LXVIII

SIXTY-EIGHTH SESSION

BOARD OF FACEBOOK

BERKELEY MODEL UNITED NATIONS

WELCOME LETTER

Dear Delegates,

I would like to warmly welcome you to Berkeley Model United Nations' 68th session and to our committee, the Facebook Board of Directors! My name is Nikhil Pimpalkhare and I will be the head chair for this committee this year. I am currently a junior at UC Berkeley, majoring in Electrical Engineering and Computer Science with a minor in Logic. Last year, I was a head chair for BMUN 67's Interpol committee, and before that I was a vice chair for BMUN 66's Cybersecurity Crisis Committee. Outside of MUN, I enjoy rock climbing, playing chess poorly, and teaching computer science.

Facebook is a company with enormous societal impact, a company under heavy fire over numerous political and privacy-related scandals, and a product which many of you probably use on a daily basis. UC Berkeley is a proud Silicon Valley school, and so it's quite fitting that you, the delegates, will be facing some of the most interesting problems in technology right here. The main reason I am excited for this committee is because of the unique role you will take on. With varying ways to interact with the committee and your fellow delegates, the possibilities for corporate complications and diplomatic opportunities are endless. In addition, debating from the perspective of the board and upper executives of a technology company should give you an experience unique from most other Model UN committees. As you discover the nuances and intricacies of each of the following two topics, I hope you will share my excitement about having a committee centered around such interesting issues.

Allow me to introduce you to your vice chairs:

Hello, my name is Elle Mahdavi! I am a fourth year majoring in Political Economy and French. This is my eighth and last year of doing Model United Nations, as I did it all throughout high school and my time at Berkeley. I am so thankful for these past four years doing BMUN, and I'm sad to say this will be my last conference! Outside of BMUN, I have an on-campus job, I do research at the Human Rights Center, and I am in the midst of writing an Honors Thesis for the French department. The focus of my thesis is French immigration policy. If you have any questions about UC Berkeley, doing research in college, or good restaurants in Berkeley, please email me at elle.mahdavi@berkeley.edu! I'm excited to meet you all in March!

Hey Guys! My name is Deepak Ragu, and I am super excited to be one of your vice chairs for the Board of Facebook this year! I am a freshman at UC Berkeley, and I have done MUN for the last 4 years, where I've grown super passionate about the intersection of international politics with technology, as I've travelled to various conferences and met many interesting people by debating a wide variety of topics. Since this is a crisis committee, we will be using BMUN crisis procedure, and this committee will be fast paced in order to respond to the ever-changing tech climate. If you have any questions related to BMUN, MUN in general, or otherwise, feel free to send me an email at dragu@bmun.org or contact the BMUN secretariat. Happy Prepping!

I look forward to meeting each and every one of you in March and can't wait to hear the solutions that you come up with. Enjoy the process of discovering each of these topics and writing your position papers!

Best,

Nikhil Pimpalkhare

INTRODUCTION

In October 2003, a sophomore computer science student at Harvard University released facemash.com, a website based around showing the id pictures of every student at the school. Harvard had 13 distinct residential houses, each with different "face books", or student directories - Mark Zuckerberg sought to compile them into a single accessible website. Zuckerberg hacked into each online facebook and added its contents to his growing user database. His first use of this data? A "hot or not" game which asked players to compare two randomly selected photos and decide who was more attractive (Hall).

As of 2019, Facebook is one of the most popular social media platforms and most dominant technology companies in the world, boasting over 2.3 billion users. It is difficult to understate this company's impact on society - words like "friend", "tag", "like", "poke", and many more have been imbued with new meaning due to their usage on the website. Small businesses, advertising campaigns, and thousands of social groups are based around Facebook - it is fitting that the company's mission statement is "to give people the power to build community and bring the world closer together."

Facebook is also quite large, with roughly 35 thousand employees and more than 80 subsidiary companies (V, Ramzeen). Some of their most notable acquisitions include Instagram, a photo-sharing social media app, WhatsApp, a free cross-platform messaging service, and Oculus Rift, a virtual reality gaming console. It also has had significant influence on the wider technology community, creating several open-source tools such as React and PyTorch which are now the industry standard in their respective subdomains.

