

FIRST DRAFT'S ESSENTIAL GUIDE TO

Closed Groups,
Messaging
Apps &
Online Ads

November 2019

FIRSTDRAFT

TABLE OF CONTENTS

	Introduction	5
CHAPTER 1	Understanding ad libraries	13
CHAPTER 2	Facebook groups	21
CHAPTER 3	Closed messaging apps	27
CHAPTER 4	Ethical considerations	37
	Conclusion	43

ABOUT THE AUTHORS

Carlotta Dotto is a research reporter at First Draft, specialising in data-led investigations into global information disorder and coordinated networks of amplification. She previously worked with *The Times'* data team and *La Repubblica's* Visual Lab, and written for a number of publications including *The Guardian*, the *BBC* and the *New Internationalist*.

Rory Smith is a senior investigator at First Draft where he researches and writes about information disorder. Before joining First Draft, Rory worked for *CNN*, *Vox*, *Vice* and *Truthout*, covering various topics from immigration and food policy to politics and organized crime.

Claire Wardle currently leads the strategic direction and research for First Draft. In 2017 she co-authored the seminal report, *Information Disorder: An interdisciplinary Framework for Research and Policy*, for the Council of Europe. Previous to that she was a Fellow at the Shorenstein Center for Media, Politics and Public Policy at Harvard's Kennedy School, the Research Director at the Tow Center for Digital Journalism at Columbia University Graduate School of Journalism and head of social media for the United Nations Refugee Agency. She was also the project lead for the BBC Academy in 2009, where she designed a comprehensive training program for social media verification for BBC News, that was rolled out across the organization. She holds a PhD in Communication from the University of Pennsylvania.

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit

<http://creativecommons.org/licenses/by-nc-nd/4.0/>.

Introduction

IN 2016, THE SOCIAL NETWORKS, SEARCH ENGINES, NEWSROOMS AND THE PUBLIC WERE NOT READY FOR ELECTION-RELATED MISINFORMATION.

From the [headlines pushed by Macedonian teenagers](#)¹, to the [Facebook ads published by the Russian Internet Research Agency](#)², to the automated and [human coordinated networks pushing divisive hashtags](#)³, everyone was well and truly played.

Three and a half years later, there is more awareness of the tactics used in 2016, and measures have been put in place. [Google and Facebook changed their policies](#)⁴ making it harder for fabricated ‘news’ sites to monetize their content, [Facebook has built an ad library](#)⁵ so it’s easier to find out who is spending money on social and political advertising on the platform. [Twitter has become more effective at taking down automated networks](#)⁶.

It is unlikely, however, that the same tactics we saw in 2016 will play out in 2020. The technology companies have strengthened their policies and rolled out projects like the [Facebook Third Party Fact-Checking project](#)⁷ to down-rank false content in the newsfeed, and invested in additional engineering resources to monitor these threats. But those who want to push divisive and misleading content are devising and testing new techniques that won’t be impacted by the new platform developments.

While it’s impossible to know exactly what will happen in 2020, one of the most worrying possibilities is that

most of the disinformation will disappear into places that are harder to monitor, particularly Facebook groups and closed messaging apps.

Facebook ads are still a concern. One of Facebook’s most powerful features is their advertising product. It allows the administrators of a Facebook page to target a very specific subsection of people, like women aged between 32-42 who live in Raleigh-Durham, have children, have a graduate degree, are Jewish and like Kamala Harris’ Facebook page, for example.

Facebook even allows ad-buyers to test these advertisements in environments which allow you to fail privately. These ‘dark ads’ allow organizations to target certain people, but they don’t sit on that organization’s main Facebook page — making them difficult to track. Earlier this year Facebook rolled out their [Ad Library](#)⁸ which gives some ability to look at the types of ads certain candidates are running, or to search around a keyword like ‘guns’. We explain how to use the Ad Library later in this guide.

Another major threat is going to be damaging or false information leaked to newsrooms for political gain. In France, in the lead up to the Presidential election in 2017, documents purported to be connected to Macron’s financial records [were leaked 44 hours before the election](#)⁹. In France, a law prohibits news coverage of candidates and their supporters in this period and the French newsrooms agreed to stick with the law, meaning the leaked information did not get wider amplification.

In the US, the [leaking of emails connected to Hillary Clinton](#)¹⁰ and the Democratic National Committee staff and their publication in the weeks before election day took a different path. According to a study published in the [Columbia Journalism Review](#)¹¹ “in just six days, The New York Times ran as many cover stories about Hillary Clinton's emails as they did about all policy issues combined in the 69 days leading up to the election.”

An opinion piece in the New York Times by Scott Shane from May 2018, entitled [When Spies Hack Journalism](#)¹² is worth a read. As Shane writes: “The old rules say that if news organizations obtain material they deem both authentic and newsworthy, they should run it. But those conventions may set reporters up for spy agencies to manipulate what and when they publish, with an added danger: An archive of genuine material may be seeded with slick forgeries.”

Overall, the threats are going to move to places that are a lot harder to monitor. In 2020, there are a number of countries that will have a reason to try to impact the election, not just Russia. And while everyone likes to focus on foreign interference, domestic actors — either campaign operatives, zealots for certain candidates, or those just trying to cause mayhem for the sake of it — will be mobilized as well. And there will be an intersection. As the tech companies have cracked down on foreign entities paying for ads, and clues like a foreign IP address are a potential red flag, we're seeing the targeting of domestic actors and influencers as a way to push or amplify a message. So even if it looks domestic, it might have threads leading elsewhere.

