

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

Case No. 21-10016-EFM

RANDY SPORN,

Defendant.

MEMORANDUM AND ORDER

This matter comes before the Court on Defendant Randy Sporn's Motion to Suppress (Doc. 24). Defendant seeks suppression of all evidence obtained from the search of his Twitter account by Wichita police, as well as information derived from several state search warrants which were premised on information from the Twitter account. The Government opposes the motion, offering a wide variety of rationales for determining that the evidence should not be suppressed. The Court finds that Defendant lacked any objective expectation of privacy in the Twitter content, that the review of the Twitter content violated no property right of Defendant, and the police search of the account information occurred in good faith. Because the search of the preserved Twitter account information was valid, the state search warrants were also valid. Accordingly, the Court denies Defendant's Motion to Suppress.

I. Factual and Procedural Background

In the March 23, 2021 Indictment, Defendant is charged with sexual exploitation of a child through the production of child pornography, in violation of 18 U.S.C. § 2251(a); commission of a felony by a registered sex offender in violation of 18 U.S.C. § 2260A; and possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). These charges stem from Defendant's use of the Twitter messaging service. In late 2019 and early 2020, Twitter reported two accounts violations of its child sexual exploitation policy to the National Center for Missing and Exploited Children (NCMEC). Reviewing NCMEC's CyberTipline reports, Wichita police were able to link both accounts to Defendant.

A. Twitter's Terms of Service

Evan Anderson is the lead policy expert at Twitter's Trust and Safety Department, where his duties include maintaining and defining policies relating to child safety. Anderson has worked at Twitter for seven years. Before joining Twitter, Anderson worked for five years at NCMEC. In that position, he reviewed reports and gave advice as to the CyberTipline reports issued by NCMEC. The Court finds Anderson testified credibly.

Twitter allows registered users to post content in the form of "tweets," which may be text (subject to a character limit), an image, or a short video. A tweet may be published generally, visible to anyone using the Twitter service, or it may be restricted and visible only to the user's followers. By default, Tweets are unrestricted. Twitter also allows users to send direct messages to another user or users.

Twitter is a private company which receives no government subsidies. While Twitter follows the laws and regulations of the United States, the Government does not tell Twitter how to run its business.

Most of Twitter's registered users are outside the United States. On any given day, some 200 million users around the globe interact on Twitter.

Any person may view publicly-available tweets, by use of a web browser or by using Twitter's mobile app. Only persons who register with Twitter and create an account can tweet. Registration is free, but the user must submit an email address or telephone number. In addition, the user must agree to Twitter's Terms of Service (TOS). As discussed below, the TOS is actually a global set of rules defining the relationship of Twitter and the user, and includes express prohibitions on content based on child sexual exploitation.

Twitter uses its TOS because it believes it is important for users to understand the boundaries of permissible conduct. Twitter wants to ensure that users and the public understand it is working to maintain a safe environment.

It is important for Twitter's business that it is known to be aggressively inhospitable to persons engaging in child sexual exploitation. If people perceived this was not the case, they would no longer use the service. Twitter believes it could not exist if it allowed child sexual exploitation to exist on its platform.

Twitter's TOS tells users they retain rights to content they submit, including photos or videos. "What's yours is yours – you own your Content," the TOS explains. However, the rest of the TOS makes clear that these "rights" are limited; the assurance that users "own" their content appears in the section addressing the Twitter's ability to *publish* the information to third

parties. The user gives Twitter “a worldwide, non-exclusive, royalty-free license [to] make your Content available to the rest of the world.”

Not only does the TOS does not guarantee that Twitter will *retain* the content, it expressly warns storage may stop at any time:

Our Services evolve constantly. As such, the Services may change from time to time, at our discretion. We may stop (permanently or temporarily) providing the Services or any features with the Services to you or to users generally. We also retain the right to create limits on use and storage at our sole discretion at any time. We may also remove or refuse to distribute any Content on the Services, limit distribution or visibility of any Content on the service, suspend or terminate users, and reclaim users without any liability to you.

The TOS tells users they are “responsible for . . . compliance with applicable laws, rules, and regulations,” and warns that Twitter “reserve[s] the right to remove Content that violates the User Agreement.”

The TOS also contained a nonexclusive statement of the reasons it might terminate its services, although the language evolved slightly during this time. The TOS in effect until the end of 2019 provided:

We may suspend or terminate your account or cease providing you with all or part of the Services at any time for any or no reason, including, but not limited to, if we reasonably believe: (i) you have violated these Terms or the Twitter Rules and Policies or Periscope Community Guidelines, (ii) you create risk or possible legal exposure for us; (iii) your account should be removed due to prolonged inactivity; or (iv) our provision of the Services to you is no longer commercially viable.