In this committee, you will represent the board and upper executive team behind Facebook. Although we, the chairs, will be representing Mark Zuckerberg, you will all be assigned critical positions at the helm of the company. This will be a crisis committee, which means that many of the subjects which you will be debating will be revealed to you during conference weekend. If a particular action is within your position's realm of influence, you will be able to submit a personal directive to perform that action. In accordance with reality, only board members will vote on committee-wide directives. However, non-board members will have the power to unilaterally pass personal directives regarding their domain of responsibility.

COMMITTEE POSITIONS

Mark Andreessen - a board member of Facebook. Also General Partner of venture capital firm Andreessen Horowitz, or a16z.

Erskine Bowles - a board member of Facebook. Previous White House Chief of Staff and previous president of the University of North Carolina system of universities

Kenneth Chenault - a board member of Facebook. Previously CEO and Chairmen of American Express

Susan Desmond-Hellman - a board member of Facebook. Also CEO of the Bill and Melinda Gates Foundation

Reed Hastings - a board member of Facebook. Also CEO and Chairman of Netflix.

Peter Thiel - a board member of Facebook. Also a co-founder of Paypal and Palantir Technologies

Jeffrey Zients - a board member of Facebook. Also President of The Cranemere Group

Chief Operating Officer - an executive position responsible for the day-to-day operations of a company, including operating budget and much of the tactical decision making.

Chief Financial Officer - an executive position responsible for a company's financial management and decision making

Chief Technology Officer - an executive position responsible for a company's technical and engineering-related decision making

Chief Information Officer - an executive position responsible for managing data security and infrastructure.

Chief Privacy Officer - an executive position responsible for aligning a company with privacy laws and regulations

Chief Revenue Officer - an executive position responsible for driving revenue growth

Chief Marketing Officer - an executive position responsible for managing marketing and product promotion decisions

General Counsel - the chief lawyer of a company's legal department

Head of Calibra - the leader responsible for decisions regarding Calibra, the Facebook subsidiary responsible for managing the new cryptocurrency, Libra. Also responsible for any blockchain related endeavors at Facebook.

Head of Instagram - the leader responsible for decisions regarding Instagram, the Facebook subsidiary app based around photo-sharing

Head of Facebook - the leader responsible for decisions regarding the Facebook web application

Head of Messenger - the leader responsible for decisions regarding Messenger, the Facebook messaging service

Head of Whatsapp - the leader responsible for decisions regarding Whatsapp, the Facebook subsidiary based around cross-platform messaging and voice communication.

VP of Growth - an officer responsible for driving acquisition of new customers

VP of Connectivity - an officer responsible for ensuring customers are able to get online at high speeds

VP of Mobile and Global Access Policy - an officer responsible for interacting with international laws regarding access.

VP of Partnerships - an officer responsible for creating mutually-advantageous partnerships with other organizations

VP of Global Communications - an officer responsible for interacting with international laws regarding communication.

VP of Infrastructure Engineering - an officer responsible for maintaining and developing Facebook's engineering infrastructure

VP of Product - an officer responsible for making new product design decisions

VP of Integrity - an officer responsible for maintaining data integrity and adhering to government regulation

VP of Product Design - an officer responsible for designing new products and adding to existing ones

VP of VR - an officer responsible for Facebook's suite of virtual reality products

TOPIC A: DIGITAL PRIVACY

WHAT IS PRIVACY?

A key implication of Facebook's massive user base and wide array of apps is that the company has a massive amount of user data - as of the second quarter of 2019, the platform has 2.41 billion active users (Noyes). Between Marketplace, Messenger, Instagram, Whatsapp, and a distributed network of tracking widgets on hundreds of websites, this company knows everything there is to know about its users' digital identities. While this trove of data is Facebook's secret weapon in designing personalized products, it is also its Achilles Heel - over the past 15 years, Facebook has been plagued by data privacy scandals which have endangered its users and eroded the public's trust in the platform.