If you haven't seen the New York Times' excellent documentary [Operation Infektion](#)¹³ about the ways today's information operations mirror those of the KGB in the 1980s and 1990s, it comes highly recommended.

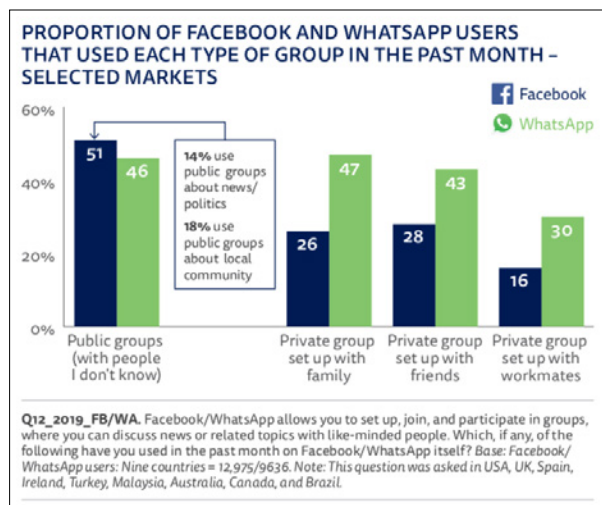
WHY ARE THESE DARK SPACES SO WORRYING?

In March 2019 Mark Zuckerberg talked about [Facebook's pivot to privacy](#)¹⁴. This description actually reflects what had already started to happen. Over the past few years people have moved away from spaces where they can be monitored and targeted. This is probably a result of users learning what happens when you post in public spaces, whether it's children growing up and complaining that they never consented to those baby photos being searchable in Google, or people losing their jobs after drunk or just ill-considered tweets, or realising that law enforcement, insurance adjusters and Border Protection Officers are watching what gets posted, or the disturbing reality of online harassment, particularly targeted at women and people of color.

Some people are turning their Instagram profiles to private, others are reading the Facebook privacy tips and are locking down the information available on their profiles, and there's [more self-censorship on Twitter](#)¹⁵. In certain parts of the world, regulation aimed at punishing those who share false information [might have a chilling effect on free speech](#),¹⁶ according to activists.

This shift is completely understandable, and we suspect historians will look back at the last ten years as a very strange and unique period where people were actually happy broadcasting their activities and opinions. The pivot to privacy is really only a transition back to the norm, having conversations with smaller groups of people, and those with whom you have a higher level of trust or affinity.

This graph from the 2019 Reuters Institute [Digital News Report](#)¹⁷ shows how many people currently rely on groups on Facebook and WhatsApp for news and politics.



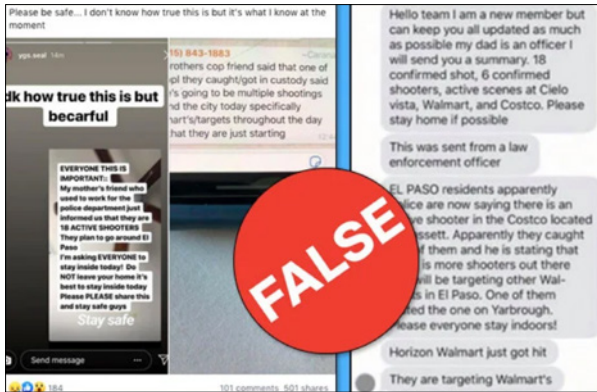
How Facebook and WhatsApp users rely on groups for news and politics.

However, for journalists attempting to understand what rumors and false information are spreading to play a role in refuting and hopefully slowing down the distribution, this shift makes things very difficult.

When information travels on closed messaging apps, whether that's WhatsApp, iMessage or FB Messenger, there is no provenance. There is no metadata. There is no way of knowing where the rumors started and how it has traveled through the network.

Many of these spaces are encrypted. There's no way of monitoring them with a Tweetdeck or CrowdTangle. There's no advanced search for WhatsApp. Encryption is a very positive thing. It's vital that as a society we have these types of spaces, but when it comes to tracking disinformation, particularly disinformation that is designed to be hidden, like voter suppression campaigns, it starts to become quite worrying.

Jane Lytvynenko from [BuzzFeed](#)¹⁸ regularly tracks rumors and falsehoods during breaking news events. As she watched events unfold during the mass shootings in El Paso and Dayton in mid-August 2019, she saw for the first time significant levels of problematic content circulating in closed spaces including FB messenger, Telegram, Snapchat and Facebook groups. She wrote up her observations in BuzzFeed.



Misinformation about the El Paso and Dayton shootings circulated in closed messaging spaces

This shift in tactics creates a number of new challenges for journalists, particularly ethical challenges. How do you find these groups? Once you find them, should you join them? Should you be transparent about who you are when you join a group on a closed messaging app? Can you report on information that you've gleaned from these groups? Can you automate the process of collecting comments from these types of groups? We'll tackle these challenges and more throughout this guide.

CHAPTER 1

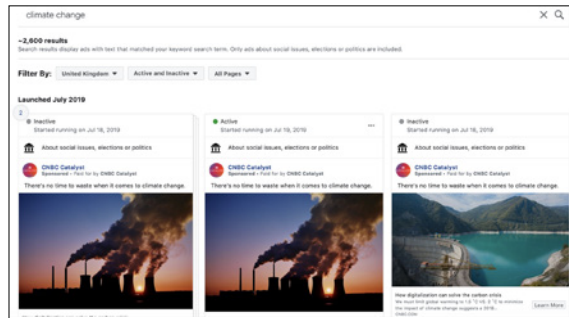
Understanding ad libraries

FACEBOOK AD LIBRARY

The Facebook Ad Library allows you to investigate advertisements running across Facebook products. The library grants anyone — you don't have to have a Facebook account — the ability to see active and inactive ads related to any topic.