After January 1, 2020, the TOS provided:

We may suspend or terminate your account or cease providing you with all or part of the Services at any time for any or no reason, including, but not limited to, if we reasonably believe: (i) you have violated these Terms or the Twitter Rules and Policies or Periscope Community Guidelines, (ii) you create risk or possible legal exposure for us; (iii) your account should be removed due to unlawful conduct, (iv) your account should be removed due to prolonged inactivity; or (v) our provision of the Services to you is no longer commercially viable.

The TOS also expressly states that, in its discretion, Twitter could disclose user content under certain circumstances:

We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.

The TOS does not stand by itself. It also expressly incorporates Twitter's Rules and Policies and its Privacy Policy. Section 3.3 of the Privacy Policy provides:

Law, Harm and the Public Interest

Notwithstanding anything to the contrary in this Privacy Policy or controls we may otherwise offer to you, we may preserve, use, or disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to protect the safety or integrity of our platform, including to help prevent spam, abuse, or malicious actors on our services, to address fraud, security, or technical issues; or to protect our rights or property or the rights or property of those who use our services.

Under the heading of "Safety," the Rules and Policies contains a list of prohibited actions, and includes the statement, "We have zero tolerance for child sexual exploitation on Twitter." The Rules link this statement to Twitter's "Child sexual exploitation policy" adopted in March 2019.

Twitter **has zero tolerance towards any material that features or promotes child sexual exploitation**, one of the most serious violations of the Twitter Rules. This may include media, text, illustrated, or computer-generated images. Regardless of the intent, viewing, sharing, or linking to child sexual exploitation material contributes to the re-victimization of the depicted children. This also applies to content that may further contribute to victimization of children through the promotion or glorification of child sexual exploitation. For the purposes of this policy, a minor is any person under the age of 18. (Emphasis in original).

The policy defined what content would constitute violations of the policy. After addressing how violations could be reported, the policy provides:

What happens if you violate this policy?

In the majority of cases, the consequence for violating our child sexual exploitation policy **is immediate and permanent suspension**. In addition, violators will be prohibited from creating any new accounts in the future. Note: when we're made aware of content depicting or promoting child sexual exploitation, including links to third party sites where this content can be accessed, they will be removed without further notice and reported to the National Center for Missing & Exploited Children (NCMEC). (Emphasis in original).

Finally, this policy on child exploitation links to Enforcement Philosophy, which explains that Twitter considers a number of factors in deciding how to sanctions violations of its rules, including the severity of the violation. On that issue, the policy states:

Certain types of behavior may pose serious safety and security risks and/or result in physical, emotional, and financial hardship for the people involved. These egregious violations of the Twitter Rules—such as posting violent threats, non-consensual intimate media, content that sexually exploits children—result in the immediate and permanent suspension of an account.

As noted earlier, Twitter believes its “zero tolerance” for child sexual exploitation to be vital for its business. This belief underlies the broad language in the TOS, which was written entirely by Twitter without government input. It is also behind Twitter’s actual enforcement efforts.

Twitter actively engages in the detection of child sexual exploitation. Anderson oversees a team of full-time Twitter employees who review content for violations of the policy against exploitation. The team reviews reports by other users of potential violations, which Twitter encourages and facilitates. Twitter also affirmatively seeks to detect potential violations through keyword association or by matching images or videos to known depictions of child sexual exploitation.

When the team receives a report of a potential violation, it conducts a comprehensive review of all the content posted by the account in question. A team member will view every image or media file posted by the account in tweet or profile form. The team may also review direct interactions and messaging between the reported account and other, following accounts. The team normally resolves reports within an hour, but in some instances it may require up to 24 hours to reach a conclusion. This review, and the ultimate conclusion, takes place without any input from law enforcement.

If team members determine an account has posted content which violates the policy against child sexual exploitation, Twitter “suspends” the account, Twitter jargon which essentially means the account is terminated. The account is locked so that no one outside Twitter—including the user—can access it or make changes to its content. The content itself is preserved by technical means, and Twitter may subsequently review the preserved material to help improve its detection efforts. Twitter considers its relationship to the user terminated, and purges the preserved data from its servers after 90 days.

Almost immediately after terminating the account, Twitter summarizes its findings in a CyberTip report to NCMEC. Twitter does not make reports directly to law enforcement organizations. In 2020, Twitter submitted 65,000 unique CyberTips.

A CyberTip is intended to be a comprehensive account of the violation that Twitter found on its servers. The tip includes image or video files which the Trust and Security Team has found to indicate exploitation, as well as a .zip compressed preservation file of the entire account.

Twitter includes the preservation file as a comprehensive snapshot of the account which might be helpful for further investigation. The preservation file includes not only content posted

by the user (including tweets and direct messages), but additional information such as IP logs and information about the user. This additional information is in a raw format which would not be viewable by the user.

Twitter alone decides what to include in the CyberTips. Neither law enforcement, the user, or the person reporting the apparent violation have any control over what information Twitter includes in a CyberTip.