Past Supreme Court Justice Louis Brandeis put it eloquently when he stated that privacy is "the right to be left alone." Privacy is a fundamental human right and involves enabling personal autonomy over one's information - we should be able to control "who knows what about us." Privacy is ingrained in most international documents concerning human rights; the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The same sentiment is echoed in the International Covenant on Civil and Political Rights (What is Privacy).

From a conceptual standpoint, privacy can be split into three realms: decisional, informational, and local. Decisional privacy involves protection of one's choices and opinions from others' awareness. It is particularly relevant in politically controversial decisions such as voting and media. This form of privacy could be endangered by reckless management of data. Informational privacy involves maintaining agency over information about yourself. This subcategory is especially relevant to this topic, because we are concerned with user data online. Local privacy is privacy in the physical sense - the right to not be watched or have your possessions monitored. This form of privacy is not particularly relevant to this topic (Roessler).

In the United States, laws concerning the use of the internet are outdated and sparse - when Zuckerberg testified before the Senate in April 2019, he faced dozens of questions from senators without significant background in internet-based companies and regulation - at one point, Zuckerberg even had to contest a conspiracy theory that Facebook uses people's microphones in order to gather data about their interests (Roose). The Federal Trade Commision is the main government body concerned with regulating the internet, but it's stated purview is to prevent "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce, or enforcing privacy policies in the market." The main legal documents concerning the internet are the Privacy Act of 1974, which establishes controls over what personal information the US government can store and disseminate, the Computer Fraud and Abuse Act, which criminalizes accessing and sharing protected information for third parties, and the Children's Online Privacy Protection Act, which mandates websites which collect information on users younger than 13 to comply with the FTC on management and use of that data (LII Staff). Even without much knowledge on how companies like Facebook gather, store, and use data, it's apparent that every legal control is either from a different century or not really related to what Facebook does.

FACEBOOK'S DATA COLLECTION

Advertisements are abundant and widespread from the moment you open Facebook. They litter the sidebar, are interspersed throughout the news feed, and divert you from your Farmville zen. Ads are absolutely critical to Facebook's business model, and are the primary source of its revenue. As Mark Zuckerberg said in an op-ed in the Wall Street Journal, "I believe everyone should have a voice and be able to connect. If we're committed to serving everyone, then we need a service that is affordable to everyone. The best way to do that is to offer services for free, which ads enable us to do." (Zuckerberg). A critical part of Facebook's ad platform is to leverage its massive trove of user data in order to show relevant ads to its users. From the advertiser's perspective, this allows them to target their ads to specific demographics and save money by only buying ad space for people likely to buy. From the consumer's perspective, if they are going to be shown an ad anyway, it might as well be relevant to their interests and desires (Korosec).

In this way, Facebook's competitive advantage as a place to buy ads is its large amount of user data, which it collects in various ways. Broadly, whenever you are using one of Facebook's products, the company is tracking personal information about you, including your name, school, and birthday; your network of friends, even those who have deleted their Facebook accounts (Korosec); and an activity log of every action you've made on the website since the inception of your account (Explore Your...). This tracking should not come as a surprise - pretty much every product-based company collects information about the usage of their product in order to improve it.

Where Facebook begins to differentiate itself from the brunt of technology companies is in tracking users when they are not on one of its applications. Facebook offers several services which other companies use in order to build their websites - when these components are loaded, Facebook also receives information about the user's usage of that site. Facebook tracks data whenever third party websites use social plugins like the Like and Share button, Facebook Login which allows you to log in with your Facebook account, Facebook Analytics which allows websites to get details about how people are using their website, and Facebook Ads, which allows outside websites to show ads from Facebook advertisers which are personalized to the user. Importantly, a given user need not click on a Facebook component to send information to the company - instead, simply by visiting the website, they are tracked (Baser).

What does tracking entail? Facebook records users' IP, or virtual address, operating system, browser information, and which website was visited. In many cases, Facebook is able to use digital "cookies" in order to identify exactly which device is being used, in a process known as "device fingerprinting" (Online Tracking). If Facebook noticed that you were reading dozens of articles about dog nutrition and health by tracking you across the web, then it might provide ads about kibble and dog toys when you return to Facebook.