For journalists and researchers, the tool offers unprecedented scope for monitoring and finding information about political advertisements around the world, including who is paying for the advertisements.

You can use the search function to find information about politics, elections or social issues. If you searched for “climate change” for example, the library would return a list of all active and inactive ads in the library which have run around the issue.

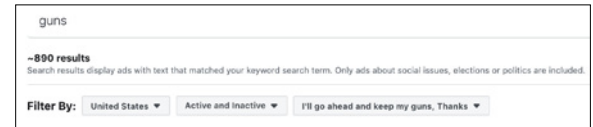


The Facebook Ad Library will show you a list of all active and inactive ads that have run around a particular topic

Clicking on each post gives you more detailed information, including who funded the advertisement, where it was shown, what demographic is targeted, and basic information on how much was spent on the ad.

You can combine your search with various filters to specify if you want to look at ads across the globe or in a particular country, and whether you want inactive or active ads or both. You can also search for keywords and then filter the results by specific Facebook pages.

For example you could search for guns and then limit the results to the page “I’ll go ahead and keep my guns, Thanks” to get insight into their advertising campaign and its financiers.



The Ad Library also allows you to limit search results by page.

Within the library there is also the Facebook Ad Library Report. Here you can get a general overview of all Facebook ads running around social issues, elections, and politics for different countries and date ranges. You can download these reports in CSV format for further analysis.

You can also access the Facebook Ad Library API, to get even more granular data or to build up your own database of Facebook advertisements. [Facebook published a guide](#)¹⁹ on how to install it and what you can do with it.

The library is not without its limitations. You can't access advertisements flagged as non-political once they are inactive, and the [API has been criticized](#)²⁰ for its bugginess, delivering incomplete data which might affect the reliability of your monitoring and research.

Also, make sure you turn off your ad-blocker when using the library — it may affect your searches — and be skeptical if your search doesn't return any results. If you try refreshing the page and performing the search again, you will likely get a new list of results.

GOOGLE AD TRANSPARENCY REPORT

Google launched their [Ad Transparency tool](#)²¹ in August 2018. It doesn't have quite the same functionality as Facebook, and right now it only works in the US, Europe and India, but it does hold ads on Google Ad networks, YouTube and other "partner networks".

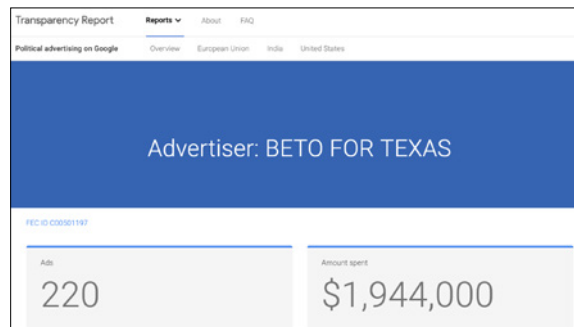
The database is updated weekly and contains information about ads running on Google which "spending on ads related to elections that feature a candidate for elected office, a current officeholder, or political party in a parliamentary system," according to Google.

The first thing you're met with when clicking through to one of the three regions is a map which breaks down the ad spend for each contested constituency: countries in the EU or states in the US and India.

Scrolling down further shows the different registered advertisers ranked by the amount they have spent and a library of all ads for the overall region. Users can explore these by date, ad spend, impressions and format.

Further down, it is possible to drill down into the top spending political campaign organizations, to see how much money they've spent and what the ads look like.

Users can also search through the library for each region by candidate or keyword and download data in a CSV format to explore further.



Google's Ad Transparency tool

TWITTER ADS

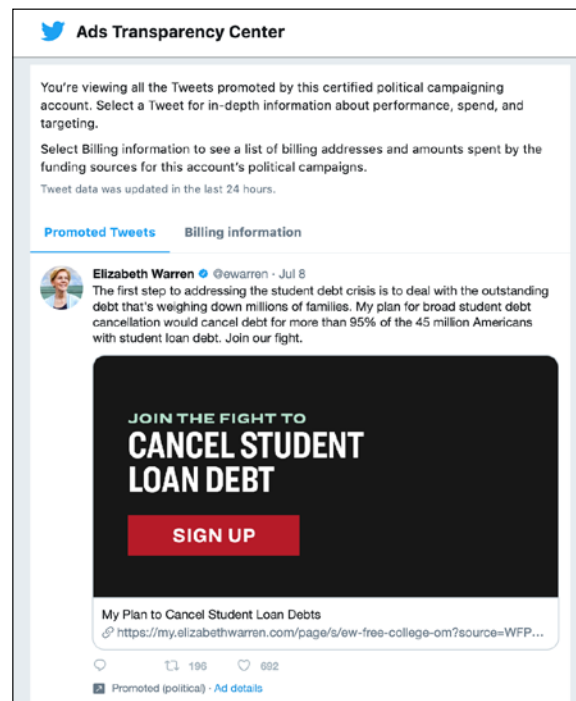
Editor's note: In the days leading up to the publication of this book, Twitter chief executive Jack Dorsey announced that the platform would ban political advertising around the world, starting from November 22, 2019. At the time of writing, the full policy has yet to be announced. Twitter's Ad Transparency Center allows any users to investigate ads currently posted on the platform, so we would be surprised if Twitter decided to abolish it entirely. We will update the book for a second edition if this is the case.

