d9946bffa6fe9344c515f77605d659d71b5e9-1602529859-0-AQXdXbPvAwJdEYpG-PnhCy4YvEiwhYFrL3crBni2xxbaHjmf5tUeT6R7x7VORPNalcjd\\_TA2dfAFSjsmtZaQ5IDG4y2PiJU3Ake0k7fMSAVZmndb7moK9r-OpiDvrXWnwPNEpmFfPTnNr46dLCJGVDgXcm7dUiaAmlbfQucb75go2kBisTuBiHd2I1vPg1Oi4Ladf84uNLyQRBxr8ufwi-F4C8DICrOmc\\_Y5kiM2amBuz6cwY6NXuuT367eoot4K6GZUI6Wvdmb2RFsEuekQj5IU1glTH7hONzWoYGoV5iGP](https://www.sacm.org/AboutSACM/History.aspx?_cf_chl_jschl_tk_=446d9946bffa6fe9344c515f77605d659d71b5e9-1602529859-0-AQXdXbPvAwJdEYpG-PnhCy4YvEiwhYFrL3crBni2xxbaHjmf5tUeT6R7x7VORPNalcjd_TA2dfAFSjsmtZaQ5IDG4y2PiJU3Ake0k7fMSAVZmndb7moK9r-OpiDvrXWnwPNEpmFfPTnNr46dLCJGVDgXcm7dUiaAmlbfQucb75go2kBisTuBiHd2I1vPg1Oi4Ladf84uNLyQRBxr8ufwi-F4C8DICrOmc_Y5kiM2amBuz6cwY6NXuuT367eoot4K6GZUI6Wvdmb2RFsEuekQj5IU1glTH7hONzWoYGoV5iGP)

<sup>35</sup> See <https://sacm.org.au/saudi-arabia-merges-higher-education-education-ministries-and-appoints-dr-azzam-al-dakhil-minister-of-education/> (discussing merger of Higher Education and Education Ministries by the Saudi regime).

operations of both SACM and MiSK are ultimately controlled and dominated by, and are the mere instrumentalities of, Defendant MBS.

139. Upon information and belief, Defendant MBS utilizes SACM and MiSK to carry out secretive operations here in the U.S., under the guise of providing educational initiatives and opportunities to Saudi Arabian citizens. In reality, Defendant MBS has, through his agents (*e.g.*, Defendants Al Qahtani and Al-Asaker) used SACM and MiSK to recruit various members of the Network described above, all with the intention of promoting pro-Saudi disinformation and attacking the regime's critics, such as Ms. Oueiss.

140. Accordingly, Al Arabiya, Saudi 24 TV, SACM, and MiSK are the mere instrumentalities of MBS. MBS dominates and controls these four entities and their operations and has used each entity to engage in improper and unlawful conduct described in this Complaint, which has proximately caused Plaintiff's harm.

141. Defendant MBS has never denounced the actions of these alter-ego co-conspirators in their campaign against Ms. Oueiss for her coverage of Mr. Khashoggi's murder. Essentially, these circumstances are effective admissions on MBS's part.

### **FACTUAL BACKGROUND**

#### **I. SAUDI ARABIA'S AND THE UAE'S *MODUS OPERANDI* IN HACKING AND CONDUCTING OFFENSIVE CYBER EFFECTS OPERATIONS AGAINST ITS PERCEIVED ENEMIES**

142. Since Defendant MBS's rise to power, the Saudi regime has substantially increased the exercise of its sphere of influence in the region to undertake various methods of offensive cyber effects operations against its critics. Indeed, Defendant Al Qahtani, at the behest of Defendant MBS, has consistently used "bot" accounts on Twitter to conduct massive cyber-attacks on Saudi and UAE critics.

143. One of the most well-known use of bot accounts to disparage and defame a critic of the Saudi and UAE regimes is the ongoing campaign against Ms. Oueiss. Indeed, Defendants MBS and MBZ have been identified as utilizing “bot” accounts to launch misogynistic campaigns against Ms. Oueiss. From late 2018 through 2020, Defendants MBS and MBZ have launched an online campaign against Ms. Oueiss and another female anchor, in which tens of thousands of tweets intended to smear Ms. Oueiss were published by Saudi-based and UAE-based bot accounts.<sup>36</sup>

144. Not only were thousands of “bot” accounts involved in this campaign against the two female anchors, but various verified accounts of the Saudi and UAE regimes were also identified as participating in the misogynistic campaign.<sup>37</sup>

145. As it relates to Mr. Khashoggi, Twitter had its hands full in trying to suspend various Saudi-based bot accounts in connection with the media coverage surrounding Mr. Khashoggi’s death. As noted above, Twitter was also infiltrated by two individuals (now former employees of Twitter), alleged to be spies for the Saudi Arabian government (who reported to Defendant Al-Asaker) who were caught “snooping into thousands of private accounts seeking personal information about critics of the Riyadh government[.]”<sup>38</sup>

146. Apparently seeking more effective means to disparage and intimidate critics of their regimes—such as Ms. Oueiss—Defendants MBS and MBZ have sought out more advanced hacking tools to carry out surveillance against their dissidents.

---

<sup>36</sup> See, e.g., <https://english.alaraby.co.uk/english/news/2020/6/11/al-jazeera-journalists-targeted-in-misogynistic-saudi-linked-smear-campaign>; see also <https://www.dw.com/en/middle-east-female-journalists-resist-targeted-online-abuse/a-54224906>

<sup>37</sup> See <https://english.alaraby.co.uk/english/news/2020/6/11/al-jazeera-journalists-targeted-in-misogynistic-saudi-linked-smear-campaign>

<sup>38</sup> See <https://www.npr.org/2019/11/06/777098293/2-former-twitter-employees-charged-with-spying-for-saudi-arabia>

147. Due to its previously limited offensive cyber effects operations capabilities, Defendant MBS, with Defendant Al Qahtani's coordination, procured advanced hacking tools from Israeli cyber firm NSO Group Technologies Limited ("NSO Group") and Italian cyber firm, Hacking Team. Specifically, in 2018, the Saudi regime acquired NSO Group's Pegasus spyware, and utilized this spyware to access over 400 WhatsApp messages between Mr. Khashoggi and another Saudi individual to track Mr. Khashoggi in the weeks leading up to his assassination.<sup>39</sup>

148. Mr. Khashoggi is not the only victim of the Saudi regime's use of Pegasus spyware. Indeed, in May 2018, at the direction of Defendant MBS, Saudi hacking teams used NSO Group hacking tools to hack the mobile device of Amazon founder, Jeff Bezos. Similar to the hacking of Mr. Khashoggi's friend's mobile device, Defendant MBS infected Mr. Bezos's phone with the spyware through WhatsApp messaging.<sup>40</sup>

149. In a complaint filed in October 2019, Facebook alleged that NSO Group used WhatsApp servers and vulnerabilities to spread the Pegasus spyware to 1,400 mobile devices in an attempt to target journalists, human rights activists, and others.<sup>41</sup> As discussed below, suspicious WhatsApp messages were identified on Ms. Oueiss' personal mobile device around the time her device was hacked.

150. The UAE, at the direction of Defendant MBZ, has also leveraged its mature offensive cyber effects operations capabilities against dissidents, its own citizens, and in support

---

<sup>39</sup> See <https://english.alaraby.co.uk/english/indepth/2019/10/3/this-israeli-spyware-helped-saudi-arabia-spy-on-khashoggi> (noting that the Citizen Lab confirmed that a Saudi individual's text messages with Mr. Khashoggi were hacked by the military-grade spyware, Pegasus, and that it was "deployed at the request of the Saudi government.").

<sup>40</sup> See <https://www.theverge.com/2020/1/21/21075968/amazon-jeff-bezos-hacked-saudi-arabia-crown-prince-whatsapp-message> (noting that Defendant MBS "targeted and successfully hacked" Jeff Bezos' mobile device through a WhatsApp message).

<sup>41</sup> *WhatsApp Inc. v. NSO Group Technologies Limited, et al.*, No. 4:19-cv-07123-PJH (N.D. Cal.)

of joint Saudi and UAE interests, such as diminishing the influence of *Al Jazeera* and its employees.

151. For example, on June 19, 2017, 14 days after Saudi Arabia, the UAE, Bahrain, and Egypt severed diplomatic ties with Qatar, the mobile devices of Faisal Al-Qassam (an *Al Jazeera* host) and Hamad bin Thamer Al Thani (chairman of *Al Jazeera*) were hacked and media contents from the devices were obtained. These hacks, and the hacks of other journalists around that time, have been attributed to an advanced hacking group known as Project Raven (also known as Stealth Falcon), which has close ties to Saudi Arabia, the UAE, and Defendant DarkMatter.<sup>42</sup>

152. Project Raven was originally contracted by a Baltimore-based cybersecurity firm CyberPoint International (“CyberPoint”). CyberPoint was contracted by the UAE in 2012 to assist and advise the newly developed Signals Intelligence Agency.

