Hate groups use of online social media has increased over the last decade. The online audience of hate groups is exposed to material with hateful agenda and underlying propaganda. The presence of hate across multiple social media platforms poses an important question for the research community: Do hate groups use different social media platforms differently? As a first step towards answering this question, we propose HateCorp: Cross-platform dataset of online hate group communication. In this project we first identify various online hate groups and their Twitter, Facebook, and YouTube accounts. Then we retrospectively collect the data over six months and present selected linguistic, social engagement, and informational trends. In the future, we aim to expand this dataset in real-time along with creating a publicly accessible hate communication monitoring platform that could be useful to other researchers and social media policy makers.

ACM Reference Format:

1 INTRODUCTION

The church shooting in Charleston, synagogue shooting in Pittsburgh, and New Zealand mosque shooting are just a few of the many incidents that have recently reinforced concerns about organized hate on social media. In a mounting number of hate crimes against various minorities, perpetrators sought support and publicized their actions on various social media platforms. Social media can enable efficient and fast communication for hate groups to exchange information [9] and spew radical beliefs and activism, amplifying what are otherwise fringe opinions [6]. To this date, the research community has not developed a strong understanding of how hate groups use social media to frame their messages and share information. To understand, we consider hate groups as Social Movement Organizations (SMO)—purpose-driven organizations with societal reconstruction agendas [15]. SMOs use social media for various purposes such as knowledge sharing, recruitment, collective action, and political advocacy [1, 2, 5, 11]. Moreover, SMOs also use different social media platforms in different ways—by providing thanks and recognition on Twitter, and soliciting feedback on Facebook [1].

A recent study claims that hate organizations do exist across multiple platforms, and looking at just one at a time might not be enough to understand the global ecosystem of hate [8]. Another study explores Twitter as a gateway into other hate communities and argues that some extreme right hate networks are evident only by considering their spread over multiple platforms [12].
While there is enough evidence that the online presence of hate groups spans across different platforms, there are no public datasets that capture the cross-platform activity. To bridge this gap, we pose two research tasks:

- **RT1**: Archiving the hate group communication posted publicly on various social media platforms
- **RT2**: Building a web interface that displays the latest trends in the collected data

Our research has implications in understanding the wider web activity of online hate groups and cross-platform content moderation. Researchers can use our trends platform to make inferences about how hate groups use different social media in different ways. Further, upon obtaining an Institutional Review Board (IRB) approval, this dataset can be used to build computational models to determine how the language of hate changes across various social spaces.

The rest of the report is organized as follows: First, we explain our data collection and validation process followed by the proposal of various trends to be observed. Finally, we conclude by outlining our future research directions and limitations.

2 **BACKGROUND**

2.1 **Identifying Hate Groups**

Ideas around freedom of speech online and a platform’s responsibility in restricting hateful communication are argued bilaterally. Moreover, the concept of "online hate" has many ethical, social, legal, and technical layers. Whether to consider an organization as hateful, ban their social media profile, or moderate individual messages is a debatable topic. Moreover, the perception that all messages by online hate groups are exclusively hateful is erroneous [10]. In this work, we instead focus on analyzing the overall pragmatic aspects of online communication by ideologically driven organizations that are labeled as hateful by the Southern Poverty Law Center (SPLC). SPLC is a non-profit social justice organization dedicated to monitoring hate group activity in the United States. Along with the names of the hate groups, SPLC also signifies the hate ideology they identify with. In this project we consider the following five ideologies:

- **White Supremacy**: We combine White nationalist, neo-Nazi, and neo-Confederate groups into a broader category of White Supremacy groups with overlapping views on white supremacy, far-right political ideology, and hatred towards other races.
- **Anti-Muslim**: Anti-Muslim groups show extreme hostility towards Muslims and Islamic countries, depicting Muslims as intolerant and violent.
- **Religious Supremacy**: We combine Radical Traditional Catholic, Christian Identity, and Black Nationalist groups into Religious Supremacy groups having underlying antisemitic and fundamentalist ideology. While there is a racial supremacy component in the black nationalist ideology, the descriptions of black nationalist hate groups provided on the SPLC website mainly stress their strong antisemitic and traditionalist attitude.
- **Anti-LGBT**: Anti-LGBT groups often consider homosexuality and pro-choice attitudes to be dangerous to society. While some Anti-LGBT groups view homosexuality and gender fluidity as unbiblical and anti-Christian, other groups claim that there is no scientific evidence that gender and sexual fluidity are inherent to humans.
- **Anti-Immigration**: Anti-Immigration groups strongly advocate for strict immigration policies and commonly target immigrants or individuals supporting immigration. Anti-Immigration ideology is rooted in the racist movement.