WHAT THE TECH?: COOKIES

A "cookie" is a small piece of data which a website can store on your computer in order to allow the website to function in certain ways. Each cookie has a name, a specified website, and some associated data. Websites use cookies in order to maintain persistent state - in other words, websites are able to consistently recognize you as you, and perform actions that are relevant to you.

A good example is shopping carts on shopping websites. Suppose you put 2 different candles into your virtual shopping cart on an online candle store. Then, you accidentally close your browser window. Is all lost? No, because the store kept a cookie on your computer with information about which candles you had in your cart - it's name was "shopping_cart", and its associated data was "cinnamon#7, apple#2". Now, when you reopen the website, it still has the information about what you wanted to order.

Facebook uses device fingerprinting by randomly generating an identification number that is unique per user. Then, when you visit a website with a like button, the button is able to send your identification number to Facebook, along with which website it has been placed on. In this way, Facebook and other companies that track users across the internet are able to identify the person visiting the website.

This tracking information has significant benefits for the website involved. Websites are able to record information about how long its users spend on their site, what they click on, what ads they're interested in, and much more. By checking IP and other identifiers, they are able to tell which part of the world a user is from and translate to an appropriate language. Cookies are also critical for security, and allow websites to track who has logged in legitimately. According to one of Facebook's press releases, additional data only increases their competitive advantage - "We can also use the fact that they visited a site or app to show them an ad from that business – or a similar one – back on Facebook." (Baser).

DESIGNING IN PRIVACY

In this committee, delegates will be challenged with designing new services and refactoring current ones; as such, it is important to understand how to frame ideas such that they maintain the privacy and security of users. Although you will not need to understand all of the technical details involved, we hope that your solutions will implement the following principles. In order to break down the task, we will use the International Association of Privacy Professionals' Fair Information Practices Framework (Cavoukian) (Rubinstein).

1. Collection Limitation: This practice involves clearly defined limitations to what data is collect-

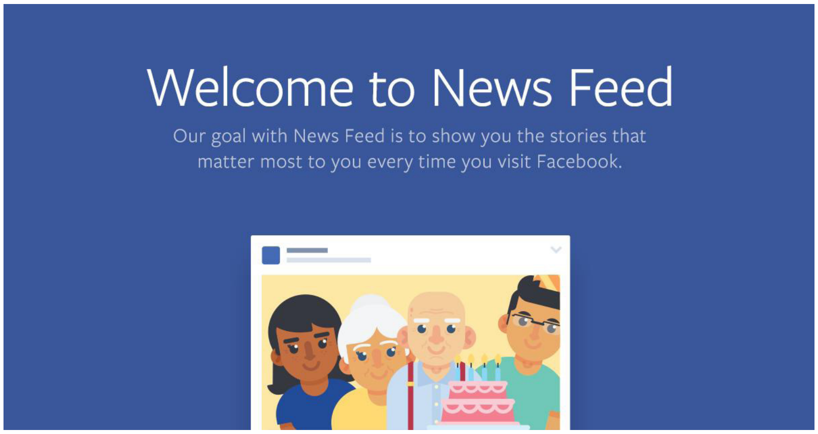
ed, stored, and used. For Facebook, this information is contained in privacy policies which users must consent to before using any products. It is important that such policies are thorough, exhaustive, and restrictive. Importantly, limitations should be the default - users should be able to use any product without customization and expect a certain level of privacy.

2. Data Quality: All personal information should be relevant to its use, complete, accurate, and current. Given social media's public nature, it is critical that any personal information is displayed responsibly.
3. Purpose Specification: Before a data is collected, the specific reasons for collecting that data should be clearly specified and documented. Any additional processing or developement upon that data should only be towards that previously stated goal. This principle frowns upon the creation of new products which leverage previously gathered data with a different purview.
4. Use Limitation: Personal data should never be disclosed in any public manner without either the consent of the user or the authority of the law. This is a critical security principle that should not be undermined in any case.
5. Security Safeguards: Building off the previous principle, this one states that personal data should be kept safe from unauthorized access, deletion, and modification. More broadly, the use of data should be kept secure constantly - a chain is only as strong as its weakest link, and so an application like Facebook is only as secure as its most vulnerable section.
6. Openness: All of these principles should be widely available, so that even the most technologically confused user can understand how their information is being used.
7. Individual Participation: This principle relates back to the idea of informational privacy - a user should have absolute control over their own participation in a database. They should be able to know if a website has data on them, be reasonably able to access that data, and be able to make appeals for the removal of data relating to them.
8. Accountability: The data controller should be responsible for the use or misuse of its data. In the case of Facebook, Facebook should be responsible for all usage of its data on users, including usage by third party applications.