153. CyberPoint hired former U.S. National Security Agency (NSA) employees to work in the UAE in support of the Signals Intelligence Agency under the name Project Raven. In 2016, control of Project Raven transferred from CyberPoint to a domestic Emirati company, Defendant DarkMatter, which also brought an unknown number of U.S. employees to the UAE to continue working on Project Raven. DarkMatter is headquartered in the same building in Abu Dhabi as the Signals Intelligence Agency and was founded by Al Arabiya. The Signals Intelligence Agency has served as Project Raven’s primary client by identifying groups and organizations to be targeted by Project Raven’s hacking teams. While the stated goal of Project Raven is to assist in the targeting and hacking of terror organizations, there is evidence that Project Raven has been (and continues to be) used to target dissidents and individuals that speak out against the UAE and its allies (e.g., Saudi Arabia).

---

<sup>42</sup> See <https://www.reuters.com/investigates/special-report/usa-raven-media/>

154. In 2016, Project Raven, under the control of Defendant DarkMatter, procured a spyware (hacking) tool called Karma. This spyware tool could be used to hack Apple iPhones remotely with little effort. Using Karma, and at the behest of the Signals Intelligence Agency, Project Raven reportedly hacked the iPhones of Sheikh Tamim bin Hamad Al Thani—the Emir of Qatar. Moreover, threat intelligence and research firms opined that Project Raven used Karma to target additional *Al Jazeera* employees and other journalists based in England, in the immediate aftermath of the blockade of Qatar in support of joint objectives with Saudi Arabia.

155. More recently, the UAE has ramped up its spying and hacking operations against dissidents. Individuals such as Tahnoun bin Zayed Al Nahyan (the son of the founder of the UAE and Defendant MBZ’s brother), Hamad Al-Shamsi (the Attorney General of the UAE), and Khaldoun Khalifa Al Mubarak (Chairman of Abu Dhabi’s Executive Affairs Authority) have been instrumental in these efforts.

156. Tahnoun has been the National Security Advisor for the UAE since February 2016. Tahnoun is linked to three companies behind the development and deployment of the messaging and Voice-over-IP (VoIP) application, *ToTok*, which has since been determined to have been used by the UAE government for domestic surveillance.<sup>43</sup> After it was revealed that the *ToTok* app was being used by Tahnoun to spy on dissidents of the UAE, Google and Apple immediately removed *ToTok* from their app stores.

157. The *ToTok* application is linked not only to Tahnoun, but also to Defendant DarkMatter. Specifically: Group 42 Holding Ltd (“Group 42”) was the creator the *ToTok* app. Al-Shamsi is the sole director of Group 42, which is a parent company of technology firm PAX

---

<sup>43</sup> See <https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html>

AI (previously known as Pegasus LLC). Pegasus LLC was formerly part of Defendant DarkMatter.<sup>44</sup>

158. *Totok's* primary developer is Group 42. Three of the UAE-based companies behind *ToTok's* creation and development, including Group 42, are all heavily influenced by Tahnoun.

159. For example, the current CEO of Group 42, Peng Xiao, is the former CEO of Pegasus LLC when it was a division of Defendant DarkMatter. Tahnoun and Peng Xiao's working relationship is widely known and ongoing. In fact, Tahnoun and Peng Xiao were in Abu Dhabi together as recently as October 27, 2020, where they were photographed together (middle left, and far left, respectively):



<sup>44</sup> See <https://medium.com/@billmarczak/how-tahnoon-bin-zayed-hid-totok-in-plain-sight-group-42-breej-4e6c06e93ba6>

160. Tahnoun has been active in procuring hacking tools for years. For example, Mauqah Technology – a company previously owned by Tahnoun – purchased spyware systems from Italian cyber firm Hacking Team, and was implicated in the 2012 hacking of human rights defendant and UAE dissident Ahmed Monsoor. Defendant Al Qahtani has also procured spyware systems from Hacking Team previously for similar operations in Saudi Arabia.

161. Project Raven and the use of NSO Group hacking infrastructure was also identified in the 2016 attempted hacking of Ahmed Monsoor, who is currently serving a prison sentence in the UAE related to his reporting on the regime, for which United Nations rights experts have urged his immediate release.<sup>45</sup>

162. Saudi Arabia has relied on the UAE as a close ally to conduct offensive cyber effects operations. Both Saudi Arabia and the UAE are well known for utilizing NSO Group's Pegasus spyware to engage in offensive cyber effects operations against their critics. The Israeli government (via NSO Group, the creator of Pegasus) sold the Pegasus spyware to the UAE in or around November 2019.<sup>46</sup>

163. The UAE uses its offensive cyber effects operations capabilities, which have been maturing for years, to target groups and individuals opposed jointly by the UAE and Saudi Arabia. While offensive cyber effects operations by Saudi groups have made it into mainstream headlines, particularly the use of NSO Group tools like Pegasus to spy on Jamal Khashoggi and Jeff Bezos, cyber operations by UAE groups, such as Project Raven, are more mature and have only come to light for mainstream audiences recently due to the involvement of American citizens with Project Raven through CyberPoint. As shown below, Defendants MBS and MBZ share a common disdain

---

<sup>45</sup> See <https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html>

<sup>46</sup> See <https://www.haaretz.com/middle-east-news/.premium-with-israel-s-encouragement-nso-sold-spyware-to-uae-and-other-gulf-states-1.9093465>

for dissidents of their regimes, including Ms. Oueiss. Upon information and belief, Defendants MBS and MBZ coordinated the hacking of Ms. Oueiss' personal mobile device and subsequently disseminated Ms. Oueiss' personal and confidential information to the public to defame, humiliate and harm Ms. Oueiss.

**II. DEFENDANTS' CONSPIRACY TO HACK MS. OUEISS' MOBILE DEVICE AND SUBSEQUENTLY DISSEMINATE PRIVATE AND FALSE INFORMATION REGARDING MS. OUEISS**

164. About a year after the Saudi regime set its sights on Ms. Oueiss, they orchestrated a calculated and multi-faceted attack against her. The overall Conspiracy against Ms. Oueiss was broken down into separate steps and cells, utilizing individuals from various nations, including the U.S. Defendants, in violation of the Foreign Agent Registration Act (among other laws).

165. The Conspiracy consists of the following three separate stages: (1) the recruiting stage of the Conspiracy and the establishment of the Network of foreign and American agents; (2) the hacking stage of the Conspiracy; and (3) the dissemination, amplification, and defamation stage of the Conspiracy. The recruiting stage has been discussed and demonstrated above, setting forth the cultivation, connection, and collaboration between each member of the Conspiracy. The remaining two stages are set forth below:

**A. Stage Two: The Hacking Stage**

**1. Defendants Carry Out the Hacking of Ms. Oueiss' Mobile Device**

166. With a Network of American citizens already in place to sway the narrative on social media, Defendants MBS, MBZ and Tahnoun, among others, hatched a plan to invade Ms. Oueiss' privacy, steal her personal and private information, and disseminate such personal information to the public with a false narrative. Defendants' plan was intended to defame, disparage and otherwise humiliate Ms. Oueiss.

167. Upon information and belief, as a key part of enhancing this effort, Defendant DarkMatter with Defendant al Bannai, consistent with prior hacking operations carried out at the behest of the UAE regime and Defendant MBZ, hacked into Ms. Oueiss' personal mobile device, an iPhone XS, with the goal of obtaining confidential information about Ms. Oueiss and other individuals whom the Saudi and UAE regimes perceived as critics.

168. Over the course of September 2019 through May 2020, DarkMatter (along with other state-sponsored, sophisticated threat actors, operating at Defendant MBS's and Defendant MBZ's behest) attempted to, and did in fact, gain unauthorized access to the contents of Ms. Oueiss' mobile device using multiple attack vectors. These attack vectors included exploiting vulnerabilities associated with WhatsApp, iMessage, Apple Mail, and Safari, establishing remote access through malicious executables delivered via WhatsApp, iMessage, or email, as well as accessing Ms. Oueiss' Apple account and attempting to use the iCloud backup functionality to access media and other content remotely.

169. Starting as early as on or about October 1, 2019, through as recently as May 28, 2020, multiple instances of suspicious iMessage messages, WhatsApp messages, and WhatsApp phone calls to Ms. Oueiss' mobile device from unknown numbers were identified. These events indicate a coordinated hacking attempt, as they correlate to suspicious activity or processes observed running on Ms. Oueiss' mobile device, which indicates that the suspicious messages were used to install malicious software on the device that could be used to access its contents remotely. During the first identified hacking events, which began on or about October 1, 2019, Ms. Oueiss was physically present in the U.S.