[1]https://www.splcenter.org/
After identifying the hate group accounts we proceed to map their social media profiles across platforms.

### 2.2 Mapping Social Media Accounts Across Platforms

We start by the hate group list published by SPLC in their *Hate Map* web page [3]. This list contains the names of 367 hate groups along with their ideologies. Next, we want to identify the social media accounts of hate groups across platforms. Previous studies have used computational matching techniques to identify cross-platform accounts of the same user [13, 16]. Such methods have a high likelihood of false matches. Hence, we decided to manually identify and verify the accounts for each of the 367 organizations as follows. First, we conducted web searches with the organization’s name to find their corresponding website. In most cases, the website had direct links to their social media accounts. In other cases, we searched the organization’s name within the search interface of social media platforms. We checked whether an account with a similar name exists and whether the account’s bio had a reference to the organization’s website. For every organization, we searched for their Twitter, Facebook, YouTube, Gab, Instagram, and Pinterest account profiles.

### 3 RT1 Method and Results

#### 3.1 Collecting Social Media Data

After selecting the hate organizations and mapping their accounts across platforms, we proceed to collect their social media data. Below we outline our method for collecting data across different platforms.

##### 3.1.1 Twitter

We collected the public tweets posted by the hate accounts using HTML page scraping. Our code was inspired by the GitHub repository of Henrique Jefferson [7]. We use Twitter handles to collect tweets and the metadata in a given time limit. Specifically, for every tweet we collected: the created timestamp, number of retweets, number of likes, tweet text, geotag, number of mentions, hashtags, tweet ID, and permanent link for the tweet. We retrospectively collected tweets from the specific handles between 1 April 2019 and 1 October 2019. This tweet collection process resulted in 50k tweets. We plan on continuing the tweet collection process in the future.

##### 3.1.2 Facebook

We used Facebook’s CrowdTangle API to collect the posts from public Facebook pages corresponding to the hate groups. CrowdTangle is a content discovery platform where

---

2https://www.crowdtangle.com/features
users can create lists of public Facebook pages and pull the data from public Facebook posts. We created the “SPLC” list on the CrowdTangle platform based on the Facebook page IDs collected in the last stage (see Figure 1). For every Facebook post, we gathered: created timestamp, number of reactions (likes, HAHA, love, etc.), number of public shares, post text, and the embedded links. Similar to the Twitter data, we collected Facebook posts between 1 April 2019 and 1 October 2019.

3.1.3 Gab. Gab is a recently developed social media platform mostly known for its right-wing user base. The site has been widely described as a “safe haven” for extremists including neo-Nazis, white supremacists, and the alt-right. The site was launched in 2017 and claimed to have almost 1,000,000 registered user accounts by July 2019. We use Gab Corpus that was published by Jason Baumgartner, the owner of the pusshif.t.io. The corpus contains a dump of Gab posts between 2016 to 2018 and is hosted on pusshif.t.io. In the future, we will work on getting real-time data to feed from Gab through its official API.

3.1.4 YouTube. YouTube is a social media platform to share videos and with the mission to “give everyone a voice and show them to the world”. We want to archive and study trends in the YouTube activity of the hate group organizations. For this, we used the Google youtube data API to get data on comments from videos. First, we had to get all the videos uploaded by the account or channel and then get all the comments on each video. Finally, our dataset contains video titles, descriptions, likes, shares, and timestamps for 25k videos uploaded by 69 hate groups. We also collected 621k comments on the videos that we do not use in this project. There was a limit on usage of the Google API on a per-day basis so we had to gather data for a couple of weeks.

3.1.5 Instagram and Pinterest. We did not have success in collecting Instagram and Pinterest data. There are only 3 accounts in Pinterest, which are less likely to produce any relevant insights.