Twitter's Ads Transparency Center was also launched in the summer of 2018, and carries information about "political campaigning advertisers" in the US, EU, Australia, India and Canada, with separate legal definitions for each.

There are dozens of such advertisers in the database for the US and a US-only list for so-called "issue advertisers". There are between five and 20 political advertisers in the EU, India and Canada and just three in Australia. The site says Twitter requires political campaigning advertisers to "self identify", so it is not clear how complete these lists are.

While Joe Biden's official account is a registered political advertiser, Donald Trump's is not (or at least at the time of writing). So while we can see all of the promoted tweets from Joe Biden since he registered as a political advertiser on the platform, we can only see promoted tweets from @realDonaldTrump for the last seven days. Given Trump's natural reach on the platform and his position as the leader of the world's

most powerful country, one could argue that he doesn't need to pay for promotion. But, the way things stand, it is difficult to know whether he has.



The screenshot shows the Twitter Ads Transparency Center interface. At the top, it says "Ads Transparency Center". Below that, there is a heading: "You're viewing all the Tweets promoted by this certified political campaigning account. Select a Tweet for in-depth information about performance, spend, and targeting." There are two tabs: "Promoted Tweets" (selected) and "Billing information". Below the tabs, a tweet by Elizabeth Warren (@ewarren) is displayed. The tweet text reads: "The first step to addressing the student debt crisis is to deal with the outstanding debt that's weighing down millions of families. My plan for broad student debt cancellation would cancel debt for more than 95% of the 45 million Americans with student loan debt. Join our fight." Below the tweet is a large black image with white text that says "JOIN THE FIGHT TO CANCEL STUDENT LOAN DEBT" and a red button that says "SIGN UP". Below the image, the text "My Plan to Cancel Student Loan Debts" and a URL are visible. At the bottom, there are icons for retweets (196) and likes (692), and a label "Promoted (political) - Ad details".

Twitter's Ad Transparency tool

Tucked away quietly in the top right of the website is the Twitter Ads Transparency Center’s most powerful tool: A search bar which allows users to find any account and see the ads it has paid to promote in the last seven days.

If the advertiser has ‘self-identified’ it will show all ads run by the account since the database opened, and extra billing information on who paid for the ad, how much, and a tiny hyperlink marked ‘Ad details’ on the promoted tweet itself.

Clicking through here will show a surprisingly comprehensive campaign summary, including the targeted demographics and who actually saw an ad, where they live, their age, gender and language.

SNAPCHAT ADS

It’s worth mentioning Snapchat, who appear to have tried to get out in front of any potential criticism by making a public library of political and “advocacy” adverts.

The offering is basic but detailed. Users download a CSV of all such adverts for 2018 or 2019 and explore the data to their heart’s content, exploring the organizations, money spent, impressions, messaging, demographics, links and imagery associated with each ad.

There were only around 2,000 entries for the 2019 spreadsheet but it offers a precision of information missing in the other platforms discussed here.

CHAPTER 2

Facebook groups

At the end of April 2019, Facebook announced that it would be focusing much more heavily on Groups.



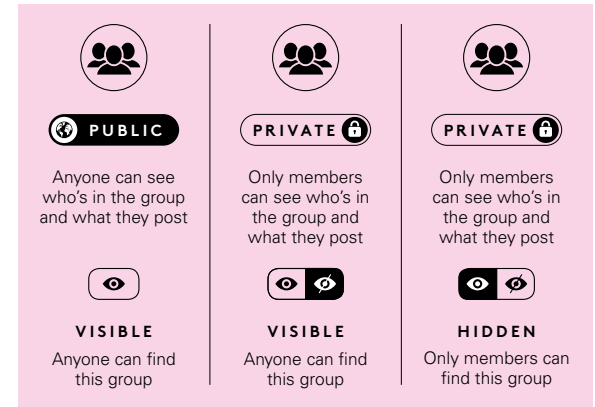
Mark Zuckerberg announced a refocus in 2019 on Facebook groups.

TYPES

There were three types of Facebook groups: Public, Private and Hidden.

The cheatsheet below helps explain the differences. Public and Private groups can be found in Facebook search but, if it's a Hidden group, you have to request to join and a group administrator will approve you, if they so wish.

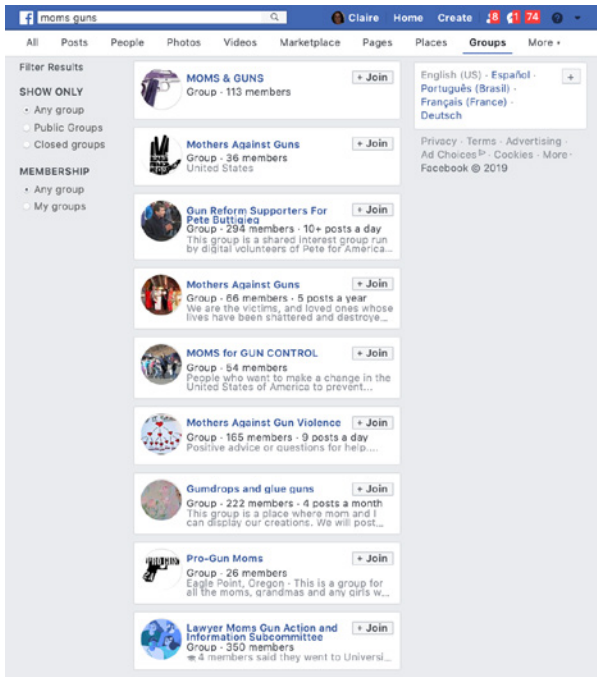
Sometimes these groups will ask you specific questions about your views and opinions, and/or will ask you to agree to confidentiality or code of conducts. (This can create ethical challenges for journalists, as discussed later in this guide).