A HISTORY OF FACEBOOK AND PRIVACY

Facebook has been plagued by privacy-related scandals since its inception. When Zuckerberg created Facemash, the first version of the app, in 2003, he did so by hacking into Harvard house databases without obtaining any sort of user consent or permission. Although the organization has become infinitely more careful and official, it has continued to face breaches in user data and other associated scandals. In this section, this paper will recount some of the most significant privacy events in this company's history, how the company responded, and the overall aftermath.

1. News Feed



Welcome to News Feed

Our goal with News Feed is to show you the stories that matter most to you every time you visit Facebook.

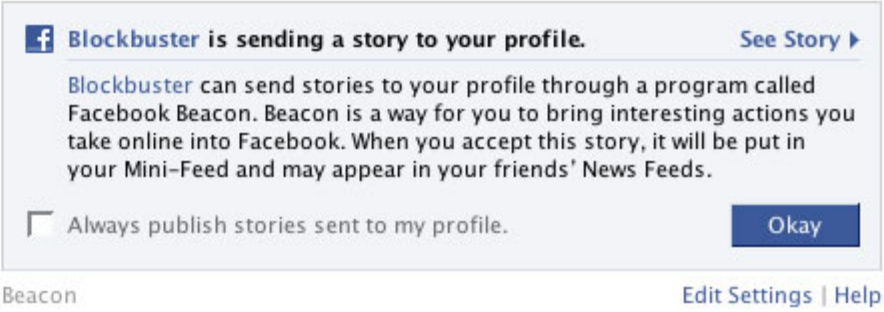
"News Feed" is the name for the modern home page of Facebook, the never-ending list of your friends' actions, your groups' posts, and Facebook's advertisements. Before the release of this feature in 2006, Facebook operated under a completely different paradigm - in order to catch up on what your friends were doing, you had to actively navigate to their "wall" and view their activities. News feed change the model from "pull" to "push" - instead of having to pull in information by navigating to your friends' pages, information about your friends was pushed towards you in the form of News Feed (Rubinstein).

One issue with News Feed was that it was released as opt-out - by default, users were involved. This idea goes against the previously mentioned Fair Information Practices - the purpose of data gathered about users changed from its original limited scope, and was now broadcast to all friends. In addition, releasing a feature as opt-out goes against the principle of user consent - in this case, users on Facebook had their data automatically surrendered to News Feed without explicitly enabling it.

Another issue with News Feed was its lack of privacy control. Facebook released the feature without fine-grained controls on what information was and wasn't broadcasted on News Feed, and also failed to release sufficient information about the privacy controls that users could customize. In terms of Fair Information Practices, this violated the Openness and Individual Participation principles, because users were not clearly informed on what they could control, and the mechanisms for control were loose.

Mark Zuckerberg quickly released a blog post, which he opened with "We really messed this one up." The CEO promised finer privacy controls and to be better in the future. In the end, fall-out from this incident was quite limited because the feature was so useful - News Feed was a great innovation in social media because it made it easier to catch up with your friends. Because of the feature's popularity, dissidence quickly died down, and the company was able to move on relatively scot-free (Arrington).

2. Beacon



Blockbuster is sending a story to your profile.

