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'S MOTION TO DISMISS

Docket No. 30

I. INTRODUCTION

Plaintiff Al-Ahmed is a critic of the Kingdom of Saudi Arabia ("KSA") and has been granted asylum in the United States. Between 2013–2015, two of Twitter's (now former) employees, Defendants Ahmad Abouammo and Ali Hamad A. Alzabarah, accessed user information on Al-Ahmed without authorization and provided it to KSA government officials. Al-Ahmed filed this lawsuit against Abouammo, Alzabarah, and Twitter for violating the Electronics Communications Privacy Act ("EPCA"), violating the Computer Fraud and Abuse Act ("CFAA"), violating the Stored Communications Act ("SCA"), violating 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. 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 ratifies its former employees' conduct. Pending in this Court is Twitter's motion to dismiss Al-Ahmed's Complaint. The Court **GRANTS** Twitter's motion for the reasons stated below.

II. BACKGROUND

Al-Ahmed alleges as follows in the Complaint:

Al-Ahmed is one of the leading critics of the KSA who resides and has been granted asylum in the United States. Docket No. 1 ("Complaint") at 2. Between August 2013 and December 2015, Twitter user information was accessed without authorization and provided to KSA government officials, which Twitter failed to detect for a period of time spanning over a year. *Id.* at 4, 7. Al-Ahmed's Arabic Twitter account, which has over 36,000 followers worldwide, was one of the accounts breached during this time. *Id.* at 6. Al-Ahmed contends that his private information, including his personal phone number and email address, which he never made publicly available, was compromised due to Twitter's conduct. *Id.* at 16. His account also had confidential information provided by his followers and journalistic sources. *Id.* at 3. 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.* at 6–7. His followers on Twitter, or those who otherwise contacted him using Twitter, have disappeared, been arrested, or have been executed. *Id.* at 8. According to him, "the KSA managed to fully silence [him] when they . . . suspend[ed his] Arabic Twitter account, without explanation, warning, or justification." *Id.* at 8.

On November 19, 2019, Abouammo and Alzabarah were indicted for acting as agents for the government of Saudi Arabia while employed at Twitter. *Id.* at 4. Abouammo was the Media Partnerships Manager responsible for the Middle East and North Africa region at Twitter. *Id.* at 3. Alzabarah was a Site Reliability Engineer whose responsibility was maintaining Twitter's hardware and software to ensure uninterrupted service. *Id.*

A. Twitter's Notice

On or about December 11, 2015, Twitter sent the following notice to a small group of its users:

> 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**

> **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. at 14. Al-Ahmed alleges that this notice was insufficient because it failed to indicate that these state-sponsored actors committed these data breaches while they were located on Twitter's premises, employed by Twitter, using Twitter's resources, at the direction of Twitter. *Id.* at 15.

B. Twitter's Actions in Aid of the KSA

Al-Ahmed alleges that Twitter provided the two employees with access to Twitter's resources with the full knowledge that they were improperly accessing user data, helped them provide the information to the KSA, and helped them cover up their tracks by purging its internal database of incriminating evidence. *Id.* at 7. Al-Ahmed also alleges that Twitter's Privacy Policy suggests that Tweets may be protected by opting to allow only Twitter followers to see them through account settings, which created an illusion of security and safety. *Id.* at 10. Al-Ahmed lastly alleges that Twitter failed to safeguard user data, evidenced by its disclosure to the Securities and Exchange Commission in 2020. The disclosure stated that Twitter 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.* at 12. Thus, Twitter negligently failed to implement policies, practices, and safeguards that would have prevented the acts of its former employees. *Id.* at 37.

C. Twitter's Relationship with the KSA

In 2011, Saudi Prince Alwaleed Bin Talal purchased $300 million worth of stock in Twitter. *Id.* In 2015, Bin Talal made an additional investment, owning 5.2% of the company, more than Twitter's founder and CEO. *Id.* at 2. Bin Talal later signed over many of his assets to

Crown Prince Bin Salman. *Id.* Thus, Al-Ahmed alleges that Twitter's acts were designed to appease Bin Salman, a significant investor. *Id.* According to Al-Ahmed, Bader al-Asaker is the head of Bin Salman's affairs and the "Saudi mastermind" behind the Twitter spy scandal. *Id.* at 13. He claims that Asaker is "Foreign Official-1" in the United States Attorneys Offices' indictment against Abouammo and Alzabarah. *Id.* 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, Twitter CEO Jack 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.* at 13. Dorsey and Asaker follow each other on Twitter. *Id.*

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

In 2018, Al-Ahmed's Twitter account was suspended, preventing access to his followers. *Id.* at 8. 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.* at 16. Al-Ahmed further alleges that his appeal of the suspension failed despite Alzabarah and Abouammo's indictment. *Id.* at 8. According to Al-Ahmed, preventing access to his account and the list of his followers, punishes the victim and "ratifie[s] the actions of its supposedly errant employees and show[s] [Twitter's] continuing allegiance to the KSA." *Id.*

III. LEGAL STANDARD

A. Motion to Dismiss

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Fed. R. Civ. P. 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) and *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success.'" *Levitt v. Yelp! Inc.*, 765 F.3d

construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135 (quoting *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014)). "A claim has facial plausibility when the Plaintiff pleads factual content that allows the court to draw the reasonable inference that the Defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (quoting *Twombly*, 550 U.S. at 556).

B. Judicial Notice

Under Federal Rule of Evidence 201, "[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201. Courts may take judicial notice of "undisputed matters of public record," but generally may not take judicial notice of "disputed facts stated in public records." *Lee v. City of Los Angeles*, 250 F.3d 668, 690 (9th Cir. 2001). Facts subject to judicial notice may be considered on a motion to dismiss. *Mullis v. U.S. Bankr. Ct.*, 828 F.2d 1385, 1388 (9th Cir. 1987). "Proper subjects of judicial notice when ruling on a motion to dismiss include . . . publically accessible websites[.]" *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1204 (N.D. Cal. 2014) (citing *Caldwell v. Caldwell*, No. 05–4166, 2006 WL 618511, at *4 (N.D. Cal. Mar. 13, 2006); *Wible v. Aetna Life Ins. Co.*, 375 F.Supp.2d 956, 965–66 (C.D. Cal.2005).

The doctrine of incorporation by reference is distinct from judicial notice. The doctrine "permits a district court to consider documents 'whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the . . . pleadings.'" *In re Silicon Graphics Sec. Litig.*, 183 F.3d 970, 986 (9th Cir. 1999) (quoting *Branch v. Tunnell*, 14 F.3d 449, 454 (9th Cir.1994)). The court may incorporate such a document "if the

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.