170. Upon information and belief, the manner in which contents on Ms. Oueiss' mobile device were accessed, together with the underlying data ingress and egress from her device and

then-existing vulnerabilities in WhatsApp's application, indicates that Defendants intentionally accessed WhatsApp's servers located around the world, and possibly servers located in California, to access confidential content stored on the mobile device. These servers, in part, provided Defendants with access to files physically and electronically stored on Ms. Oueiss' mobile device while such files were in electronic storage in such systems, as was done by foreign actors in a recent case involving the Pegasus spyware and access to WhatsApp servers. *See WhatsApp Inc. v. NSO Grp. Tech. Ltd.*, No. 19-cv-07123-PJH (N.D. Cal.).

a. April 14, 2020 – Ms. Oueiss Receives a Suspicious WhatsApp Message

171. On April 14, 2020 at 10:45:58 PM (AST), Ms. Oueiss' mobile device received a WhatsApp message from a Moroccan phone number that was unknown to Ms. Oueiss. The WhatsApp message was suspicious, as Ms. Oueiss: (1) did not have any previous interaction with the sender; (2) the WhatsApp message was deleted from Ms. Oueiss' mobile device in a method of deletion that does not match the method for typically deleted messages by the device owner or by the message sender (which is standard WhatsApp functionality); and (3) approximately two hours following receipt of the WhatsApp message, suspicious processes ran on Ms. Oueiss' mobile device and a system crash occurred, all within two hours of receipt of this message. Investigation found a reference to the WhatsApp message on the device's history. However, the WhatsApp message database, which typically includes entries for all messages (even those deleted by the user or sender), did not contain the entry. This means that the message had been deleted from the WhatsApp database, which would only be possible with privileged access to the WhatsApp database on the device.

b. April 15, 2020 – A Kernel Panic Occurs on Ms. Oueiss’ Mobile Device

172. As referenced previously, iOS crash logs from Ms. Oueiss’ mobile device further reveal that on April 15, 2020 at 01:06:07 AM (AST), a kernel panic<sup>47</sup> occurred on the device. The kernel panic was associated with a likely successful attempt at a local privilege escalation, which occurs when a bug or vulnerability is exploited to gain administrative privileges on a device or application. This privilege escalation would most likely have caused the device to crash.

173. Multiple iOS vulnerabilities existed on Ms. Oueiss’ mobile device during this time and could have been leveraged to gain access to the device and achieve persistent access. Multiple WhatsApp on iOS vulnerabilities, with Common Vulnerabilities and Exposures (“CVE”) severity scores rated “High” or “Critical,” existed on Ms. Oueiss’ mobile device during this time. There were four (4) vulnerabilities that were published in October 2020 related to WhatsApp that were not remediated until after the suspicious WhatsApp message to Ms. Oueiss on April 14, 2020.

174. Immediately prior to and during the kernel panic, a suspicious process (watchdogd) was running. The process, “watchdogd,” is associated with NSO Group’s Pegasus malware and is not associated with any legitimate processes within the iOS operating system. The process, “watchdogd,” may be the process that likely achieved successful privilege escalation on the device.

175. What’s more, an additional process (itunesstored) was identified as running on Ms. Oueiss’ device at this time. While the “itunesstored” process is a legitimate iOS process associated with the iTunes Store, it is also associated with NSO Group’s Pegasus tool and it was observed during the crash. The process, “itunesstored,” was observed immediately after the kernel panic

---

<sup>47</sup> A kernel panic is a safety measure taken by an operating system's kernel upon detecting an internal fatal error in which it either is unable to safely recover or cannot have the system continue to run without having a much higher risk of major data loss. In the absence of evidence of a legitimate process failing, a kernel panic can be an indicator of a vulnerability being exploited on the system.

event and immediately after the suspicious “watchdog” process and mimicked observations that were reported in threat intelligence reporting on previous NSO Group Pegasus attack chains, which suggest vulnerabilities in it are exploited to execute malicious code in order to gain access to the target device.<sup>48</sup>

c. April 17-20, 2020 – Unexplained Data Egress Occurs

176. Furthermore, on April 17, 2020, 43.32 MB of unexplained data egress occurred from Ms. Oueiss’ mobile device. This was two days before Defendants leaked the first group of stolen private photographs to social media, on April 19, 2020.

177. Additionally, between 12:56 AM (AST) and 06:59 PM (AST) on April 20, 2020, at least 5,207 individual files (images, videos, documents) were accessed on the file system of Ms. Oueiss’ mobile device. This quantity far exceeds the average daily file access count. Ms. Oueiss did not explore or access these files on April 20, 2020, which demonstrates that the files were cataloged by an actor with unauthorized remote access to the device in a continued search for potentially disparaging content that could be leaked to social media. 4,615 of the 5,207 files were accessed between 12:56:09 AM (AST) and 07:58:52 AM (AST). Ms. Oueiss did not access files during this time. Additionally, based on technical data available and confirmation by Ms. Oueiss, Ms. Oueiss was asleep between 03:00 AM (AST) and 07:00 AM (AST), during which time 2,423 files were accessed on the device.

d. Additional Information Obtained Through Investigatory Efforts

178. Furthermore, a malicious URL was identified from deleted content on Ms. Oueiss’ personal mobile device that could be used for command and control activity and to send commands and data back and forth to Ms. Oueiss’ mobile device. Suspicious phone calls and messages

---

<sup>48</sup> <https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf>

through WhatsApp were identified as possible delivery mechanisms of the malicious URL, which operated using Safari's Private Browsing mode. The WhatsApp messages and some targeted browsing history were subsequently wiped from Ms. Oueiss' mobile device in an attempt to eliminate evidence of the hacking activity. Significant data egress was observed by Ms. Oueiss' mobile device around the time of the suspicious WhatsApp phone calls and messages.

179. A network of ten (10) malicious web domains were identified on the mobile device. Malicious URLs found on Ms. Oueiss' mobile device are associated with this network of domains and subsequent research of these domains identified a series of malicious executables meant to target and compromise mobile devices. Indicators of compromise that have been tied to advanced cyber operations against human rights activists were identified as existing on Ms. Oueiss' mobile device.

180. While, at the time, Ms. Oueiss was unaware that her personal and confidential information had been stolen from her phone, the Defendants' Conspiracy was well underway and, indeed, was close to fruition.

## **2. The Content Stolen from Ms. Oueiss' Mobile Device**

181. There were at least two separate groups of personal photographs and videos stolen from Ms. Oueiss' mobile device.

182. The first group of photographs that were stolen from Ms. Oueiss' mobile device (and subsequently disseminated to the public, as discussed below) were personal photographs of Ms. Oueiss smoking a cigarette and drinking alcohol with her friends.

183. The second group of photographs that were disseminated to the public were screenshots of a private and personal video of Ms. Oueiss in a hot tub that her husband had recorded on Ms. Oueiss' mobile device. In addition to being leaked, these screenshots of the video were doctored to make it falsely appear as though Ms. Oueiss were naked at the time of the video,

and were disseminated by Defendants with the false and repugnant narrative that Ms. Oueiss was engaged in sexual acts at the time of the video in exchange for financial incentives.

184. While these are the only groups of photographs that have been leaked thus far, the amount of data accessed on Ms. Oueiss' mobile device indicates that there are additional private images, videos and documentation that were stolen but have not yet been leaked. Additionally, Ms. Oueiss has received numerous threats from anonymous actors that they intend to publish additional information obtained from her mobile device in the near future.

**B. Stage Three: The Dissemination, Amplification and Defamation Stage**

**1. On February 17, 2020, Defendants Released Doctored Financial Documents Related to Ms. Oueiss and Her Employer**

185. On February 17, 2020, Defendant Al Arabiya posted a supposed leaked document through its Twitter account, which purported to show financial rewards paid in bonuses to *Al Jazeera* journalists, including Ms. Oueiss (the "Doctored Financial Photo").

186. The Doctored Financial Photo posted by Defendant Al Arabiya was inauthentic and was intended to defame Ms. Oueiss and harm her reputation. Specifically, Al Arabiya posted the Doctored Financial Photo and stated on Twitter that the Doctored Financial Photo revealed "hundreds of thousands in bonuses" were paid by the Emir of Qatar to certain journalists at *Al Jazeera*, including Ms. Oueiss.

187. The dissemination and reposting of the Doctored Financial Photo by pro-Saudi news outlets and social media accounts led to a significant spike in negative Twitter activity aimed at Ms. Oueiss that would only be surpassed by the subsequent photograph leaks.

**2. On April 19, 2020, Defendants Released the Stolen Private Photographs of Ms. Oueiss Behind Masked Social Media Accounts**

188. As discussed above, Saudi Arabia and the UAE routinely create and manage fake "bot" accounts on social media as a means of engaging in cyber warfare with their enemies and

critics. As part of the Conspiracy, Defendants MBZ, MBS, and Al Qahtani, among others, used the same means of cyber warfare to begin disseminating the stolen photographs of Ms. Oueiss throughout the Internet.

189. Specifically, Defendants MBS and MBZ directed Defendants Al Qahtani and Al-Asaker, among others, to create and utilize multiple accounts across various social media platforms, including Twitter, with the pre-meditated purpose of spreading disinformation about Ms. Oueiss. One of the key social media accounts created for this purpose was a Twitter account: @Uncareer1.