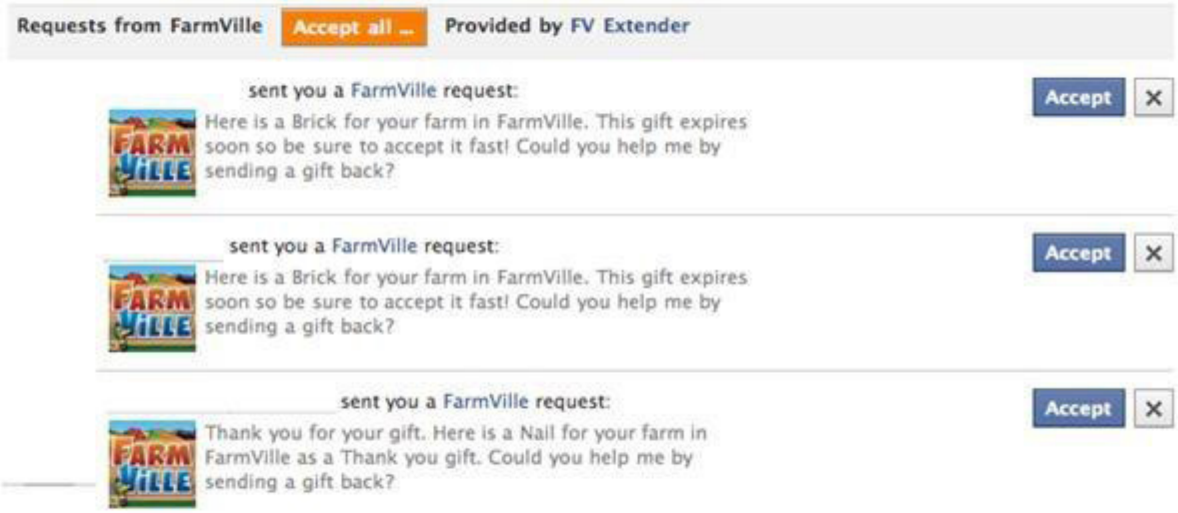
Blockbuster can send stories to your profile through a program called Facebook Beacon. Beacon is a way for you to bring interesting actions you take online into Facebook. When you accept this story, it will be put in your Mini-Feed and may appear in your friends' News Feeds.

Beacon was Facebook's new advertisement service, released in 2009. When users bought a product or clicked on an ad from one of Facebook's partners, details about the company would be broadcast to the user's friends through News Feed. The idea behind this feature was to utilize "word of mouth" advertising, as well as provide increased opportunities for exchange of information for its users (Rubinstein).

Like News Feed, the feature was released as "opt-out" - by default, users were enrolled in the feature. Releasing features as opt-out is a serious violation of privacy - when products change overnight without users explicitly consenting to new use of personal data, there is enormous potential for a privacy scandal.

Unlike News Feed, reception of this feature was extremely negative. Users voiced "concerns over the risk of embarrassment or the ruining of a surprise if activity at a partner website was shared with the wrong friend or at the wrong time." Facebook attempted to apologize, create a global opt-out setting, and eventually made the entire feature opt in, but the public view of the feature was already too negative (Facebook Shuts…). In 2008, around 20 users began a class action lawsuit that was settled for 9.5 million dollars. In 2009, Facebook formally removed the feature (EPIC).

3. Facebook Apps



sent you a FarmVille request:
Here is a Brick for your farm in FarmVille. This gift expires soon so be sure to accept it fast! Could you help me by sending a gift back?

sent you a FarmVille request:
Here is a Brick for your farm in FarmVille. This gift expires soon so be sure to accept it fast! Could you help me by sending a gift back?

sent you a FarmVille request:
Thank you for your gift. Here is a Nail for your farm in FarmVille as a Thank you gift. Could you help me by sending a gift back?

In 2007, Facebook released the Facebook Platform, a collection of tools and services that allowed developers to make third-party applications that could access and use Facebook's data about users. People could play games, message their friends, and even debate with others. Enabling third party applications massively increased the number of activities you could do on Facebook.

However, Facebook Platform was also released with some seriously destructive privacy vulnerabilities. One issue was that Facebook placed no limitations on the type of information third parties could request - a malicious app could ask for the sum total of a user's information on Facebook with one prompt. Furthermore, Facebook barely vetted the developers it allowed onto its platform - as a result, the platform hosted a large number of largely anonymous developers with extremely permissive use of Facebook data (Rubinstein).