Facebook groups: the three types.

HOW TO SEARCH THEM

You can search for Groups using the Facebook search. Below is a simple search for groups connected to 'Moms and Guns'. You can see in the results that Facebook reads Moms and also pulls out results that include the word mother.



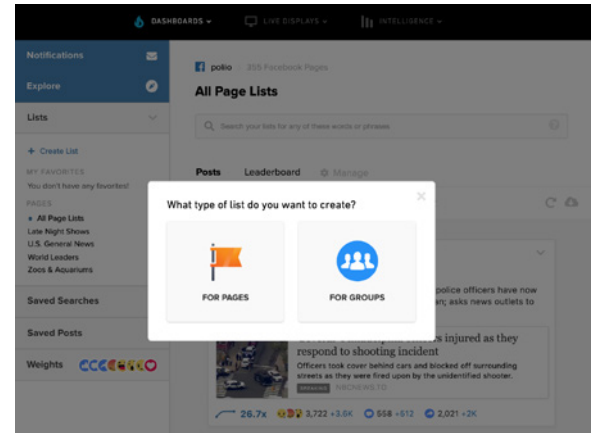
You can use Facebook’s native search bar to look for groups about a particular topic.

If you need to use more complex search operators, you can search in Google using something like “Moms AND guns” “el paso” site:facebook.com/groups

It’s hard to monitor Facebook Groups easily unless you use CrowdTangle, the platform Facebook made free for journalists in 2017.

In CrowdTangle you can set up lists of public Facebook and get regular updates on the more popular posts in the groups. CrowdTangle does not contain any public information, however, so private or hidden groups are only accessible on the main Facebook platform.

See First Draft’s Essential Guide to [Newsgathering and Monitoring on the Social Web](#)²² for more on this.



You can use CrowdTangle to set up lists of Facebook groups to monitor.

CHAPTER 3

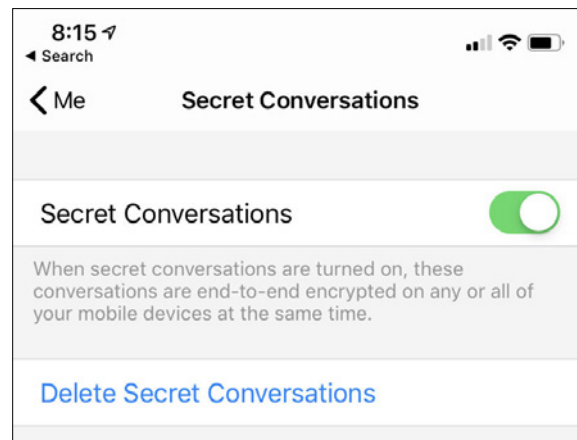
Closed messaging apps

The use of closed messaging apps is significant globally. There are over 1.5 billion users of WhatsApp and 1.3 billion users of Facebook Messenger. There are apps that are native to certain countries like KakaoTalk in Korea, and WeChat in China and then there are apps that are more popular in certain countries even though they're widely available, like Telegram in Iran, Viber in Myanmar and LINE in Japan.

The level of encryption differs, however. For example WhatsApp is encrypted by default whereas Telegram provides end-to-end encryption for voice calls and optional end-to-end encrypted “secret” chats between two online users, but not yet for groups or channels.

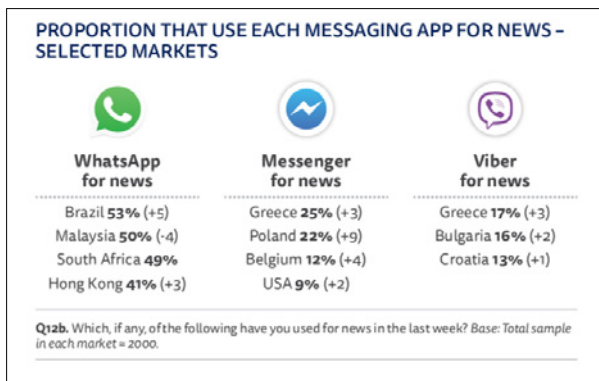
Other apps let you opt in for encryption. In the settings of Facebook’s Messenger app you can go to ‘secret conversations’ and turn on encryption there. This is important if you reach out to any sources via Facebook. Make sure they have also turned encryption on before you start talking to them.

If you really want to keep yourself and your sources protected, Signal is the app most security specialists recommend for journalists as it includes encryption and the option for messages to self-destruct after a designated period of time.



You can encrypt Facebook Messenger conversations by enabling “Secret Conversations.”

It’s easy to dismiss closed messaging apps as just another form of SMS, but it’s really important to understand that in many countries, and many communities, these spaces are used in very different ways. In the 2019 Reuters Institute Digital News Report, the number of people who use these spaces to consume news is interesting.



Popularity of closed messaging apps around the world.

WHATSAPP

WhatsApp is the most popular messaging app globally. With 1.5 billion users, the Facebook-owned messaging app is already the main messaging app in countries like Spain, Brazil and India. The addition of the app's group chat function has revolutionized mobile communication, quickly becoming one of the most popular tools to exchange information around protests, events and elections.

The closed nature of these groups along with WhatsApp's end-to-end encryption has thwarted many efforts by journalists and researchers to monitor the messaging

service. However, in the past few years several ways of tracking the service have emerged.