190. The Twitter account @Uncareer1 was created on or about February 4, 2020 and began tweeting on February 17, 2020 by replying to tweets Ms. Oueiss posted responding to the Doctored Financial Photo posted by Defendant Al Arabiya and other pro-Saudi news outlets.

191. The Arabic name associated with @Uncareer1 (خفايا المهنة) translates to “secrets of the profession” or “tricks of the trade.” The Twitter account @Uncareer1, and subsequently created related social media accounts, was created for the purpose of disseminating and spreading leaked and doctored content that disparaged key figures associated with *Al Jazeera*, including Ms. Oueiss.

192. Indeed, on April 18, 2020, a related account, @Uncareer20, was created on the social messaging app Telegram and posted links to prior tweets by the @Uncareer1 Twitter account. On April 19, 2020, both the @Uncareer1 Twitter account and then the @Uncareer20 Telegram accounts posted private photographs of Ms. Oueiss drinking alcohol and smoking with friends in a new effort to damage her public image (the “Smoking Photos”). As noted above, these images were part of the content that was stolen from Ms. Oueiss’ mobile device as a result of the Defendants’ hacking efforts.

193. After the dissemination of the Smoking Photos by @Uncareer1 on April 19, 2020, several prominent Saudi journalists identified the @Uncareer1 account on Twitter and encouraged Twitter users to follow @Uncareer1 to “learn stories of mercenaryism,” “prostitution wars”, and “obscenity.” One of these accounts is operated by Saudi journalist @hassanalsolami, which displays a link to the Saudi Ministry of Media on its account.

194. The user of @Uncareer1 created various social media accounts across numerous platforms using different naming conventions, all with the goal of utilizing the accounts to defame and otherwise injure Ms. Oueiss. This conduct was carried out at the behest of Defendants MBS and MBZ, with assistance from Defendants Al Qahtani and Al-Asaker.

**3. On June 2, 2020, Defendants Release Additional Stolen Photographs of Ms. Oueiss Behind Masked Social Media Accounts**

195. Once the Uncareer accounts had matured further in their following and reach—approximately eight months after Defendants had first attempted to hack Ms. Oueiss’ mobile device—in alignment with strategy set by Defendants MBS and MBZ, the Uncareer entity published the further disparaging photographs of Ms. Oueiss.

196. On June 2, 2020, @Uncareer20 (via Telegram) and @Uncareer1 (via Twitter) posted the contents of a stolen video from Ms. Oueiss’ mobile device, which Defendants had broken down into various screenshots (the “Personal and Private Photos”), for the world to see.

197. Over the next few days, pro-Saudi Twitter accounts continued to repost and amplify the content until it reached a critical mass of thousands of negative tweets directed at Ms. Oueiss on June 9, 2020.

198. Following Twitter’s suspension of the @Uncareer1 account in June 2020, the related telegram account (@Uncareer20) claimed to have established a further replacement account with the handle @almhna1. This newly formed Twitter account has claimed to be the

origin of the leaked photographs of Ms. Oueiss and further claims that it has “only leaked 1% of what it has.” The biography of this Twitter account states “we return to renew the pain.”

199. Further Twitter accounts have been created and promoted by the @Uncareer20 Telegram account and all purport to be managed by the same Uncareer entity: @Surr\_1; @Absenttruth1; and @LeakSkip. More recently, on September 15, 2020, @LeakSkip posted a tweet indicating that “storms and currents” would further damage or destroy *Al Jazeera* employees, such as Ms. Oueiss.

4. **Defendants Utilize the Network to Continuously Amplify and Disseminate the Stolen Photographs of Ms. Oueiss to the Public, Along with a False Narrative Surrounding the Photographs**

200. As discussed above, Defendant MBS had a Network of foreign and domestic agents prepared to disseminate defamatory information about Ms. Oueiss at a moment’s notice. Aside from their failures to register as foreign agents with the U.S. government pursuant to FARA registration requirements, Defendants committed far graver violations of U.S. law when they utilized this cohesive Network to carry out their Conspiracy against Ms. Oueiss.

201. Once the @Uncareer accounts had first posted the stolen photographs of Ms. Oueiss, the Recruiting Defendants (*i.e.*, Zeinab, Al Menaia, Al-Owerde, and Al Otaibi) instructed the Network to spread the stolen content as a way to defame, injure and humiliate Ms. Oueiss.

202. Despite their knowledge that this content was stolen from Ms. Oueiss’ mobile device, and despite their knowledge that the narrative surrounding the Personal and Private Photos was false, various members of the Network agreed—at the behest of the Recruiting Defendants—to disseminate the stolen photographs of Ms. Oueiss on Twitter with the intent to disparage and defame Ms. Oueiss.

a. Defendant Collins' Attacks on Ms. Oueiss in Furtherance of the Conspiracy

203. Defendant Collins has mentioned Ms. Oueiss in 12 tweets between August 30, 2019 and June 11, 2020, which have been retweeted 493 times in total, including by co-conspirators in Florida and elsewhere.

204. Defendant Collins took part in defaming and otherwise launching personal attacks on Ms. Oueiss. For instance, on June 7, 2020, in response to Ms. Oueiss' tweet about the stolen Personal and Private Photos, Defendant Collins responded and said that Ms. Oueiss was "in the position [she] is in" as a result of her own behavior—a similar (false) accusation hurled at Ms. Oueiss by Defendant Smith.

205. On June 9, 2020, Defendant Collins retweeted the Personal and Private Photos of Ms. Oueiss. Relatedly, on that same day, Defendant Collins posted another tweet regarding Ms. Oueiss, in which Defendant Collins claimed that Ms. Oueiss "sold [her]self to terrorists to get a story."

206. That same day, Defendant Collins responded to a tweet by Ms. Oueiss which displayed a picture of deceased journalist Mr. Khashoggi, along with numerous other journalists who were either killed, detained or missing at the hands of the Saudi regime—a picture in solidarity with the freedom of press and journalism. Defendant Collins responded to Ms. Oueiss' tweet and accused her of working for "Qatar who ended up hiding the Master Mind behind 9/11 when America was demanding for Justice."

207. Defendant Collins has launched other defamatory attacks at Ms. Oueiss, including one instance where she claimed that Ms. Oueiss' late father was involved in the Southern Lebanese Army and was responsible for killing various people. Notably, Defendants Collins and Smith were

both mentioned in the original tweet regarding Ms. Oueiss, indicating further collaboration between the Defendants to defame and disparage Ms. Oueiss:



208. Defendant Collins was instructed by the Recruiting Defendants, operating under the directed strategy of Defendant MBS, to personally attack Ms. Oueiss on Twitter.

209. Defendant Collins agreed to take part in this defamatory attack on Ms. Oueiss—and did in fact take part in the attack by publishing the stolen Personal and Private Photos of Ms. Oueiss—all while Defendant Collins was present in Florida.

210. Defendant Collins' tweets regarding Ms. Oueiss were defamatory, and were intended to embarrass, harass, and otherwise injure Ms. Oueiss by spreading disinformation regarding Ms. Oueiss.

211. Defendant Collins engaged in acts in furtherance of the Conspiracy (*i.e.*, posting defamatory tweets regarding Ms. Oueiss) while she was physically present in Florida. At least 161 of Defendant Collins' Twitter followers self-report their location as Florida. Accordingly, Defendant Collins' defamatory tweets regarding Ms. Oueiss were published and accessed in Florida.

212. Defendant Collins' defamatory tweets regarding Ms. Oueiss were directed, in part, at audiences and followers within the vicinity of her primary location, including Miami, Florida, and elsewhere. Defendant Collins' Twitter handle—@305local—is further evidence that Defendant Collins was recruited to the Network, in part, to disseminate harmful information about critics of the Saudi regime (*e.g.*, Ms. Oueiss) in Florida and to a Florida-based audience. Upon information and belief, Defendants MBS, Al Qahtani, Al-Asaker and the Recruiting Defendants intended to recruit members to the Network who were from major U.S. cities, such as Miami, Florida, to disseminate disinformation in major U.S. markets and cities.

b. Defendant Al-Jundi's Attacks on Ms. Oueiss in Furtherance of the Conspiracy

213. Defendant Al-Jundi has mentioned Ms. Oueiss in at least 39 original tweets, which have been retweeted at least 646 times in total. He has also retweeted three posts mentioning Ms. Oueiss.

214. Defendant Al-Jundi often attacks Ms. Oueiss in response to her opinions about Saudi Arabia's human rights abuses. For example, on June 16, 2019, Ms. Oueiss expressed concerns about the Saudi regime's human rights abuses via Twitter. On June 23, 2019, Defendant Al-Jundi responded to Ms. Oueiss' tweet with considerable praise for Saudi Arabia, in which Defendant Al-Jundi stated that Saudi Arabia has "god to take justice, as this is the destiny of the greats in history," and that "rights and victories are taken away through disputes and force, and not as free gifts like how this mercenary [Oueiss]."