---

3 Access to the CrowdTangle API is available through a Social Science Research Council Grant
4 https://twitter.com/jasonbaumgartne/status/1068610394992926720?lang=en
Fig. 2. Number of messages per account in all three platforms. All accounts have a very low number of YouTube videos. This intuitively makes sense as creating and uploading a video takes more commitment from the user compared to posting on Facebook or tweeting.

Fig. 3. Messages in Twitter and Facebook per ideology

Fig. 4. Distribution of messages per account. Facebook and Twitter distributions are similar.

Further, the Instagram API restricts data collection from apps that are not authorized by Instagram. Hence, we use only Facebook, Twitter, and YouTube data in the downstream analysis.

3.2 Summary of the Collected Data
We decided to use only Facebook, Twitter and Gab data for the downstream analysis as the majority number of hate organizations have accounts on all three platforms. Our final dataset has 50k social media data points of 58 hate organizations between 1 April 2019 and 1 October 2019. Figure 2 displays the number of data points per account. It can be observed that there are very few
YouTube messages compared to Twitter and Facebook. This difference propagates through all the trends observed. While we observe a large disproportion between YouTube data compared to other platforms, Facebook and Twitter have similar amounts of data. To compare the distributions, we perform paired statistical tests. First, we plot the number of messages per organization distributions for Facebook and Twitter (Figure 4). As the distributions are left-skewed, we perform the Wilcoxon signed-rank sum test—a non-parametric version of paired t-test—to compare the data distributions for Facebook and Twitter. Overall, there are a higher number of tweets compared to Facebook posts per group (283 vs. 203) but the overall distributions of messages per organization across the two platforms are not significantly different ($z = 574, p > 0.05$). We repeat the same rank-sum test to measure cross-platform distribution differences of posting activity within individual ideologies. We find no significant differences. This indicates that at its current stage, Facebook and Twitter datasets can be computationally compared without observing inherent bias in contributions by hate organizations.

### 3.3 Indexing the Collected Data with Elasticsearch

While the current dataset is smaller in size, we expect it to grow over time as we continue data collection in real-time. To enable fast access to large datasets, we utilize Elasticsearch. Elasticsearch is an open-source distributed, RESTful search and analytics engine, capable of solving a growing number of use cases. Elasticsearch employs a concept like map-reduce, where it has a master and slaves to work with big data. Elasticsearch is mostly used as a search engine. It also provides various analytic’s tools that work on big data. Elasticsearch indexes all the content that we pass it in a JSON format. It provides search results in a few seconds even for big data collections. For indexing, our Facebook, Twitter, and YouTube data consider only those fields that are common across all platforms. We perform several pre-processing operations before indexing the data.

#### 3.3.1 Text Cleaning

To enable word-based visualizations, we first need to clean the text of all punctuation, stopwords, and inline URLs. For this, we take each message in the dataset and split the words on whitespaces. We then remove words that are stopwords. Our list of stopwords is sourced from NLTK and ranks.nl. Next, we remove all punctuation and extract and remove URLs from the text. We use a combination of regular expression match and the text_cleaner package in Python to detect URLs and remove foreign language characters. We identify the URL domain names from the extracted URLs using Python’s tld package. We create a new data field titled as “Links” to record URL domains present in every message. We utilize the URL domains obtained to investigate information trends in the hate group data.

### 3.4 Final Fields in the Cross-Platform Dataset

Below we outline the fields used to index our data:

1. **Organization**: The name of the hate organization as obtained from the SPLC website.
2. **Ideology**: Ideology of the organizations as described in the Background section
3. **Text**: Text of the message cleaned using the steps explained above
4. **Links**: URL domains extracted from the links embedded in the text
5. **Replies**: Number of replies on Twitter and the number of comments on Facebook and YouTube for every message.

---

5. https://www.ranks.nl/stopwords
6. https://pypi.org/project/text_cleaner/
7. https://pypi.org/project/tld/
(6) **Reactions**: Number of likes for tweets and Facebook posts (Facebook posts also include different types of reactions such as HAHA, joy, love, etc.) and the number of upvotes for the YouTube videos.

(7) **Created UTC**: The epoch timestamp for every post calculated as the number of seconds since the epoch time (midnight 1/1/1970).