Another issue was that users were poorly informed on what agreeing to such prompts entailed. Many would simply click through the prompts without reading them in order to install the app. The apps were often all or nothing - if you didn't grant them access to your profile, you wouldn't be able to use them at all. For others, it was unclear what third party applications could do with your data once it was shared - many wrongly believed that third parties would be subject to the same privacy policy controls as Facebook. Instead, such apps were able to sell user data to think tanks, advertising agencies, and other organizations without users really understanding what was going on. Finally, a particular user giving consent to a third-party application gave the app access to a lot of information about their friends. The result was that a third-party could have gathered data about you and sold it to a third party without you ever interacting with their app (Rubinstein).

Facebook responded by limiting the information that third-party developers could access and creating a privacy dashboard to give users visibility into what data apps could access about them. A common theme throughout Facebook's history is designing in privacy retroactively, initially sacrificing it for the sake of rapid innovation and experimentation. The company has thrived thus far because more of its features have been well-received than not, and that many view social media leaks as relatively nonconsequential, at least as compared to political or financial leaks. However, the practice of release to scandal to band-aid fix is risky and irresponsible, and as Facebook's capabilities increase, it is increasingly important for the company to consider data privacy before release (EPIC).

4. Photo Sharing

Lois Lane
Just now ·
Charming as always~
Thanks Jimmy for the pic!
Like
Comment
Share
Set as Background
Write a comment...
Want to tag Clark Kent?
Yes · No
facebook.com/
NKISDRAWING

Facebook allows "tagging" on all of its photos, where different users can be linked to a photo that they are pictured in. Tagging is also prevalent on Instagram, where links to user profiles can be scattered across an upload. Tagging is interesting because it changes the scope of the image - if you are tagged, not only do you receive notifications about activity on that photo, but your unique friends are also shown the picture, increasing the audience of the post (EPIC).

Privacy issues arise when unflattering, unprofessional, or otherwise embarrassing photos are uploaded and users are tagged. The issue is exacerbated by the fact that the uploader of the photo, the user who tags someone in the photo, and the user who is tagged in the photo can be three separate people with three different opinions about what should be done with the picture. The dispute can quickly become very difficult to resolve, and involves determine who has digital ownership over what (Rubinstein).

Facebook also has facial recognition technology which scans uploaded pictures and generates suggestions on who is contained in the upload. In the past, Facebook would automatically tag users, but after complaints, changed it to a suggestion system. A serious issue with this feature is that regardless of whether or not the uploader has facial recognition enabled, Facebook will run facial recognition on the upload so that it can provide suggestions to other users. This is a serious problem because Facebook is scanning photos and extracting user data without affirmative consent. This has serious consequences in Europe with the EU General Data Protection Regulation (GDPR), and Facebook is even facing a lawsuit in Illinois over this issue (Singer).

THE CAMBRIDGE ANALYTICA SCANDAL

Cambridge Analytica gained access to the data of many Facebook users who consented to use the app "thisisyourdigitallife" and also the data of those users' Facebook friends. The app was developed originally by Aleksandr Kogan, a data science professor at Cambridge University. Kogan allowed Cambridge Analytica to have access to all the Facebook data the app had access to; however, this action was a violation of Facebook's terms of service for third-party institutions that use Facebook login for their app (Wagner). As users of the app agreed to login via Facebook, Cambridge Analytica obtained access to 97 million Facebook users' data, including their "likes", locations, photos, and statuses. In this case, there was also an issue of informed consent as users did consent for the app to have access to this information but under the guise that this app served the purpose of an academic survey. They did not directly consent to having their data shared with a third party that intended to sell their data to political campaigns and causes. Although the data collection and illicit sharing of the data began in 2014, Facebook did not suspend Kogan or Cambridge Analytica until 2018 when the scandal broke out. Cambridge Analytica used this data in advising U.S. presidential candidate Ted Cruz and President Trump during the 2016 campaign cycle (Rosenberg). As well, politicians from the UK solicited Cambridge Analytica to gain insight on the 2016 Brexit vote (Mayer), while politicians from Mexico did the same for the 2018 presidential election (Ahmed). Cambridge Analytica analyzed the data for these users into a profile in which campaigns could target specific ads to. In 2015, Facebook updated its terms of service to not allow third parties to have access to the data of the Facebook friends of users who use these apps; however, Cambridge Analytica already had access as "thisisyourdigitallife" was active since 2014. After the outbreak of the scandal, Facebook pledged to implement data privacy laws required by GDPR in the EU all around the world (Schulze). In July 2019, the Federal Trade Commission found Facebook guilty of violating a 2011 FTC-Facebook agreement, as Facebook failed to gain "express consent" from its users in regards to the Cambridge Analtyica scandal, and decided to fine Facebook $5 billion (Facebook to...). The 2011 agreement arose after the FTC found Facebook violating their user data agreement nine years ago. The FTC found the Cambridge Analytica case as a violation of this agreement, where Facebook promised to uphold certain standards with user data. This is the largest fine imposed on a tech company in the U.S., surpassing the $22 million fine levied on Google in 2012 (Kang). For the EU, however, this size of a fine has been imposed on tech companies in the last few years due to violations in market regulations. This ruling by the FTC does not include any provisions regarding how Facebook should handle user data. Due to the lack of such provisions in the final ruling, two democratic members of the FTC actually decided to vote against it believing it did not go far enough to ensure that Facebook will avoid this type of oversight in the future. After news of this ruling broke, Facebook's share rose 1.8%.