215. On June 9, 2020, Defendant Al-Jundi retweeted an image of a fabricated tweet—purporting to be a tweet from Ms. Oueiss' verified Twitter account—in which Ms. Oueiss accused her colleague at *Al Jazeera* for being responsible for the Conspiracy against Ms. Oueiss. This tweet, however, was fabricated. Ms. Oueiss never tweeted this, and the image of the tweet was fabricated at the behest of Defendant MBS. Defendant Al-Jundi retweeted this fabricated tweet with full knowledge that Ms. Oueiss never published this statement, with the intent to further the goals of the Conspiracy, all while Defendant Al-Jundi was physically present in Florida.

216. On June 11, 2020, Defendant Al-Jundi attacked another Twitter user for defending Ms. Oueiss. In his tweet, he stated that Ms. Oueiss' father was the "largest Israeli agent in the Army of Lahd[.]" As noted above, Defendant Collins hurled the same false allegation at Ms. Oueiss on the same day that Defendant Al-Jundi posted this.

217. On June 14, 2020, Defendant Al-Jundi, in response to a tweet mentioning Ms. Oueiss, replied as follows: "To the #Jacuzzi beings . . . oh Ghada, who like your father – he was the most senior Israeli agent in the Lahad Army – . . . who ate from the goodness of Saudi Arabia, was a model then excelled in betrayal. No matter how you tweet you will never be less honourable."

218. On June 18, 2020, Defendant Al-Jundi, in response to a tweet mentioning Ms. Oueiss, replied that Ms. Oueiss (and another journalist) were “all traitors” and were only concerned with money.

219. Defendant Al-Jundi was instructed by the Recruiting Defendants, operating under the directed strategy of Defendant MBS, to personally attack Ms. Oueiss on Twitter.

220. Defendant Al-Jundi agreed to take part in this defamatory attack on Ms. Oueiss—and did in fact take part in the attack—all while he was present in Florida. Defendant Al-Jundi posted defamatory tweets regarding Ms. Oueiss for the purpose of intimidating, harassing and otherwise disparaging Ms. Oueiss.

221. At least 59 of Defendant Al-Jundi’s Twitter followers self-report their location as Florida. Accordingly, Defendant Al-Jundi’s defamatory statements regarding Ms. Oueiss were accessed in Florida. Additionally, Defendant Al-Jundi, along with his co-conspirators, based upon the overall scheme, respond to defamatory tweets regarding Ms. Oueiss on Twitter from their respective locations, including in Florida, targeting, at the very least, Twitter users’ communities in their own respective locations and elsewhere.

c. Defendant Annette Smith’s Attacks on Ms. Oueiss

222. Between June 24, 2019 and June 11, 2020, Defendant Smith has posted 24 original tweets mentioning Ms. Oueiss. Notably, Defendant Smith posted 17 of these 24 tweets following the publication of the Personal and Private Photos of Ms. Oueiss in June 2020.

223. On June 9, 2020, just one day before she began posting the stolen Personal and Private Photos of Ms. Oueiss, Defendant Smith accused Ms. Oueiss of choosing a “mercenary path” against Saudi Arabia.



224. Subsequently, on June 10 and 11, 2020, Defendant Smith, like the other U.S. Defendants discussed above, posted the stolen Personal and Private Photos of Ms. Oueiss and said that Ms. Oueiss “should blame herself” for the leak of these photographs.

225. Throughout June 2020, Defendant Smith continued to post defamatory tweets about Ms. Oueiss, including outlandishly claiming that Ms. Oueiss was a “propagandist” who worked for “the same bastards that fund terrorism around the globe.”

226. Defendant Smith was influenced by the Recruiting Defendants, operating under the directed strategy of Defendant MBS, to personally attack Ms. Oueiss on Twitter.

227. Defendant Smith’s conduct was defamatory and consistent with the overall Conspiracy between her and the named Defendants in this Complaint, as well as the John Doe Defendants whose identities have yet to be discerned. The goal of the Conspiracy was to intimidate, harass, and otherwise harm Ms. Oueiss.

228. In addition to directly tweeting defamatory statements about Ms. Oueiss, Defendant Smith, in furtherance of the Conspiracy against Ms. Oueiss, has retweeted other Defendants' defamatory statements about Ms. Oueiss. For example, Defendant Smith has retweeted Defendant Collins' defamatory statement that Ms. Oueiss' late father was involved in the Southern Lebanese Army:



229. At least 74 of Defendant Smith's Twitter followers self-report their location as Florida. Accordingly, Defendant Smith's defamatory tweets regarding Ms. Oueiss targeted, and were accessed by, third parties in Florida and elsewhere.

d. Defendant Christanne Schey's Acts in Furtherance of the Conspiracy

230. Defendant Schey has posted 12 tweets mentioning Ms. Oueiss between August 24, 2018 and June 19, 2020. Notably, on June 19, 2020 Defendant Schey interacted with @KateStewart22 (Defendant Al Qahtani) on Twitter, in which Defendant Schey congratulated @KateStewart22 for getting blocked by Ms. Oueiss on Twitter:



231. Defendant Schey has retweeted numerous defamatory tweets regarding Ms. Oueiss that were originally published by the @KateStewart22 account.



232. At least 293 of Defendant Schey's Twitter followers self-report their location as Florida. Accordingly, Defendant Schey's tweets have been accessed by third parties in Florida.

233. Defendant Schey was instructed by the Recruiting Defendants, operating under the directed strategy of Defendant MBS, to amplify the defamatory attacks on Ms. Oueiss on Twitter.

e. Defendant Al Qahtani’s Use of @KateStewart22 to Attack Ms. Oueiss

234. As discussed above, upon information and belief, Defendant Al Qahtani operates and manages the @KateStewart22 Twitter account in conjunction with a currently unknown individual based in England.

235. The user(s) behind the @KateStewart22 has personally harassed Ms. Oueiss on Twitter since 2019. Specifically, in response to Ms. Oueiss’ tweet regarding the Saudi regime’s involvement in the murder of Mr. Khashoggi, @KateStewart22 personally attacked Ms. Oueiss, describing Ms. Oueiss as a “humiliating, beg-friend, low-grade wannabe TOOL,” and claiming that Ms. Oueiss was “lying about Saudi Arabia.”



236. At any rate, co-conspirators, based upon the overall scheme, respond to Defendant Al Qahtani's (@KateStewart22's) defamatory tweets from their respective locations, including in Miami, Florida, targeting at the very least Twitter communities in their own respective location and elsewhere.

237. @KateStewart22's attacks on Ms. Oueiss were so pervasive that Ms. Oueiss eventually blocked the account user on Twitter. When @KateStewart22 revealed that she had been blocked by Ms. Oueiss, Defendant Schey congratulated @KateStewart22.

238. @KateStewart22's tweets regarding Ms. Oueiss were defamatory, and upon information and belief, were perpetrated in furtherance of the Conspiracy against Ms. Oueiss alleged in this Complaint.

239. At least 85 of @KateStewart22's Twitter followers self-report their location as Florida. Accordingly, third parties accessed these defamatory statements in Florida.

240. Upon information and belief, once discovery is conducted regarding the Twitter account @KateStewart22, it will be revealed that this account was created by or at the direction of Defendants MBS and Al Qahtani for the purpose of harassing, intimidating, and disparaging Ms. Oueiss. Upon information and belief, discovery will also reveal that one of the primary users of the @KateStewart22 account is an England-based individual with significant connections to Defendants MBS and Al Qahtani, among other Saudi and UAE actors.

##### **5. The Harmful Effects and Breadth of the Attacks on Ms. Oueiss**

241. The Network's reach on Twitter is substantial. Specifically, the U.S.-based Defendants have a combined Twitter following of at least 587 Florida residents.

242. The breadth of the attack on Ms. Oueiss was massive. Specifically, while the stolen Personal and Private Photos of Ms. Oueiss were published on June 2, 2020 by @uncareer1, it was the misinformation Network that circulated the posts and amplified the content over the coming

days, which led to a spike in mentions of Ms. Oueiss (@ghadaoueiss) on Twitter on June 9, 2020. While Ms. Oueiss is normally mentioned fewer than ten (10) times per day, she was mentioned in more than 1,500 tweets on June 9, 2020 alone.