4 **RT2 METHODS AND RESULTS**

In this part of our project, we want to study the inferences from the collected data. How do hate groups frame their language differently across social media platforms? What type of information do they share across the platform? In this section, we explain linguistic, social engagement, and information trends in the hate group data. We build visualizations on Kibana. Kibana is an open-source data visualization system for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line, and scatter plots, or pie charts and maps on top of large volumes of data. We build basic surface-level trends on Kibana and also perform offline analysis for more complex methods. In the following sections, we explain the linguistic, social engagement, and informational trends separately.
4.1 Linguistic Trends

4.1.1 Surface Linguistic Trends. While there are sophisticated ways of analyzing text and narratives using Natural Language Processing (NLP), often, quick measures such as top used terms can be useful. Our eventual goal is to create a fast accessible online platform that can curate cross-platform hate group communication. Hence, we create a tag cloud visualization on the Kibana dashboard. In this report, we provide a sample of the aggregate word cloud (Figure 6). Such word clouds can be visualized for different ideologies at different time periods over various platforms. Additionally, we also include visualizations representing the top terms used by every ideology (Figure 7).

4.1.2 Deeper Linguistic Trends: SAGE. Sparse Additive Generative Models of Text (SAGE) is a generative text model that produces exclusively most and least frequent words in different groups of documents [4]. Unlike Multinomial Dirichlet distributions, SAGE distributions are added in logarithmic space. Usual topic models define the topic as distributions over words, however, in SAGE, topics are distributions over deviations from some background distribution over words. SAGE is especially useful in constantly evolving datasets—such as this—where a significant portion of the probabilities in LDA might not be well-calibrated. Agnostic to the actual semantic relationships of the words, SAGE also can be applied to text with hashtags and acronyms. We display the top 5 words in every ideology vs. platform category in Table 2. SAGE can be used to understand various linguistic styles. For example, in Table 2, Anti-Immigration groups discuss words more directly related to the immigration issue (customs, visa, etc) on Facebook. In contrast, on Twitter, the top terms correspond to common hashtags related to various information sources.

4.2 Social Engagement Trends

How does the general public respond to hate group content online? How does social engagement evolve over time? How do people engage with different ideological content on social media? To provide explanatory trends, we build several social engagement visualizations on Kibana that are explained below.

4.2.1 Number of Contributions. Overall, there are more contributions on Twitter compared to Facebook while YouTube has a lower number of contributions. The number of contributions grouped by platform (Figure 8) and ideology (Figure 9) are fairly consistent over the period of six months. The two spikes generated by Anti-Muslim accounts signify events around the Iran nuclear deal (May 2019) and remembrance of the 9/11 attack (September 2019). Such unusual spikes indicate...
that these cross-platform visualizations can be used to detect events that reverberate through social media across multiple platforms.

4.2.2 Number of Reactions. How do people react to social media posts/videos by hate groups? We create visualizations for observing trends in reactions over time. Figures 10 and 11 represent the count of reactions over time per platform and per ideology. While the number of reactions stays consistent throughout, it is of concern that on most dates, the accounts assimilate over 20k reactions per day. Consistent with the previous observations, Anti-Muslim accounts received a great number of reactions around the 9/11 remembrance day.

4.2.3 Number of Replies. We also build visualizations to understand dyadic communication between hate group accounts and their followers. Figures 12 and 13 represent the count of replies over time per platform and per ideology.

4.3 Information Trends
Apart from hosting messages rich with framings, social media also allows hate groups to share links to external sources. What different types of links are shared across platforms? To understand this, we plan on displaying link domain networks—a graph representation of URL domains shared within and across the platforms.
4.3.1 Domain Networks. Previous studies have utilized “domain network graphs” to understand the ecosystem of alternative news domains on Twitter [14]. A domain network is a graph-based representation of URL domains, where every domain is a node connected based on some predetermined criteria, such as the number of common users and frequency of sharing. We leverage the concept of domain networks and modify it to fit our analysis goals. We connect two domains (nodes in a graph) with an edge if they are shared by a hate group account. The edge weight
represents the number of accounts that share both the domains connected by an edge. We remove all edges with an edge weight less than two. Finally, for trimming the network graph, we remove all nodes that are shared less than 5 times and those that are connected with less than two other nodes. Next, to understand cross-platform sharing behavior, we color the edges differently based on the platforms they are shared on. We generate such domain networks only for Facebook and Twitter as links obtained from YouTube video descriptions are much smaller in number.