Twitter explains in the NCMEC tips that it logs IP addresses for each session, which may last several days, rather than for individual tweets or messages. However, in the two tips in issue here, Twitter explains to the recipients that it has “provided an accurate log of IPs for the timeframe relevant to the report,” and gives recipients instructions (using simple cut, paste and find operations) to match up the violation to the IP address most likely associated with the session in which it occurred.

B. Defendant’s Twitter activity

Using a Yahoo email address, “jordanpatterson426,” Defendant created the “mikeyfromtumb11” Twitter account on August 26, 2019. On or about December 23, 2019, a user reported the account, and Anderson’s team conducted an investigation and found what they believed to be violations of the exploitation policy. Twitter suspended the account, preserved its information, and forwarded CyberTip 61606638 to NCMEC the same day.

Twitter attached six files to the tip: the .zip preservation file, one .mp4 movie file, and four .jpg image files. The CyberTipline form includes a field for the reporting Electronic Service Provider to answer the question, “Did Reporting ESP view entire contents of the uploaded file?”

The tip shows “Yes” for all of the files except the .zip preservation file, which shows only “Information Not Provided by Company.”

On December 31, 2019, eight days after his first account was suspended, Defendant used a Google Gmail variant of his earlier persona, “jordanpatterson3150,” to create a new Twitter account, “survivinglife8.”

After receiving a user report of the account for violating a policy other than child exploitation, Twitter suspended this account on February 27, 2020. Because the suspension was not related to exploitation, the account was not marked for preservation and purging.

However, the account was transferred to a Trust and Safety team within Anderson’s department after Twitter received a preservation request for the account from the Minnesota Internet Crimes Against Children task force.

This request from Minnesota did not ask that Twitter turn over the account’s content, and did not seek any subscriber information. The request did not even ask that Twitter search the account, or that Twitter respond. The Minnesota task force only asked that Twitter preserve the account.

Anderson’s team reviewed the account and found that it contained violations of the child sexual exploitation policy. This determination marked the account for preservation, started the 90-day clock for purging of account content, and generated a CyberTip to NCMEC.

Twitter noted in the “Additional Information” section of the tip that “[t]his account is part of an active law enforcement investigation,” and listed email and telephone information for an officer at the Minnesota Bureau of Criminal investigation. Twitter did not contact the Minnesota task force directly.

The CyberTipline Report issued April 28, 2020 has two attachments: a .zip compressed preservation file, and a .jpg image. As before, the tip does not indicate whether the ESP (Twitter) had viewed the entire preservation file, but indicates it had viewed the other media attached to the report.

Consistent with Twitter's policy, none of the records for either of the two accounts remain on its servers.

C. Detective Neal investigates the tips

Detective Sergeant Stephanie Neal has been an officer of the Wichita Police Department for 17 years. Before becoming a sergeant, she worked as a detective for the Internet Crimes Against Children (ICAC) task force of the WPD and Sedgwick County Sheriff's Department. In that role, she was assigned the first (mikeyontumb11) CyberTip on February 20, and the second (survivinglife8) on May 18 of 2020.

Consistent with her practice, Neal reviewed the media attached to the tips, and noted that they had been viewed by Twitter. She also reviewed the information in the .zip preservation file, including tweets and direct messages, and was able to match up postings to the exploitative media files that Twitter had reviewed and attached to the tip.

Neal noted that both accounts were registered from the same IP address, which indicated that the same person made both accounts. She also noted that the second tip indicated a 316 area code telephone number was associated with the registration.

Neal ran the phone number through department records, and found it belonged to Defendant, a registered sex offender.¹

Using this information, Neal obtained search warrants from the 18th Judicial District for the State of Kansas for information from AT&T, Cox Communications, Google, and Oath Holdings (Yahoo), as well as Twitter.

The AT&T and Cox warrants were premised on IP addresses from the CyberTips, and sought “subscriber and account information, including name and address, phone number, physical address for internet services, date account was created; any alternative contact information including email addresses.” The Google and Yahoo warrants sought similar information based on the “jordanpatterson” email accounts at those providers.

Neal testified that the purpose of the service provider warrants was to identify the user of the accounts. She did not seek to recover the content of any emails from those accounts.

The Twitter warrant sought a wide variety of information associated with another Twitter user’s account. Neal based the warrant request on a series of direct messages, found in the .zip preservation file, between the “survivinglife8” account and another user. These messages included sexually explicit photos and suggested that the account belonged to a minor. Information from the warrant led to the identification of the account owner, a minor, and Neal interviewed him on January 5, 2021.