243. As shown in the table below, each member of the Network has engaged in significant activity on Twitter in mentioning Ms. Oueiss between their account creation and September 29, 2020, which was conducted in part with the goals and objectives of the Conspiracy against Ms. Oueiss, all at the behest of Defendants MBS, MBZ, Al Qahtani, Al-Asaker and the Recruiting Defendants:

User	Total Mentions of 'Ghada' or @ghadaoueiss	Total Mentions of غادة (Ms. Oueiss' name in Arabic)	Total Mentions	Total Number of retweets
KateStewart22 (Defendant Al Qahtani)	265	1	266	718
SamJundi (Defendant Al-Jundi)	155	65	220	1342
tareklebanon1 (Defendant Zeinab)	74	7	81	388
Orchardcitygal (Defendant Smith)	37	1	38	237
305local (Defendant Collins)	26	3	29	42
ScheyChris (Defendant Schey)	49	4	53	10
Tarek1975leb (Defendant Zeinab)	14	4	18	141
Turki_AlOwerde (Defendant Al-Owerde)	7	1	8	347

244. Furthermore, since the dissemination of the stolen Personal and Private Photos, Ms. Oueiss has blocked over 300 foreign numbers due to scam and harassment calls. To this date, Ms.

Oueiss continues to be harassed and threatened by the social media influence army and the Uncareer network of accounts, who claim to possess additional private information that was unlawfully obtained from Ms. Oueiss' personal mobile device during the hacking event. Ms. Oueiss continues to be harassed via phone call and text message by an ever-changing series of voice-over-internet-protocol (VOIP) or spoofed phone numbers with U.S. country codes.

245. On July 8, 2020, an opinion written by Ms. Oueiss titled "I'm a female journalist in the Middle East. I won't be silenced by online attacks," was published by *The Washington Post*.<sup>49</sup>

246. In August 2020, still two months after the leak of her personal photographs, Ms. Oueiss received an alert to her Google account that informed her of potential nation-state backed hacking attempts against her account, demonstrating that the Conspiracy against Ms. Oueiss is still ongoing.

247. This ongoing Conspiracy against Ms. Oueiss has caused her to suffer reputational harm, loss of business opportunities and income. Ms. Oueiss has also suffered emotional harm and mental anguish as a result of Defendants' ongoing conduct. For example, Ms. Oueiss has visited Florida in the past to visit her family members who reside in this State. However, as a direct result of Defendants' conduct, Ms. Oueiss is now scared to visit her family in Florida, as several Defendants (*e.g.*, Collins and Al-Jundi) reside in Florida.

**6. None of the Defendants Have Satisfied FARA's Registration Requirements**

248. The Foreign Agents Registration Act ("FARA"), codified at 22 U.S.C. § 611 *et seq.*, requires that persons acting as agents of foreign principals who conduct political activity in

---

<sup>49</sup> <https://www.washingtonpost.com/opinions/2020/07/08/im-female-journalist-middle-east-i-wont-be-silenced-by-online-attacks/>

the U.S. disclose the details of their relationship with the foreign principal and report all activities, receipts, and disbursements made on the foreign principal's behalf. The purpose of FARA disclosures is to give the American people the ability to fully evaluate political communications that are sponsored by a foreign state and to prevent foreign states from concealing their attempts to influence U.S. government policy.

249. Defendants were aware they were foreign agents subject to FARA's registration requirements, yet chose to act as unregistered, secret agents to Saudi Arabia and the UAE for months. In doing so, Defendants not only conspired to bombard the public with pro-Saudi and pro-UAE disinformation warfare against all perceived foes of the regimes, they also conspired to and conducted a scheme in violation of FARA, whereby the American Nodes in the Network received payments for their services, in secret, from the Saudi regime. Defendants conducted this scheme without registering with the U.S. Government and without otherwise indicating the warfare they conducted was linked to Saudi Arabia or the UAE.

250. In addition to violating FARA's registration requirements, the American Nodes have also acted as foreign agents for Defendant MBS and the Saudi regime and have not notified the U.S. Attorney General. These acts and omissions by the American Nodes were committed in violation of 18 U.S.C. § 951, which requires those acting as agents of a foreign government to notify the U.S. Attorney General.

### **III. DEFENDANTS CREATE "FAKE NEWS" WEBSITES FOR THE PURPOSE OF SPREADING THE PERSONAL AND PRIVATE PHOTOS OF MS. OUEISS**

251. Separate from Defendants' coordinated use of Twitter (and other social media platforms) to attack and spread misinformation regarding Ms. Oueiss, upon information and belief, Defendants also created and operated various websites that were created specifically for the purpose of spreading disinformation about Ms. Oueiss.

252. Upon information and belief, Defendants coordinated the creation and subsequent operation of the following websites to defame Ms. Oueiss: (1) FNGML [www.fngml.com](http://www.fngml.com) (2) Mashahed [www.mashahed.org](http://www.mashahed.org) (3) <http://www.watannews-sa.com/> (4) [www.tahaanews.com](http://www.tahaanews.com) (5) [www.ahdathnet.net](http://www.ahdathnet.net) (collectively referred to herein as “John Does Websites”).

253. Each of the John Doe Websites participated in a united attack on Ms. Oueiss with respect to the stolen Personal and Private Photos. Specifically, between June 1, 2020 and June 20, 2020, each of the John Doe Websites posted the stolen Personal and Private Photos, along with a uniform (false) narrative that Ms. Oueiss was present at a “sexual” and “pornographic” party when the photographs were taken, and described Ms. Oueiss an employee of a “terrorist platform.”

254. The contents of the numerous articles posted by the operators of the John Doe Websites were false. The articles continue to cause Ms. Oueiss anxiety and mental anguish, as she is constantly reminded that these photographs were stolen from her personal mobile device.

255. The creator(s) of the John Doe Websites have taken efforts to mask their identity. Upon information and belief, discovery will reveal that the websites are operated by, or were created at the direction of, several named Defendants in this Complaint.

256. Publicly available information about the John Doe Websites indicates that they were created at the behest of the Defendants. Specifically, in August 2020, Facebook published a public report of a takedown operation, where Facebook had engaged in the takedown or removal of 28 Pages, 15 Groups, and 10 Instagram accounts for suspected coordinated inauthentic behavior in Yemen. Ahdathnet—one of the five websites mentioned above—was one of the accounts taken down during Facebook’s effort to prevent inauthentic coordinated behavior on its platform.

257. A report evaluating Facebook’s takedown operation was published by Stanford University’s Internet Observatory on August 6, 2020. In its report, Stanford University opined

that Ahdathnet was a Saudi-linked fake news website, with potential connections to the Saudi Ministry of Labor. Specifically, Stanford University evaluated Facebook’s efforts to purge its platform of “coordinated inauthentic behavior,” and noted that Ahdathnet was among those websites associated with involvement in Saudi-backed false reporting:<sup>50</sup>

The relatively active Saudi Ministry of Labor Page can shed some light into what the ultimate goal of these Pages may have been: pushing users to newsweb.news. The Page provided announcements about Saudi news and often linked to newsweb.news. This website lists its Twitter handle as @ahdathnet and Facebook Page as facebook.com/ahdathnetye. The latter is one of the Pages included in this takedown. As such, we assess that newsweb.news is likely connected to ahdathnet.net. Additionally, the fake Ministry of Finance Telegram channel was primarily used to share ahdathnet.net links.

258. Not only was Ahdathnet’s Facebook page removed for inauthentic activity, but in late July to early August 2020, Ahdathnet’s Twitter account was suspended:

---

<sup>50</sup> See [https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20200806\\_yemen\\_report.pdf](https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/20200806_yemen_report.pdf)

Ahdathnet's **Twitter account** was suspended in late July/early August 2020. It has a still-live **YouTube channel** (57 followers) and **Telegram channel** (1,478 followers).



## **CAUSES OF ACTION**

### **FIRST CAUSE OF ACTION (AGAINST ALL DEFENDANTS) HACKING OF PLAINTIFF'S MOBILE DEVICE ATS 28 U.S.C. § 1350**

259. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 145, and 164 through 258 of this Complaint.

260. The conduct described above, *i.e.*, the hacking of Plaintiff's mobile device and the subsequent dissemination of Plaintiff's confidential and sensitive information to the public, constitutes a "tort . . . committed in violation of the law of nations or a treaty of the United States" under 28 U.S.C. § 1350.

261. Specifically, the unlawful hacking operation carried out at the behest of Defendants MBZ and MBS violated universally agreed upon legal principles and violated the norms of customary international laws, including but not limited to the Convention on Cybercrime.

262. Defendants' hacking of Plaintiff's mobile device and subsequent dissemination of Plaintiff's confidential and sensitive information to the public has caused Plaintiff to suffer extreme mental anguish and emotional suffering, including anxiety.

263. Due to Defendants' conduct which, as set forth above, was in violation of the law of nations, Plaintiff is entitled to damages in an amount to be determined at trial.

264. Defendants' acts were premeditated, willful, intentional, malicious and oppressive, and Plaintiff is thus entitled to an award of punitive damages in an amount to be determined at trial.

**SECOND CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
COMPUTER FRAUD AND ABUSE ACT  
18 U.S.C. §§ 1030(a)(2)(C)**

265. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5 and 164 through 258 of this Complaint.

266. Upon information and belief, Defendants accessed or caused to be accessed Plaintiff's mobile device and the files and photographs physically located therein. Defendants utilized hacking technology to access the contents of Plaintiff's personal mobile device (and all files physically located in her mobile device), during a time when Plaintiff and her mobile device were physically present in California, among other locations, without authorization.