You can manually look for public WhatsApp groups on various platforms like Google, Facebook, Twitter, and Reddit, using the search term chat.whatsapp.com. You can join each group and monitor them individually. How you use information gleaned from these groups requires ethical considerations (see below).

There is a way to computationally monitor these groups, but it breaks WhatsApp's Terms of Service. You can scrape the web for publicly open WhatsApp groups related to your country or your beat. This technique has been used mainly by researchers²³ and it has started debates about the ethics of this approach²⁴.

The scraping and decryption methods outlined here raise serious ethical questions, specifically around privacy violations. Immense care, thought and planning should be taken by you or your organization before undertaking these techniques.

The simplest way of monitoring and researching WhatsApp for particular information is by establishing a tip line around particular topics, which can be sent to a phone in the newsroom. Depending on the quantity of tips and information, you may think about integrating it with Zendesk — a pay-for service — which allows you more flexibility in terms of how you organize these tips.

In Comprova, [First Draft's collaborative journalism project around the 2018 Brazilian election](#)²⁵, organizers created a central tipline 12 weeks ahead of polling day, and the project received over 200,000 tips from the public.

TELEGRAM

Telegram has similar functionality to WhatsApp, in that there are encrypted one-to-one chats and groups, but where WhatsApp limits groups to 256, Telegram's basic groups hold 200. Supergroups on Telegram can hold 100,000 people in a group.

The main difference from WhatsApp is that Telegram also has a functionality called channels, which allows a person or organization to 'broadcast' to an unlimited number of subscribers.

Telegram has gained a reputation as a favoured messaging platform of extremists. Once a home for supporters of so-called Islamic State, it has also seen an influx of extremists of other stripes in recent months as the major platforms crack down on activity which breaches their community guidelines.

DISCORD

Discord is real-time messaging app similar to Slack that is popular with gamers. Over the last couple of years, however, it has developed a reputation as a hub of conversation for political and social issues. During the

#MacronLeak it was possible to find people talking about tactics and techniques (as outlined by [this post](#)²⁶ by Ben Decker and Padraic Ryan at the time). There are also connections between those who use anonymous forums like Reddit and 4Chan, and you can find short links to Discord communities on these sites.

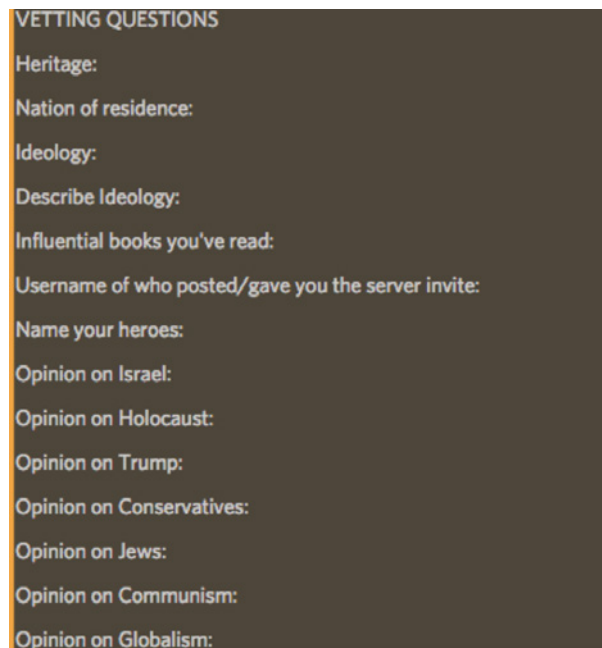
The service is organized by servers, also known as guilds. During the lead up to the midterms it was possible to follow conversations where people were coordinating in servers around particular campaigns or candidates.

In his 2018 [guide for journalists reporting from closed and semi-closed spaces](#)²⁷, former BBC Social Media Editor Mark Frankel describes Discord this way:

"For those less comfortable about talking in a fully open or public online forum, Discord provides an alternative outlet. Through my daily searches in different servers, I found that many individuals would share links to documents I hadn't seen on public websites and spoke freely about a number of subjects, from the Trump administration's attitude to child migrants to Supreme Court judgments and local gubernatorial races. In many ways, the platform hearkens back to those early days of the social web where largely anonymous groups hung out on MySpace, AOL, or Yahoo."

Some servers are open and anyone can join. Others require you to 'prove' your identity by linking to other digital profiles and will ask questions before letting you in, which is similar to some Facebook groups.

A screenshot included in Frankel’s guide gives you an example of one of these ‘vetting’ questionnaires.



Vetting questions on Discord

For journalists who want to spend time on Discord, we would recommend you use a VPN. We would also recommend having a conversation with your editor ahead of time about some of the challenges posed by being on the platform. While it is possible to lurk in these spaces, it’s necessary to think about the potential repercussions of publishing information sourced from these closed apps. Please see the ethical considerations section at the end of this book for more.

Two good, but slightly out of date guides are ‘[Secure Your Chats](#)’²⁸ from Net Alert and the [Guide to Chat Apps](#)²⁹ by Trushar Barot and Eytan Oren.

CHAPTER 4

Ethical considerations

Whether you are looking to understand the ideologies of potentially hostile groups or to write a human-interest story about a traditionally undercovered community, entering into closed groups and messaging apps presents various ethical, security and possibly even legal challenges.

This [ABC Australia write-up](#)³⁰ on the experience of a woman whose comment in a private Facebook group was picked up and amplified by the media is well worth a read, as a reminder of how small decisions by journalists can end up having a massive impact on those whose words are used.