As an alternative to the state search warrants, Neal could have contacted HIS Special Agent Jay Ferreira in her office and obtained a federal administrative subpoena. If the state court

¹ Defendant was convicted in 1989 in Sedgwick County District Court (No. 89-CR-777) of Aggravated Criminal Sodomy (with a minor), and in 1996 (No. 96-CR-739) of Aggravated Criminal Sodomy (with a minor), Aggravated Indecent Liberties (with the same minor), and Indecent Solicitation of a Child (with a different minor).

had declined to authorize the warrants, Neal testified she would have contacted Ferreira to seek HIS subpoenas for the subscriber information from the service providers.

After determining Defendant was actually communicating with a minor, Neal contacted Ferreira and engaged him to obtain federal search warrants for Defendant's home and place of employment. After the warrants were executed, agents found devices which were examined forensically, and Defendant was arrested.

While executing the warrants, Neal spoke with Defendant's roommate, Nathaniel Rabideau. Rabideau later called Neal to tell her that Defendant, while in custody, had called another person, Kim Betancourt, to ask her to hide some things for him that he believed law enforcement had missed. From her conversation with Rabideau, Neal came to understand that one of the missing devices was a white Galaxy Note cellphone. This device has never been recovered.

Neal told Rabideau she was not asking him to search, but that if he found the cellphone on his own, he should call her and she would pick it up. Rabideau later called Neal after locating additional devices, which Agent Ferreira picked up. A search of the devices pursuant to warrant found that they contained evidence of child pornography.

Neal then received another call from Rabideau, who related that Betancourt had been looking in Defendant's dresser and found a tablet. However, agents were not able to extract any information from it.

Defendant testified at the hearing. He stated that he did not read the Twitter TOS before creating his accounts. He later skimmed them, but never understood them. He testified he believed that because his account was set to private, only his followers would be able to see his posts.

Defendant acknowledged in cross-examination that his publicly-available Twitter biography stated, “I was on Tumbler many times & nuked.” Defendant testified that his account on Tumbler, another social media service, was actually terminated only once.

He also acknowledged that he created the “Jordan Patterson” account on Yahoo specifically so that he could register for Twitter. He agreed that the Yahoo email was “basically a fake account.” He later used a variation of that identity at Google because it was “easy to remember.” Defendant did not use these email addresses for any purpose other than registering with Twitter.

Defendant agreed that he created his second Twitter account because he knew the first had been “nuked, it’s been suspended and terminated.” Asked if he had abandoned the first account, Defendant testified, “Well, I couldn’t get on, so I didn’t know what I could do so I just went on.”

After he found he could no longer post to the second account, “I thought, okay, well I guess I’m done.”

II. Legal Standard

The Fourth Amendment of the U.S. Constitution provides in relevant part: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”² “The defendant has the burden of showing the Fourth

² U.S. Const. amend. IV.

Amendment was implicated.”³ “If the defendant meets his burden of establishing a warrantless seizure, the burden then shifts. The Government must establish the warrantless seizure was reasonable.”⁴ In reviewing a motion to assess, the Court will “assess the credibility of witnesses and determine the weight to give to the evidence presented; the inferences the district court draws from that evidence and testimony are entirely within its discretion.”⁵

III. Analysis

Defendant argues that Detective Neal violated his rights under the Fourth Amendment when she searched the preservation file without a warrant. He contends that this search violates both his reasonable expectation of privacy in the account content,⁶ and that it reflected a trespass to chattels, as recently articulated in *United States Ackerman*.⁷ Defendant further argues that the results of the state search warrants should be suppressed, because these warrants were premised on Neal’s unlawful search of the preservation file. The Government has advanced ten arguments why the Court should deny the motion to suppress.⁸

The Court finds that Detective Neal’s review of the preservation file was lawful because (1) under the circumstances of the case, Defendant had consented to Twitter’s broad TOS and

³ *United States v. Goebel*, 959 F.3d 1259, 1265 (10th Cir. 2020) (citations omitted).

⁴ *United States v. Shrum*, 908 F.3d 1218, 1229 (10th Cir. 2018) (citing *United States v. Carhee*, 27 F.3d 1493, 1496 (10th Cir. 1994)).

⁵ *Goebel*, 959 F.3d at 1265.

⁶ See *United States v. Jones*, 565 U.S. at 400, 406 (2012) (The Fourth Amendment protects against governmental searches that “violate a person’s ‘reasonable expectation of privacy’”) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)).

⁷ 831 F.3d 1292, 1307 (10th Cir. 2016).

⁸ At hearing on Defendant’s motion, the Government expressly stated it is not contending the search was valid under the third-party search articulated in *United States v. Miller*, 425 U.S. 435, 440-43 (1976) and *Smith v. Maryland*, 442 U.S. 735, 742-46 (1979). See *v. Ackerman*, 831 at 1304-05 (noting “lower courts have only begun to consider whether (and to what extent) the doctrine should be extended to email”).

Detective Neal reasonably understood that Twitter had the apparent authority to agree to her search of the preservation file, (2) Defendant lacked any reasonable expectation of privacy in the postings, (3) Defendant lacked any possessory or property interest in the accounts once they were terminated, and (4) Detective Neal reviewed the preservation file in objective good faith in light of applicable law and the circumstances of the case.