267. Upon information and belief, Defendants compromised Plaintiff's mobile device in a deliberate and premeditated scheme, whereby Defendants MBS, MBZ, Al Qahtani, and Al-Asaker, among others, utilized sophisticated cyber hacking group Defendant DarkMatter to hack into Plaintiff's mobile device and unlawfully obtain confidential content from the device.

268. By engaging in this conduct, Defendants accessed "protected computers," defined by 18 U.S.C. § 1030(e)(2)(B) as computers "used in or affecting interstate or foreign commerce or

communication.” A cell phone, such as Ms. Oueiss’ personal mobile device, constitutes a “computer” for purposes of the Computer Fraud and Abuse Act. *See U.S. v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011).

269. As a direct result of the actions of Defendants, Plaintiff suffered losses, including but not limited to costs associated with repairing the integrity of Plaintiff’s personal mobile device after the hacking, and other consequential damages, such as evaluating the intrusion, theft and conduct relating to the theft, as well as damages related thereto, in an amount to be proven at trial, but in any event, in excess of \$5,000.

270. Defendants intentionally caused such damage to Plaintiff.

271. Defendants’ conduct in carrying out the hacking of Plaintiff’s personal mobile device has caused, and will continue to cause Plaintiff irreparable injury, including reputational harm, loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be compensated by monetary damages. Accordingly, Plaintiff seeks an injunction prohibiting Defendants from engaging in the conduct described in this count.

**THIRD CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
STORED COMMUNICATIONS ACT  
18 U.S.C. §§ 2701-12**

272. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5 and 164 through 258 of this Complaint.

273. Plaintiff is a “person” within the meaning of 18 U.S.C. § 2707(a).

274. Defendants willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided. The manner in which Defendants hacked Plaintiff’s mobile device, together with the underlying data ingress and egress from Plaintiff’s device and then-existing vulnerabilities in WhatsApp’s application, indicates that

Defendants accessed WhatsApp servers to access confidential content stored on Plaintiff's device. These servers, in part, provided Defendants with access to files physically and electronically stored on Plaintiff's mobile device and with access to several files that were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

275. As a result of Defendants' willful and intentional violations, Plaintiff has suffered damages and, as provided for in 18 U.S.C. § 2707, is entitled to an award of the greater of the actual damages suffered or the statutory damages, punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

276. Defendants' conduct has caused, and will continue to cause Plaintiff irreparable injury, including reputational harm, loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Such injury cannot be compensated by monetary damages. Accordingly, Plaintiff seeks an injunction prohibiting Defendants from engaging in the conduct described in Plaintiff's Third Cause of Action.

**FOURTH CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS (FLORIDA LAW)**

277. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 137, and 164 through 258 of this Complaint.

278. Defendants' actions described in this Complaint, including but not limited to, intentionally accessing Plaintiff's mobile device to obtain photographs of Plaintiff and disseminate them publicly, was intentional or reckless. Specifically, Defendants knew or should have known that Plaintiff would suffer emotional distress as a result of the dissemination of her personal and confidential photographs to the public, while simultaneously spreading a false narrative that Plaintiff was, at that time that several of the stolen photographs were taken, engaged in sexual acts in exchange for notoriety, fame, and other favors.

279. Defendants' actions described in this Complaint were outrageous. Specifically, Defendants' conduct went beyond all bounds of decency and is utterly intolerable in a civilized community.

280. Defendants' actions described in this Complaint have caused Plaintiff to suffer severe emotional distress. Specifically, Plaintiff suffered mental anguish as a result of the public ridicule and harassment that she has faced (and continues to face) every day since these photographs were wrongfully accessed and disseminated from her mobile device.

281. As a result of Defendants' actions, Plaintiff has suffered severe emotional distress. Plaintiff is entitled to monetary damages in an amount to be determined at trial.

**FIFTH CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
INTRUSION (FLORIDA LAW)**

282. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 137, and 164 through 258 of this Complaint.

283. Defendants, through their acts of accessing Plaintiff's electronic files from her personal mobile device, physically or electronically intruded into Plaintiff's private quarters.

284. Upon information and belief, Defendants hacked, stole, doctored, and disseminated to others the personal and private information stored on Plaintiff's mobile device. Defendants committed these acts without Plaintiff's consent, and with the deliberate intent to unlawfully access Plaintiff's personal and private information.

285. Defendants' conduct described in this Complaint, including the intrusion into Plaintiff's mobile device described herein, is highly offensive to a reasonable person. A reasonable person would expect to be free from the intrusion that Plaintiff was subjected to as a result of Defendants' concerted actions to silence, intimidate, harass, and destroy Plaintiff's reputation.

286. The public disclosure of Plaintiff's personal and confidential information has caused, and will continue to cause, Plaintiff injury, including reputational harm, an increased risk of further theft, and an increased risk of harassment.

287. Plaintiff will continue to suffer this injury as long as her personal information is available to Defendants.

288. Defendants' conduct described in this Complaint was so outrageous in character as to go beyond all possible bounds of decency.

289. Defendants' conduct has caused, and will continue to cause Plaintiff irreparable injury, including reputational harm, loss of goodwill, an increased risk of further harassment. Such injury cannot be compensated by monetary damages. Accordingly, Plaintiff seeks an injunction prohibiting Defendants from engaging in the conduct described in this count.

**SIXTH CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
PUBLIC DISCLOSURE OF PRIVATE FACTS (FLORIDA LAW)**

290. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 137, and 164 through 258 of this Complaint.

291. Through the conduct described in this Complaint, Defendants accessed electronic files (including photographs) on Plaintiff's mobile device, which Defendants then distributed through a vast network of social media, including but not limited to, Twitter accounts and websites.

292. In disseminating these photographs of Plaintiff, Defendants attached a false narrative to such photographs, including but not limited to false narratives that Plaintiff was engaged in sexual acts at the time the photographs were taken in exchange for favors.

293. The photographs and other electronic information contained on Plaintiff's personal mobile device were private and confidential, and Defendants accessed them and disseminated them to the public without Plaintiff's consent.

294. The photographs which Defendants unlawfully accessed on Plaintiff's mobile device were offensive when disseminated to the public because Defendants utilized such photographs to create a false narrative intended to destroy Plaintiff's reputation and otherwise subject Plaintiff to humiliation and hatred.

295. The photographs of Plaintiff were not of public concern. These photographs of Plaintiff were not publicly available, nor did Plaintiff consent to their use.

296. Defendants' conduct has caused, and will continue to cause, Plaintiff irreparable injury, including reputational harm, loss of goodwill, an increased risk of further harassment. Such injury cannot be compensated by monetary damages. Accordingly, Plaintiff seeks an injunction prohibiting Defendants from engaging in the conduct described in this count.

**SEVENTH CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
LIBEL (FLORIDA LAW)**

297. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 137, and 164 through 258 of this Complaint.

298. Defendants, through the conduct described in this Complaint, unlawfully accessed electronic files (including photographs) on Plaintiff's mobile device.

299. Subsequent to obtaining possession of such electronic files, Defendants, through various networks on social media and other websites, disseminated the photographs of Plaintiff along with a false narrative that, at the time the photographs were taken, Plaintiff was engaged in sexual acts in exchange for favors.

300. These false narratives, along with the stolen and doctored photographs, were disseminated through numerous Twitter accounts (including the accounts of several named Defendants discussed herein), and were also displayed on the John Doe Websites which, upon

information and belief, were created at Defendants' direction for the sole purpose of harassing Plaintiff.

301. These false narratives circulated along with the photographs of Plaintiff were incorrect, incomplete, or otherwise erroneous, and thus implied a false statement of fact regarding Plaintiff's activities at the time these photographs were taken.

302. These false narratives and the stolen photographs were published by Defendants Collins and Al-Jundi while they were physically present in Florida. These narratives were also accessed by Florida residents on Twitter, as each Defendant who published the photos and false narratives has numerous Twitter followers who reside in Florida.

303. Defendants' conduct exposed Plaintiff to distrust, hatred, ridicule and extreme embarrassment.

304. As a result of Defendants' conduct, Plaintiff has suffered injury to her personal and professional reputation, and Plaintiff's reputation is now lowered in the estimation of the community and audience with which she regularly engages during her employment as an international broadcaster and journalist.

305. As a result of Defendants' conduct, Plaintiff has suffered monetary damages, as well as the reputational harm described above, in an amount to be determined at trial.

**EIGHTH CAUSE OF ACTION (AGAINST ALL DEFENDANTS)  
CIVIL CONSPIRACY (FLORIDA LAW)**

306. Plaintiff incorporates and adopts by reference all the allegations contained in Paragraphs 1 through 5, 33 through 137, and 164 through 258 of this Complaint.