Before you start your reporting, carefully go over your organisation’s existing policy about newsgathering in closed online spaces with your editor, the ethics and standards department and the legal team. If your newsroom does not have such a policy, consult with your editor, ethics and standards, and legal about the best way to go about your newsgathering.

A preliminary question to ask:

- Are there ways of obtaining the information you are seeking without entering into closed online spaces?

If the answer is no, we recommend moving on to the following questions. They weigh privacy and potential harm against public interest, and encourage you to think about proportionality:

- What do you hope to obtain from joining this group? Are you looking to find sources and tips,

or to gain background knowledge to inform your reporting? Or are the existence and the content of the group itself the focus of your intended story?

- Is this a group that would expect “lurkers”? Would members reasonably expect conversations and other content from these groups to be made public?
- What is the size of each closed group you are planning on entering, and how does that affect the expectation of privacy for each group? Group members may have a different expectation in a WhatsApp group consisting of 10 people than in a closed or secret Facebook group of 5,000 people.
- Would your writing a story expose group members to negative consequences?
- What is the public interest in your potential story?
- Are you planning on entering multiple groups? What is the minimum number of closed spaces you can enter into to find the information you need?

Next, consider whether you will use your true identity when entering the closed group, and whether you will affirmatively disclose your identity or merely refrain from concealing it.

Making these decisions responsibly requires both an understanding of the group you are entering and an

understanding of your own identity in relation to the group, weighing transparency against security:

- What is the purpose of this group? Is the group likely to be hostile, and how would group members react to a reporter within their midst? Entering a closed group that facilitates criminal activity or advocates extremist ideologies, for example, may lead to a different disclosure decision than entering a WhatsApp conversation consisting of local parents or a secret group of employees looking to unionize.
- Is your entry and presence in the group, using your real identity, likely to draw unwanted attention or abuse? Journalists of color and women, for example, may face additional security concerns when entering into certain potentially hostile groups, which may lead to a different disclosure decision.
- If you decide to enter the group using your real identity, to whom will you disclose this information? Will you disclose it to the group administrator, or to the whole group?
- When will you disclose your identity? Will you disclose when you first enter the group, when you find something useful in the group you'd like to include in your reporting, when you have completed newsgathering in the group, or when your story is published? If you plan on being in the group for an extended period, or the group gains new members after your initial disclosure, will you re-disclose your identity?

- Will you also disclose your reasons for being in this group?
- If the group requires you to answer certain questions before admission, will you answer these questions honestly?

Additionally, consider before embarking on this kind of reporting:

- Whether there are explicit confidentiality clauses in the community guidelines of the groups you are entering.
- How you are going to describe the methods of newsgathering in the resulting story.
- Whether you will go back into the group after the story's publication and share the information you have learned.

Whether you use your true identity or an alias, it is absolutely critical to discuss with your editors, and implement, digital security measures — particularly so when newsgathering in potentially hostile communities. The Committee to Protect Journalists' [Digital Safety tips](#)³¹ may be a useful starting point.

For an in-depth look into the ethical questions around entering non-hostile communities, we recommend [Mark Frankel's piece on the promises and pitfalls of reporting within chat apps and other semi-open platforms](#)³².

Conclusion

Information is moving into the dark. In 2020, we expect to see the greatest amount of information disorder in closed and semi-closed spaces. As monitoring capabilities grow in sophistication, those trying to spread disinformation will migrate to places where their tactics are harder to find and track.

Monitoring these spaces will be labor-intensive and require journalists to spend time locating and observing these places. It will also necessitate an industry-wide discussion about the ethics of this type of work.

Audience tiplines are one recommended approach to monitoring closed online spaces. This method requires newsrooms to build trust with their communities, and specifically audiences that are more likely to be targeted by coordinated campaigns of disinformation and voter suppression. During the lead-up to elections, it's vital that newsrooms think about ways to partner with community and grassroots groups, religious groups and libraries, in order to track what these communities see in Facebook ads, Facebook groups, WhatsApp and Messenger Groups.

Just as newsrooms had to prepare for the age of social media when tips, stories and sources suddenly became available in real time, we now have to prepare for the next era, when poor quality information — the rumors, hoaxes and conspiracies — disappear out of sight, away from those who can rebut and debunk.

ENDNOTES

- 1 Subramanian, S. (2017, February). Inside the Macedonian Fake-News Complex. *Wired*. <https://www.wired.com/2017/02/veles-macedonia-fake-news/>
- 2 Lapowsky, I. (2018, May). House Democrats Release 3,500 Russia-linked Facebook Ads. *Wired*. <https://www.wired.com/story/house-democrats-release-3500-russia-linked-facebook-ads/>
- 3 Bernstein, J. (2017, April). Never Mind the Russians, Meet The Bot King Who Helps Trump Win Twitter. *BuzzFeed*. <https://www.buzzfeednews.com/article/josephbernstein/from-utah-with-love>
- 4 Wingfield, N., Isaac, M. and Benner, K. (2016, November). Google and Facebook Take Aim at Fake News Sites. *New York Times*. <https://www.nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html>
- 5 Shukla, S. (2019, March). A Better Way to Learn About Ads on Facebook. Facebook Newsroom. <https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads/>
- 6 Roth, Y. and Harvey, D. (2018, June). How Twitter is fighting spam and malicious automation. Twitter. https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html
- 7 How is Facebook addressing false news through third-party fact-checkers? Accessed on October 30 2019. Available at: <https://www.facebook.com/help/1952307158131536>
- 8 Facebook Ad Library. Accessed on October 30 2019. Available at: https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=GB&impression_search_field=has_impressions_lifetime
- 9 Mohan, M. (2017, May). Macron leaks: the anatomy of a hack. BBC. <https://www.bbc.co.uk/news/blogs-trending-39845105>
- 10 Conger, K. (2017, February). John Podesta talks email hack, fake news and Russia. TechCrunch. <https://techcrunch.com/2017/02/08/john-podesta-talks-email-hack-fake-news-and-russia/>