Given these conclusions, the Court need not resolve the additional arguments advanced by the Government, including its claims that the search was appropriate under the private search doctrine,⁹ that Defendant abandoned his Twitter content by failing to challenge his suspensions, that he had no subjective expectation of privacy in the content, that he should not be considered as within the class of persons protected by exclusion,¹⁰ or that any constitutional violation was too attenuated to the actual search to warrant exclusion.¹¹

A. Twitter authorized Detective Neal’s review

The Government argues that Detective Neal did not violate any rights of Defendant, because he agreed to Twitter’s broad TOS, and Twitter granted its consent for tip recipients to review the content of the account.

A governmental search will not violate the Fourth Amendment where its agent was granted permission to search by a party with actual or apparent authority over the area searched.

As the Tenth Circuit has observed:

⁹ See *United States v. Jacobsen*, 466 U.S. 109, 111 (1984).

¹⁰ See *Rakas v. Illinois*, 439 U.S. 128, 138, (1978) (recognizing that “misgivings as to the benefit of enlarging the class of persons who may invoke [the exclusionary] rule are properly considered when deciding whether to expand standing to assert Fourth Amendment violations”).

¹¹ *Utah v. Strieff*, 579 U.S. 232, 232 (evidence need not be excluded “when the connection between unconstitutional police conduct and the evidence is sufficiently remote or has been interrupted by some intervening circumstance”).

The doctrine of apparent authority holds that a search based on consent is reasonable under the Fourth Amendment even when the officer relies on facts that turn out to be wrong or incomplete so long as the officer's belief at the time of the search was reasonable. "[D]etermination of consent to enter must 'be judged against an objective standard: would the facts available to the officer at the moment warrant a man of reasonable caution in the belief' that the consenting party had authority over the premises?"¹²

Whether authority to consent to a search exists is determined from the totality of the circumstances.¹³

Here, Twitter's TOS are not private, but are publicly available.¹⁴ In addition, the Company Information section of the CyberTipline reports expressly informs recipients where to find Twitter's policies online, and also expressly states that the tips are made pursuant to 18 U.S.C. § 2258A.¹⁵ This statute authorizes an internet service provider who uncovers apparent child pornography to disclose information about the individual involved "to the extent the information is within [its] custody or control" and "at [its] sole discretion."¹⁶

As discussed above, the TOS gives Twitter broad authority to scan uploaded content and, where it receives a report of a potential violation of the child sexual exploitation policy, to review an entire account. If it finds a violation, the TOS provides that Twitter can disclose information from the account.

¹² *United States v. Romero*, 749 F.3d 900, 905 (10th Cir. 2014) (quoting *Illinois v. Rodriguez*, 497 U.S. 177, 188 (1990)).

¹³ *See United States v. Kimoana*, 383 F.3d 1215, 1223 (10th Cir. 2004)..

¹⁴ The relevant TOS's for 2019 and 2020, entered into evidence without objection at the hearing, are freely available online. *See* <https://web.archive.org/web/20191223004607/https://twitter.com/en/tos>.

¹⁵ The tips actually state, "This is being reported to NCMEC in accordance with Title 18 U.S.C. 22558A [sic]." Given the context, any experienced law enforcement officer reviewing the report would understand the reference.

¹⁶ 18 U.S.C. § 2258A(b).

The CyberTipline report reviewed by Detective Neal indicates that Twitter had used its authority under the TOS to actually review some content from the account and had found multiple violations. While the report does not indicate that Twitter had actually reviewed the entirety of the attached .zip preservation file, it includes express instructions on how to navigate the preservation file to match up IP address with particular tweets and direct messages. This information is essentially the key to Defendant's Twitter content, and the report invited Neal to step into its own broad authority to review that content.¹⁷ Thus, Twitter authorized the search.

B. Defendant lacked a reasonable expectation of privacy in the account

Courts in the District of Kansas have addressed the privacy expectations of social media users in several decisions. In *United States v. Ackerman*,¹⁸ the court held that the defendant had only a limited expectation of privacy in postings to AOL, because the platform's TOS required users to comply with applicable laws, and stated that AOL could take technical and legal action against him if he posted illegal content. In *United States v. Stratton*,¹⁹ the court reached the same conclusion, finding that the TOS of the Sony PlayStation Network, which warned users of potential monitoring and Sony's right to disclose illegal conduct to law enforcement, "explicitly nullified its users['] reasonable expectation of privacy." Other courts have also concluded that

¹⁷ See *Kimoana*, 383 F3d. at 1223 (even though third party "was not the registered property owner or renter" of motel room, he had apparent authority to consent to a search by law enforcement officers who "knew that [he] had a key to the room and that he had stayed there."). Here, Neal knew that Twitter had already searched through Defendant's room extensively (if not completely) and had then forwarded the key to the recipients of the tip.

