UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALI AL-AHMED,

Plaintiff,

v.

TWITTER, INC., et al.,

Defendants.

Case No. 21-cv-08017-EMC

ORDER GRANTING DEFENDANT TWITTER'S MOTION TO DISMISS

Docket No. 62

I. INTRODUCTION

Plaintiff Al-Ahmed is a critic of the Kingdom of Saudi Arabia ("KSA") who has been granted asylum in the United States. Between 2013 and 2015, two of Twitter's (now former) employees accessed user information without authorization and provided it to KSA government officials. The employees were indicted in 2019. On October 13, 2021, Al-Ahmed sued the former employees and Twitter. Specifically, Al-Ahmed sued Twitter for violating the Electronics Communications Privacy Act ("EPCA"); the Computer Fraud and Abuse Act ("CFAA"); the Stored Communications Act ("SCA"); California's Unfair Competition Law ("UCL"); breach of contract; intrusion upon seclusion; unjust enrichment; promissory estoppel; negligence; negligent hiring, supervision, and retention; civil conspiracy; and replevin. *See* Docket No. 1 ("original complaint"). In Al-Ahmed's First Amended Complaint, he adds claims for breach of the duty of loyalty, aiding and abetting breach of fiduciary duty, an additional UCL claim, and interference with prospective economic advantage. *See* Docket No. 55 ("FAC"). Notably, Al-Ahmed does not add a claim under the Lanham Act, for which he was granted leave to amend after this Court dismissed the original complaint. Al-Ahmed alleges that his Twitter account was hacked, which

led to the KSA targeting him and those around him. Furthermore, he alleges that Twitter's suspension of his account in 2018 punishes him—the victim—and demonstrates that Twitter was complicit in their former employees' conduct, or at least that Twitter ratified their conduct.

The Court dismissed Al-Ahmed's first complaint with leave to amend. *See Al-Ahmed v. Twitter, Inc.*, No. 21-CV-08017-EMC, 2022 WL 1605673, at *5 (N.D. Cal. May 20, 2022). He filed an amended complaint. *See* FAC. Pending now is Twitter's motion to dismiss Al-Ahmed's FAC. *See* Docket No. 62 ("Mot."). Twitter argues that (1) Al-Ahmed lacks Article III standing, (2) his claims are barred by the statute of limitations, (3) he does not plausibly plead that Twitter is vicariously liable for its rogue employees' acts on behalf of the KSA, (4) the Community Decency Act ("CDA") immunity bars many of his claims, (5) Twitter's Terms of Service ("TOS") bars many of his claims, and (6) individual actions fail for numerous claim-specific reasons. The Court only addresses Article III standing, the statute of limitations, and CDA immunity because each of Al-Ahmed's claims fail for one of these three reasons.

II. BACKGROUND

A. Factual Background

Al-Ahmed alleges as follows in his FAC:

Al-Ahmed is one of the leading critics of the KSA who resides and has been granted asylum in the United States. FAC ¶ 17. Between August 2013 and December 2015, Twitter employees accessed user data without authorization and provided the data to KSA government officials. *Id.* ¶¶ 22–23. Twitter failed to detect these breaches for more than a year. *Id.* ¶ 26. Al-Ahmed's Arabic Twitter account, which has over 36,000 followers worldwide, was one of the accounts breached during this time. *Id.* ¶ 21. Al-Ahmed contends that Twitter's conduct resulted in the compromising of his private information, including his "email addresses, contacts, phone numbers, birth dates, and internet protocol ("IP") addresses;" and his "Tweets, private messages, direct message, online chats, friend requests, file transfers, file uploads, and file downloads." *Id.* ¶¶ 24, 79. He also alleges confidential information provided by his followers and journalistic sources was compromised. *Id.* ¶ 4. Al-Ahmed alleges his private information was used by the KSA to silence him by stripping him of his Saudi nationality, keeping him under surveillance, and

attempting to kidnap and kill him on multiple occasions. *Id.* ¶ 18. Al-Ahmed alleges his followers on Twitter and those who otherwise contacted him using Twitter, have disappeared, been arrested, or have been executed. *Id.* ¶ 27. Examples of such third-party harms include the jailing of Saudi dissident Abdullah al-Hamid, whom the KSA jailed in 2013, and the murder of journalist Jamal Khashoggi in 2018, which Al-Ahmed alleges was not uncoincidental to the KSA's espionage against Twitter. *Id.* ¶¶ 27, 57. According to the FAC, "the KSA managed to fully silence Al-Ahmed when [Twitter] . . . suspend[ed his] Arabic Twitter account, without explanation, warning, or justification. *Id.* ¶ 28.

On November 19, 2019, the two Twitter employees allegedly responsible for hacking Al-Ahmed's account were indicted for acting as agents of the KSA. *Id.* ¶ 7. Defendant Ahmad Abouammo ("Abouammo") was the Media Partnerships Manager responsible for the Middle East and North Africa region at Twitter. *Id.* ¶ 5. Defendant Ali Hamad A. Alzabarah ("Alzabarah") was a Site Reliability Engineer whose responsibility was maintaining Twitter's hardware and software to ensure uninterrupted service. *Id.* ¶ 6.