307. Upon information and belief, Defendants willfully and knowingly agreed and conspired with each other to engage in the wrongful conduct alleged in this Complaint, including but not limited to hacking Ms. Oueiss' mobile device, obtaining unlawful access and possession

of private data on Ms. Oueiss' mobile device, and thereafter agreeing to disseminate such private information and content by using the cohesive Network described in this Complaint.

308. Upon information and belief, the term of the Conspiracy amongst all Defendants commenced in mid-2018 and is still ongoing.

309. Upon information and belief, each Defendant named herein entered into an agreement (either explicitly or tacitly) whereby they conspired to commit the following acts, among other acts set forth above:

- a. Form the Network to promote Saudi Arabian and UAE interests and simultaneously condemn, defame, and otherwise intimidate any dissidents of the Saudi and UAE regimes, in violation of FARA's registration requirements, set forth in 22 U.S.C. § 611 *et seq.*;
- b. Utilize Defendant DarkMatter, along with other agents of Defendants MBS and MBZ, to hack Ms. Oueiss' personal mobile device on or about October 2019 through May 2020, and thereby obtain confidential and sensitive information physically stored on Ms. Oueiss' personal mobile device without authorization and then stealing and doctoring Ms. Oueiss' data, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C) and Florida common law;
- c. Utilize Defendant DarkMatter, along with other agents of Defendants MBS and MBZ, to willfully and intentionally access, without authorization, a facility through which an electronic communication service is provided. Specifically, as discussed above, the data ingress and egress from Plaintiff's mobile device indicates that Defendants accessed WhatsApp's servers and thereby obtained access to data while in electronic storage in such systems, in violation of the Stored Communications Act, 18 U.S.C. § 2701(a);
- d. Utilize John Doe Defendants to create several anonymous social media accounts, as well as the John Doe Websites, solely for the purpose of disseminating the stolen photographs of Ms. Oueiss to the public, along with the false narrative that Ms. Oueiss was engaged in sexual acts at the time the photographs were taken, with the intent to defame and disparage Ms. Oueiss;
- e. Utilize the named Defendants in this Complaint (who are a part of the Network discussed above) to further publish the stolen photographs of Ms. Oueiss as a means to intimidate, harass and defame Ms. Oueiss;

- f. Utilize the named Defendants in this Complaint (who are a part of the Network discussed above) to assassinate Ms. Oueiss' character through Twitter by, among other things, tweeting false stories regarding Ms. Oueiss with the intent to disparage, intimidate, and otherwise harm Ms. Oueiss; and
- g. Utilize the named Defendants in this Complaint (who are a part of the Network discussed above) to threaten Ms. Oueiss with the release of additional private and personal information that was unlawfully obtained from Ms. Oueiss' personal mobile device.

310. Upon information and belief, the Conspiracy was agreed to within and outside of the U.S.

311. As noted above, at least one step in furtherance of the Conspiracy occurred within the U.S., namely, Defendant Collins' and Defendant Al-Jundi's defamation of Ms. Oueiss while both Defendants were present in Florida. Upon information and belief, Defendant Collins also disseminated the images of Ms. Oueiss with full knowledge that such images had been stolen from Ms. Oueiss' mobile device, and with the intent to further the goals of the Defendants' Conspiracy.

312. Additionally, Defendants published doctored images of the original photographs of Plaintiff to make it appear as though Plaintiff was naked to further the false narrative that Plaintiff was engaged in sexual acts at the time the photographs were taken. These photographs and false narratives were disseminated by individual Defendants named herein on their public Twitter accounts, as well as the John Doe Websites which, upon information and belief, were created at Defendant MBS's behest for the purpose of harassing, intimidating and causing harm to Plaintiff.

313. Each Defendant named in this Complaint committed an overt act in furtherance of the Conspiracy:

- a. Upon information and belief, Defendants MBS, MBZ, Al Qahtani, and Al-Asaker, among others, utilized Defendant DarkMatter to hack into Ms. Oueiss' mobile device and unlawfully obtain access to Ms. Oueiss' personal and confidential information, with the intent to use such information to defame, disparage and otherwise harm Ms. Oueiss;

- b. Defendant Al Arabiya committed the overt act of knowingly publishing the Doctored Financial Photo, and attempted to attribute such false documents to Ms. Oueiss as a way of defaming and disparaging Ms. Oueiss;
- c. Defendants MBS, Al-Asaker and Al Qahtani committed the overt act of directing Defendants Zeinab, Al Menaia, Al Otaibi, and Al-Owerde to recruit each member of the Network discussed above, with the goal of promoting Saudi Arabia's and UAE's public image, while disparaging those who criticized the Saudi and UAE regimes, including Plaintiff. Upon information and belief, Defendants Al-Asaker and Al Qahtani used their positions at SACM and the MiSK Foundation to recruit members of the Network in furtherance of the Conspiracy against Ms. Oueiss;
- d. The Recruiting Defendants (*i.e.*, Zeinab, Al Menaia, Al-Owerde, and Al Otaibi), at the direction of Defendants MBS, Al Qahtani, Al-Asaker and officers of Saudi 24 TV, committed the overt act of recruiting each individual in the Network for the purpose of spreading pro-Saudi Arabian propaganda. Upon information and belief, the Recruiting Defendants also instructed members of the Network to disseminate the photographs of Ms. Oueiss via Twitter, along with the false narrative that Ms. Oueiss was somehow responsible for the release of the photographs;
- e. Defendant Collins committed an overt act in furtherance of the Conspiracy while present in Florida. Specifically, from at least June 7, 2020 to June 9, 2020, Defendant Collins repeatedly harassed, defamed and disparaged Plaintiff on Twitter. Defendant Collins, among other defamatory acts described herein, posted the stolen photographs of Plaintiff and accused her of selling herself "to terrorists to get a story[.]" Upon information and belief, Defendant Collins engaged in this conduct at the request or direction of the other Defendants, and with the intent to defame Ms. Oueiss;
- f. Defendant Smith committed an overt act in furtherance of the Conspiracy. Specifically, on June 10, 2020, Defendant Smith posted the stolen photographs of Plaintiff, along with the false narrative that the release of such photographs were somehow Plaintiff's fault;
- g. Defendant Al-Jundi committed an overt act in furtherance of the Conspiracy when he defamed and disparaged Plaintiff on Twitter, while Defendant Al-Jundi was physically present in Florida;
- h. Defendant Schey committed an overt act in furtherance of the Conspiracy when she retweeted defamatory tweets regarding Ms. Oueiss that were published by the @KateStewart22 account, among other defamatory tweets.

314. Upon information and belief, each of the overt acts described above were committed in furtherance of Defendants' Conspiracy, *i.e.*, to harass, intimidate, humiliate and

otherwise cause harm to Plaintiff through the unlawful access and dissemination of personal and private information contained on Plaintiff's personal mobile device.

315. As a direct, proximate, and foreseeable result of Defendants' concerted and unlawful acts, Plaintiff has suffered the injuries described in this Complaint, including reputational harm, loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Additionally, Plaintiff has suffered mental anguish, anxiety, lost business opportunities, and other tangible and intangible harm. Plaintiff's family resides in Florida, and while Plaintiff has visited her family here before, Plaintiff is now frightened to visit this State, as several Defendants involved in this Conspiracy reside in Florida (*e.g.*, Defendants Collins and Al-Jundi). Accordingly, due to Defendants' ongoing conduct, Plaintiff has been precluded from visiting her own family, causing her to suffer emotional harm.

316. These injuries and losses have occurred in the past, are occurring in the present, and likely will continue in the future. Plaintiff also seeks equitable relief in the form of an injunction and punitive damages under this count.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff requests this Court enter judgment against Defendants, setting forth as follows:

- (1) A declaration that Defendants' conduct constitutes violations of the statutes and common law cited herein;
- (2) A permanent injunction to be issued enjoining Defendants, their employees, agents, successors and assigns, and all those in active concert and participation with Defendants, and each of them who receives notice directly or otherwise of such injunctions, from:

- a. Continuing to engage in any defamatory action affecting Plaintiff's business interests or reputation;
  - b. Conspiring to hack Plaintiff's personal mobile device to obtain personal and confidential information for dissemination; and
  - c. Any other efforts to unlawfully harm Plaintiff.
- (3) A monetary judgment, for an amount equal to actual damages sustained by Plaintiff, plus reasonable attorneys' fees, punitive damages, and costs in prosecuting the action; and
- (4) For any other relief this Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff respectfully requests a trial by jury of all issues properly triable by jury.

Dated: December 9, 2020

Respectfully submitted,  
/s/ Daniel L. Rashbaum  
DANIEL L. RASHBAUM  
Fla. Bar No. 75084  
drashbaum@mnrlawfirm.com  
JEFFREY E. MARCUS  
Fla. Bar No. 310890  
jmarcus@mnrlawfirm.com  
Marcus Neiman & Rashbaum LLP  
One Biscayne Tower  
2 South Biscayne Blvd., Suite 1750  
Miami, Florida 33131  
Telephone: (305) 400-4260