¹⁸ 296 F. Supp. 3d 1267, 1272 (D. Kan. 2017).

¹⁹ 229 F. Supp. 3d 1230, 1242 (D. Kan. 2017).

social media users lack a reasonable expectation of privacy where the platform's TOS contain similar warnings.²⁰

In contrast, in *United States v. Irving*,²¹ this court held that a Facebook user retained a reasonable expectation of privacy in material submitted to that service. The court stressed that Facebook's TOS was substantially different from that of AOL's in *Ackerman* and of Sony PlayStation Network's TOS in *Stratton*. The TOS's of those providers expressly prohibited illegal activity, warned that accounts could be monitored, gave the provider the sole discretion to determine whether content violated the TOS, and warned that violations could lead to termination of the account and reporting of unlawful conduct. In contrast, the court wrote, Facebook's TOS did not expressly prohibit unlawful conduct and was silent about monitoring.

Furthermore, unlike the service providers in *Stratton* (Sony PSN) and *Ackerman* (AOL), Facebook did not terminate Defendant's account due to a violation of its TOS. Here, Defendant's account was active and viable at the time the government sought a search warrant. Indeed, at the time the government sought the search warrant, there was no indication that Defendant had violated Facebook's TOS.²²

Here, of course, Twitter had terminated Defendant's accounts, having manually reviewed content of the accounts and determined they were violations of the TOS, before it issued the CyberTipline reports to NCMEC.

²⁰ See *United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (“[I]f the ISP expresses an intention to ‘audit, inspect, and monitor’ its subscriber’s emails, that might be enough to render an expectation of privacy unreasonable.”); *United States v. Tolbert*, 2019 WL 2931659, at *4 n. 3 (D.N.M. 2019 (“due to the terms of AOL’s [TOS], to which he agreed, Tolbert lacked a reasonable expectation of privacy in his emails that contained child pornography”); *United States v. DiTomasso*, 56 F. Supp. 3d 584, 597 (S.D.N.Y. 2014) (defendant consented to email monitoring given AOL’s express policy of helping law enforcement).

²¹ 347 F.Supp.3d 615, 622-23 (D. Kan. 2018).

²² *Id.* at 623.

Twitter explicitly informs users that they are responsible for “compliance with applicable laws” in general, and specifically states that the platform has “zero tolerance” for child sexual exploitation. Twitter tells users that it “reserve[s] the right to access [and] read” user information to enforce the TOS. The linked Privacy Policy informs user that “we will store and process your [Direct Message] communications,” but notes that this processing “includes link scanning for malicious content, [including the] detection of spam, abuse and prohibited images.”

The linked child sexual exploitation policy of Twitter explains that any person, “whether they have a Twitter account or not,” may report a potential policy violation, using a form to explain what “led you to believe the account should be reviewed.” Thus, the TOS thus warns users that Twitter may scan individual communications, including direct messages for policy violations, as well as generally review an entire account if it receives a report of a potential violation of the child sexual exploitation policy.

Defendant has pointed to no decision holding a social media user enjoys a reasonable expectation of privacy where the platform deploys a similarly robust reservation of rights by its TOS. The Court finds under the circumstances of the case and in light of Twitter’s express zero tolerance policy for child sexual exploitation, once Defendant violated that policy, he lacked a reasonable expectation of privacy in the Twitter account.

C. The search did not interfere with any possessory interest of Defendant

In *United States v. Jones*,²³ the Supreme Court concluded that the Fourth Amendment prohibited not only government conduct infringing a reasonable expectation of privacy, but also conduct which interferes with a defendant’s lawful possessory interests. In *Ackerman*, the Tenth

²³ 565 U.S. 400, 409 (“[T]he *Katz* reasonable-expectation-of-privacy test has been *added* to, but not *substituted for*, the common-law trespassory test.”) (emphasis in original).

Circuit held that the “traditional trespass test suggested by *Jones*” could mean a seizure occurs when the government reviews “(presumptively) private correspondence” on social media.²⁴

The parties vigorously dispute the applicability of the property rights theory of *Ackerman* to the present case. Defendant has not cited, and the Court has not found, any decision actually applying the *Ackerman* property-based test to suppress a search of electronic communications. The Government contends that the analysis in *Ackerman* is dicta, and also notes that the cases cited in *Ackerman* as having “applied the common law’s ancient trespass to chattels doctrine to electronic, not just written, communications”²⁵ do not reach so broadly. Each of the cited cases indicate simply that the sheer volume of a user’s electronic messages may be actionable if they cause damage to the servers of an electronic communications provider; none address a claim of trespass by a person posting electronic messages.²⁶ Other courts have not broadly interpreted the trespass doctrine, and at least one court has agreed that *Ackerman*’s conclusion on the issue is dicta.²⁷

²⁴ 831 F.3d at 1307-08.