1. Twitter's Notice

On or about December 11, 2015, Twitter sent the following notice to the users whose data was accessed by Abouammo and Alzabarah:

> Dear @{{screen_name}}, As a precaution, we are alerting you that **your Twitter account is one of a small group of accounts that may have been targeted by state-sponsored actors**. We believe that **these actors (possibly associated with a government) may have been trying to obtain information such as email addresses, IP addresses, and/or phone numbers**.
>
> At this time, we have no evidence they obtained your account information, but we're actively investigating this matter. We wish we had more we could share, but we don't have any additional information we can provide at this time.
>
> It's possible your account may not have been an intended target of the suspected activity, but we wanted to alert you as soon as possible. We recognize that this may be of particular concern if you choose to Tweet using a pseudonym. For tips on protecting your identity online, you may want to visit the Tor Project or EFF's Protecting Yourself on Social Networks.

Id. ¶ 45.

According to Al-Ahmed, this notice was insufficient to inform him of the scope and nature of the problem because it did not indicate that Abouammo and Alzabarah committed these data breaches at the direction of Twitter, and while located on Twitter's premises, employed by Twitter, and using Twitter's resources. *Id.* ¶ 46. Therefore, Al Ahmed alleges he did not, and could not have reason to know of Twitter's involvement until the public indictment of the employees in 2019. *Id.* ¶ 47. Further, Al-Ahmed alleges for the first time in his FAC that he did not in fact receive the notice. *Id.* ¶ 48.

2. Twitter's Alleged Actions in Aid of the KSA

Al-Ahmed alleges that Twitter provided Abouammo and Alzabarah with access to Twitter's resources with the full knowledge that they were improperly accessing user data, that Twitter helped them provide the information to the KSA, and Twitter helped them cover their tracks by purging its internal database of incriminating evidence. *Id.* ¶ 25.

Al-Ahmed also alleges that Twitter's Privacy Policy suggests that a user can adjust their account settings so their Tweets can only be viewed by the user's Twitter followers. *Id.* ¶¶ 31–32. This created an illusion of security and safety relied upon by Al-Ahmed and others. *Id.* Al-Ahmed alleges that Twitter failed to safeguard user data, evidenced by its disclosure to the Securities and Exchange Commission in 2020 that it received a draft complaint from the Federal Trade Commission alleging "violations…[r]elate[d] to the Company's use of phone number and/or email address data provided for safety and security purposes [ostensibly for targeted advertising] during periods between 2013 and 2019." *Id.* ¶ 38. Thus, he argues Twitter negligently failed to implement policies, practices, and safeguards that would have prevented the acts of its former employees. *Id.*

3. Twitter's Relationship with the KSA

In 2011, Saudi Prince Alwaleed Bin Talal purchased $300 million worth of stock in Twitter. *Id.* ¶ 3. In 2015, Bin Talal made an additional investment, and now owns 5.2% of the company, more than Twitter's founder and former CEO, Jack Dorsey ("Dorsey"). *Id.* Bin Talal later signed over many of his assets to Crown Prince of Saudi Arabia Mohammed Bin Salman. *Id.* Al-Ahmed further alleges that Bader al-Asaker, the head of Bin Salman's office, was the "Saudi

mastermind" behind the Twitter spy scandal. *Id.* ¶ 39. He claims that Asaker is "Foreign Official-1" in the United States Attorneys Offices' indictment against Abouammo and Alzabarah. *Id.* ¶ 41. Al-Ahmed alleges that Asaker provided Abouammo and Alzabarah with "gifts, cash payments, and promises of future employment in exchange for nonpublic information about Twitter uses, which constituted valuable property..." *Id.* Furthermore, Dorsey met with both Asaker and Bin Salman at Twitter's headquarters on June 25, 2016, and at least one additional time in Riyadh thereafter. *Id.* ¶ 43. Dorsey and Asaker follow each other on Twitter. *Id.* ¶ 44.

4. Twitter's Suspension of Al-Ahmed's Account

In 2018, Al-Ahmed's Twitter account was suspended, preventing him from accessing his followers. *Id.* ¶¶ 28, 30. The basis of his suspension was an allegedly abusive direct message ("DM") Al-Ahmed sent using his Arabic language Twitter account. *Id.* ¶ 50. Al-Ahmed alleges that as a result, he lost significant revenue and earning potential related to his work as a journalist, as much of his work was contingent on his online presence. *Id.* ¶ 59. Al-Ahmed further alleges that his appeal of the suspension failed despite Alzabarah and Abouammo's indictment. *Id.* ¶ 29. According to Al-Ahmed, preventing access to his account, punishes the victim and "ratifie[s] the actions of its supposedly errant employees and show[s] [Twitter's] continuing allegiance to the KSA." *Id.*

Al-Ahmed also alleges that his suspension is the result of Twitter and the KSA's campaign against him. *Id.* ¶ 50. He asserts "agents of the KSA or other Twitter employees accessed his "private Twitter accounts to read and manipulate content, including, but not limited to, purported private/direct exchange messages that were then used as a pretext by Twitter" to suspend his Arabic-language account. *Id.* Al-Ahmed claims he does not recognize the statement attributed to him, the message was a "fabrication," and is an incorrect translation. *Id.* ¶¶ 50–51. The English translation of the message provided by Twitter reads, "Damn your mother, you Ahmari, you mountain monkey, you Ethiopian, you slave, you pagan, you cow, you beast of burden! … I see your face and your teeth sticking out. Damn your father and Khomeini, you slave, you beast of burden, you animal!" *Id.* ¶ 50; *see* Docket No. 31, Ex. 5. According to Al-Ahmed, "Twitter's translation of the word 'slave' could be more accurately translated to 'lowlife' and is a common

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.