- 11 Watts, D. and Rothschild, D. (2017, December). Don't blame the election on fake news. Blame it on the media. *Columbia Journalism Review*. <https://www.cjr.org/analysis/fake-news-media-election-trump.php>
- 12 Shane, S. (2018, May). When Spies Hack Journalism. *New York Times*. <https://www.nytimes.com/2018/05/12/sunday-review/when-spies-hack-journalism.html>
- 13 Ellick, A. and Westbrook, A. (2018, November). Operation Infektion. *New York Times*. <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>
- 14 Lapowsky, I. (2019, March). Facebook's Pivot to Privacy is Missing Something Crucial. *Wired*. <https://www.wired.com/story/facebook-zuckerberg-privacy-pivot/>
- 15 Toxic Twitter - The Silencing Effect. Amnesty International. Accessed on October 30 2019. Available at: <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-5/#topanchor>
- 16 Priday, R. (2018, April). Fake news laws are threatening free speech on a global scale. *Wired*. <https://www.wired.co.uk/article/malaysia-fake-news-law-uk-india-free-speech>
- 17 Reuters Institute Digital News Report 2019. Accessed on October 30 2019. Available at: <http://www.digitalnewsreport.org/>
- 18 Lytvynenko, J. (2019, August). The El Paso And Dayton Shootings Show How Disinformation Spreads On Messaging Apps. *BuzzFeed*. <https://www.buzzfeednews.com/article/janalytvynenko/telegram-disinformation-fake-news>
- 19 Facebook Ad Library API. Accessed on October 31 2019. Available at: <https://www.facebook.com/ads/library/api/?source=archive-landing-page>
- 20 Methods — EU Ad Transparency Report. Accessed on October 31 2019. Available at: <https://adtransparency.mozilla.org/eu/methods/>
- 21 Google Transparency Report. Accessed on October 31 2019. Available at: <https://transparencyreport.google.com/political-ads/region/US>
- 22 Dotto, C. and Smith, R. (2019). First Draft's Essential Guide to Newsgathering and Monitoring on the Social Web, London: *First Draft*. https://firstdraftnews.org/wp-content/uploads/2019/10/Newsgathering_and_Monitoring_Digital_AW3.pdf?x95059
- 23 Garimella, K. and Tyson, G. (2018, April). WhatsApp, Doc? A First Look at WhatsApp Public Group Data. Cornwell University. <https://arxiv.org/abs/1804.01473>
- 24 Wadhwa, V. (2018, April). WhatsApp public groups can leave user data vulnerable to scraping. *VentureBeat*. <https://venturebeat.com/2018/04/03/whatsapp-public-groups-can-leave-user-data-vulnerable-to-scraping/>
- 25 Burgos, P. Conter, G. Dias, N. Pimenta, A. and Wardle, C. (2019, June). An Evaluation of the Impact of a Collaborative Journalism Project on Brazilian Journalists and Audiences. *First Draft*. https://firstdraftnews.org/wp-content/uploads/2019/07/comprova_ING_web_OK_v5.pdf?x19860
- 26 Storyful Team (2017, May). Online 'Alt-Right' Attempts to Influence France's Electorate. *Storyful*. <https://storyful.com/blog/online-alt-right-wants-influence-frances-electorate-meme-wars-working/>
- 27 Frankel, M. (2018, July). The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. *The Nieman Foundation for Journalism*. <https://www.niemanlab.org/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/>
- 28 Open Effect, The Citizen Lab and Crandall, J. (2017, November). Secure your Chats! *Net Alert*. <https://netalert.me/encrypted-messaging.html>
- 29 Barot, T. and Oren, E. (2015, November). Guide to Chat Apps. Tow Center for Digital Journalism. *Columbia Journalism Review*. https://www.cjr.org/tow_center_reports/guide_to_chat_apps.php
- 30 De Poloni, G. (2019, August). How Perth vegan Zoe Callis got caught in viral media storm after a Facebook post. *ABC News*. <https://www.abc.net.au/news/2019-08-11/what-it-feels-like-to-be-caught-in-a-viral-media-storm/11385410?pfmredir=sm>
- 31 Committee to Protect Journalists (2019, July). Digital safety kit. <https://cpj.org/2019/07/digital-safety-kit-journalists.php>
- 32 Frankel, M. (2018, July). The promises and pitfalls of reporting within chat apps and other semi-open platforms: A journalist's guide. *The Nieman Foundation for Journalism*. <https://www.niemanlab.org/2018/07/a-journalists-guide-to-the-promises-and-pitfalls-of-reporting-within-open-and-closed-and-semi-open-platforms/>

ABOUT FIRST DRAFT

First Draft is a global, non-profit, non-partisan organisation that exists to help those on the frontline of reporting. We provide practical guidance and training that is informed by ongoing research. Skills, tools and recommendations are continuously tested and revised with the help of partners around the world.

FIRSTDRAFT

Supported by

Google News Initiative

@firstdraftnews

Learn more at firstdraftnews.org/resources