²⁵ *Id.* at 1308.

²⁶ See *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058, 1063, 1069 (N.D. Cal. 2000) (electronic auction site alleged injury from defendant’s automated electronic web crawlers, which sent 100,000 queries a day to plaintiff’s “servers [which] are private property”); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp.1015, 1023 (S.D. Ohio, 1997) (internet service provider alleged bulk spam emails of the defendant imposed “a tremendous burden on its equipment”); *Thrifty-Tel, Inc., v. Bezenek*, 46 Cal.App.4th 1559, 1567 (1996) (long-distance telephone company alleged defendants use of an automated hacking program seeking to obtain authorization codes reflected interference with its system, and the court noted that “defense counsel essentially conceded [defendants] trespassed”).

²⁷ See *Porters Bldg. Ctrs. v. Sprint Lumber*, 2017 WL 4413288, at *11 n. 15 (W.D. Mo. 2017) See also *Exeter Township v. Gardecki*, 2018 WL 6616930, at *4 (E.D. Pa. 2018) (noting *Ackerman* but concluding that electronic files would not constitute chattels under Pennsylvania law). Cf. *Intel Corp. v. Hamidi*, 71 P.3d 269, 300 (Cal. 2003) (trespass to chattels “does not encompass ... an electronic communication that neither damages the recipient computer system nor impairs its functioning”).

However, the Court need not resolve that issue, as even assuming in general a social media user may have hypothetical property right to data stored on that platform's servers, that right is so highly circumscribed here by the TOS that neither Twitter nor Detective Neal violated that right by accessing the data. Property and possessory right are not unlimited,²⁸ and they may be modified by contract.²⁹

The Tenth Circuit in *Ackerman* expressly noted that the defendant's reasonable expectations of privacy could be constrained by "the parties' dealings," including the defendant's acquiescence in the service provider's policies regarding child pornography, and remanded the case for further analysis, as these were "[f]acts that could well impact the legal analysis."³⁰ This is equally true for Defendant's trespass-to-chattels theory. That is, his voluntary consent to Twitter's broad TOS not only renders his claimed expectation of privacy unreasonable, it also sharply circumscribes whatever possessory interest he might otherwise have had in the preservation file.

Twitter did not guarantee or even offer the safe return of electronic "property" stored on its servers. To the contrary, the TOS warns users that no such right "right of return" exists. Under the TOS, Twitter reserves the right to stop providing services "at our sole discretion at any time." Section 3 of the TOS states: "We reserve the right to remove Content that violates the User Agreement. In Section 5, Twitter expressly disclaims "all responsibility and liability for . . . loss of data [and] the deletion of, or the failure to store . . . any Content." Twitter users "own"

²⁸ See *United States v. 16.92 Acres of Land*, 670 F.2d 1369, 1373 (7th Cir. 1982) ("It is axiomatic that property rights are not absolute.").

²⁹ See, e.g., *Geis v. Mathes*, 128 Kan. 753, 280 P. 759, 760 (1929) ("here, we must repeat, the ordinary rules of bailment law were superseded by the special contract" between the parties).

³⁰ 831 F.3d at 1305.

their content only in the sense that they can post it without losing whatever “title” they might have to it, but the TOS establishes that the content (and the entire account) can be deleted by Twitter at any time.

But Twitter not only warns users that it might vaporize an account at any moment, it was expressly informs them that it will “read, preserve, *and disclose* any information” it believed necessary to enforce and prevent violations of the TOS. (Emphasis added). To “disclose” means “to make known” or “open up to general knowledge,” especially “to reveal in words (something that is secret or not generally known).”³¹ A unilateral right to publish account content is inconsistent with either a reasonable expectation of privacy, or any exclusive possessory or property right.

With specific reference to “zero tolerance” child sexual exploitation policy, users are informed “the consequence . . . is **immediate and permanent suspension.**” (Emphasis in original). Not only will the account itself be deleted, users will be barred “from creating any new accounts in the future.” And exploitative content “will be removed without further notice and reported to the National Center for Missing & Exploited Children (NCMEC).”

Trespass to chattels requires proof that another intentionally interfered with a possessory interest “without authorization.”³² Similarly, the Restatement recognizes that a non-physical trespass to chattels arises where the “intermeddling with another’s chattel is done without his

³¹ Webster’s 3d New Int’l Dict. (1981) p. 645, col. 2.

³² *Turner v. Apple, Inc.*, 2022 WL 445755, at *5 (N.D. Cal. 2022). *See also Mohon v. Agentra LLC*, 400 F. Supp. 3d 1189, 1239 (D.N.M. 2019) (noting cases holding that “unauthorized and unwanted” spam telephone calls may constitute common law trespass to chattels)

consent and without any other privilege.”³³ By the same token, no claim for a trespass to chattels exists where a person has effectively consented to the alleged interference.³⁴

The TOS authorized Twitter to read and disclose the account’s content, once it received reports of potential violations of its child sexual exploitation policy. By violating that zero tolerance policy, it was Defendant who trespassed on Twitter’s servers.