Figure 14 displays examples of information trends within various hate ideologies displayed using domain networks.

5 FUTURE WORK AND CONCLUSION

In this course project, we first identified cross-platform hate group accounts with various ideologies, collected and indexed their social media data over six months, and provided visualizations and analysis for various linguistic, engagement, and information trends. We see this project going in several directions. First, a real-time data collection pipeline can be built using Kibana and Elasticsearch to update the visualizations created every 15 minutes. This can give an overview of the latest trends in hate group activity online. Further, more complex machine learning models

<table>
<thead>
<tr>
<th>Facebook</th>
<th>Twitter</th>
<th>YouTube</th>
</tr>
</thead>
<tbody>
<tr>
<td>assembly</td>
<td>lol</td>
<td>sailor</td>
</tr>
<tr>
<td>Buchanan</td>
<td>right</td>
<td>vdale</td>
</tr>
<tr>
<td>race</td>
<td>red</td>
<td>Buchanan</td>
</tr>
<tr>
<td>Europe</td>
<td>friday</td>
<td>Wilson</td>
</tr>
<tr>
<td>Sailor</td>
<td>white</td>
<td>Steve</td>
</tr>
<tr>
<td>Comatlahworldwide</td>
<td>ilright</td>
<td>Mediafacebook</td>
</tr>
<tr>
<td>Tridentinemass</td>
<td>hourthe</td>
<td>Questionschurchmilitant</td>
</tr>
<tr>
<td>Catholiclife</td>
<td>leftism</td>
<td>Contactchurchmilitant</td>
</tr>
<tr>
<td>Orgonline</td>
<td>cbot</td>
<td>Tipschurchmilitant</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>catholicsaint</td>
<td>Churchmilitantcomwrite</td>
</tr>
<tr>
<td>Standinthegapradio</td>
<td>Somepeopleididosomething</td>
<td>Monthly pledged</td>
</tr>
<tr>
<td>Orgstore</td>
<td>Ilhanomarmustgo</td>
<td>Israeli</td>
</tr>
<tr>
<td>Published</td>
<td>Ilhanomarresign</td>
<td></td>
</tr>
<tr>
<td>Post</td>
<td>Hamastrormists</td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>Wither</td>
<td></td>
</tr>
<tr>
<td>Feast</td>
<td>Farrakhan</td>
<td>Hebrew</td>
</tr>
<tr>
<td>CfN</td>
<td>Remnant</td>
<td>Donate</td>
</tr>
<tr>
<td>Saint</td>
<td>Andrew</td>
<td>San</td>
</tr>
<tr>
<td>Iuic</td>
<td>Minister</td>
<td>Remnant</td>
</tr>
<tr>
<td>Saints</td>
<td>Cfn</td>
<td>Subscribe</td>
</tr>
<tr>
<td>Customs</td>
<td>Jxhnbindere</td>
<td>Studies</td>
</tr>
<tr>
<td>Verify</td>
<td>Fairblog</td>
<td>Matthew</td>
</tr>
<tr>
<td>Dan</td>
<td>Rmconservative</td>
<td>Fairs</td>
</tr>
<tr>
<td>Fairs</td>
<td>Washtimes</td>
<td>To</td>
</tr>
<tr>
<td>Visa</td>
<td>Dcexaminer</td>
<td>Dan</td>
</tr>
</tbody>
</table>

Table 2. Top 5 terms in each category resulting from Sparse Additive Generative Models of Text (SAGE)
Fig. 14. Domain co-sharing in [a] White Supremacy [b] Religious Supremacy [c] Anti-Muslim [d] Anti-Immigration and [e] Anti-LGBT accounts. Blue links represent exclusive co-sharing on Twitter, red on Facebook and green links indicate that the pair of connected domains is shared on both platforms. Domain label size corresponds to the number of times the domain is shared. breitbart.com and small cis.org are popularly shared on both platforms.

can be incorporated with the Kibana visualizations to have complex analyses such as SAGE and
domain graphs in near real-time. Further, by adding differential privacy to the data, this platform can be made public to be used by other researchers and enthusiasts.

REFERENCES