D. Detective Neal acted in good faith

“[W]hen the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force and exclusion cannot pay its way.”³⁵ The good faith exception recognizes the need to balance the societal cost of exclusion and the need to deter wrongful conduct. “The extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct.”³⁶

Real deterrent value is a necessary condition for exclusion, but it is not a sufficient one. The analysis must also account for the substantial social costs generated by the rule. Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.³⁷

³³ Restatement (Second) of Torts § 217 (1965).

³⁴ *Id.* at § 252 (“One who would otherwise be liable to another for trespass to a chattel or for conversion is not liable to the extent that the other has effectively consented to the interference with his rights.”) *See Rajala v. Allied Corp.*, 919 F.2d 610, 632 (10th Cir. 1990) (citing § 252 in holding that consent barred debtor’s claim for conversion of two railroad cars of chemical resin under Kansas law, as there was no evidence the consent was fraudulently induced).

³⁵ *Davis v. United States*, 564 U.S. 229, 238 (2011) (citations and internal quotations omitted).

³⁶ *Herring v. United States*, 555 U.S. 135, 143 (2009)

³⁷ *Davis*, 564 U.S. at 237 (citations and internal quotations omitted).\

Thus, pursuant to the good faith exception, the Court may suppress evidence obtained in violation of the Fourth Amendment “only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.”³⁸

In *United States v. Angevine*,³⁹ the Tenth Circuit held that a university professor lacked any reasonable expectation of in data he downloaded from the internet onto the university’s computers. The reasonableness of a privacy expectation, the court held, “may be reduced by . . . legitimate regulation.”⁴⁰ Further, the court noted, the university had reserved the right to randomly audit internet use, had warned of consequences for illegal conduct, and seized the data from servers under its control.⁴¹

In concluding that the defendant had no reasonable expectation of privacy in material posted to the Sony PlayStation network in *Stratton*, the court found *Angevine* was applicable, even though the Tenth Circuit decision involved an employer-employee relationship.⁴² *Angevine* instructed the result in *Stratton* “because the Circuit considered whether the employer’s regulations reduced the employee’s expectation of privacy.”⁴³ Even though the relevant regulations in *Stratton* arose from a social media service’s TOS rather than an employment

³⁸ *Illinois v. Krull*, 480 U.S. 340, 348-49 (1987).

³⁹ 281 F.3d 1130, 1134 (10th Cir. 2002).

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² 229 F. Supp. 3d at 1242.

⁴³ *Id.*

contract, “[t]he same rationale applies.”⁴⁴ And in *Ackerman*, the court reached the same conclusion, summarizing *Stratton* as holding that “the rationale [of *Angevine*] applied equally to Sony and its users.”⁴⁵

At the time Detective Neal received and reviewed the CyberTipline reports and the Twitter preservation files, the Tenth Circuit in *Angevine* had expressly determined that, where restrictions on internet service use are explicit and robust, a user of those services “could not have an objectively reasonable expectation of privacy.”⁴⁶ Both *Stratton* and *Ackerman* recognized that *Angevine* was not limited to the employer-employee relationship, but “applied equally” to social media platforms and their users.

As noted earlier, the CyberTipline reports were expressly made pursuant to 28 U.S.C. § 2258A, which gives internet service providers discretion to provide information to NCMEC to identify users trafficking in apparent child pornography. Twitter’s “zero tolerance” and privacy policy and TOS are freely available online and also expressly linked in the Company Information section of the reports. As noted earlier, the TOS gives Twitter the right, upon receiving a report of a violation of its child sexual exploitation policy, to review an entire account and to disclose information from an account.

Detective Neal’s review of the preservation file took place in a good faith believe she was acting properly under the law and Twitter’s TOS. Because the review was not unlawful, the state search warrants were valid and there is not basis for suppression of the information obtained from those warrants. Further, as to the results of these warrants, the information appears to be

⁴⁴ *Id.*

⁴⁵ 296 F. Supp. 3d at 1272.

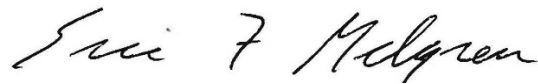
⁴⁶ 281 F.3d at 1135.

largely the narrowing of the search for and identification of the person behind the Twitter accounts. “Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”⁴⁷ The court finds that the results of the state search warrants should not be suppressed.

IT IS THEREFORE ORDERED that Defendant’s Motion to Suppress (Doc. 24) is hereby denied.

IT IS SO ORDERED.

Dated this 4th day of March, 2022.



ERIC F. MELGREN
CHIEF UNITED STATES DISTRICT JUDGE

⁴⁷ *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (listing cases).