KEY GOVERNMENTS

In 2018, the European Union implemented the General Data Protection Regulation, or GDPR, which is widely considered to be one of the most critical pieces of data privacy legislation in the world today. The brunt of the agreement concerns establishing a minimum threshold of data protection law in the EU which all nations within the organization must implement. The overarching goal is to standardize data privacy laws and make data transfers across European borders easy, because the data is already stored in an acceptable format. One key tenet of the act is maintaining affirmative user consent before any collection of data. This agreement is important for Facebook because it has a significant number of users in the EU, and because it is an international company which regularly transfers data across borders. Importantly, the GDPR affects transfer of user data in and out of the EU - the regulation vaguely states that other countries must have "adequate data protection". Facebook must adhere to such regulations in order to avoid significant fines and legal troubles in Europe (Fromholz).

Facebook is based in the United States, and thus the nation's privacy laws are of great importance to the operations of the company. The main regulatory body which Facebook interacts with is the Federal Trade Commission, or FTC. As mentioned earlier in the synopsis, laws concerning data collection and use are nonspecific and antiquated - in general, government use of personal data is governed far more strictly than private company use of personal data. Without any real overarching internet privacy law, the US has significantly fewer regulations (Fromholz).

KEY COMPANIES

Google is similar to Facebook when it comes to privacy concerns and scandals. Originally based around a search engine for the internet, this massive technology company has influence in pretty much every field, including email, mapping, developer tools, and much more. Google has faced numerous scandals over its lifetime, and is even facing some today. Just like Facebook tracks users across the web, Google tracks users across its suite of apps, generating profiles for each user that it can use to personalize ads (Nield). In addition, Google Chrome, Google's web browser, is designed to enable web tracking with cookies, which both Facebook and Google use. Competitor web browsers like Mozilla's Firefox have created "containerized tabs", a technological solution to prevent web tracking (Fowler).

On the other side of the battle for user privacy is Apple, the technology giant behind the

MacBook and the iPhone. In the past year, Apple has been on a serious privacy tear - in January 2019, Apple redacted Facebook's licence to publish apps to the iPhone App Store after they tried to release a market research app which would pay users to allow Facebook to monitor every action taken on their phone (Chong). Additionally, Apple recently announced "Sign In with Apple", a new sign in service that is designed with user privacy in mind. Apple is also compelling all apps on its App Store which offer "Sign In with Facebook" or "Sign In with Google" to also include their sign in option. (Kovach)

QUESTIONS TO CONSIDER

1. What regulations, if any, should be placed on Facebook's data storage and usage?
2. Even if Facebook were to never have a scandal again, it would take years for public opinion to organically shift in its favor. How can Facebook address widespread public distrust?
3. Facebook prides itself on being a technology company, and its research division explores the furthest reaches of computer science. What is a potential future technological advancement that could further Facebook's mission, improve one of its products, or help the world in some way? Your technological advancement should be within the realm of possibility.
4. How can Facebook decrease the likelihood of a data privacy scandal in the future?

WORKS CITED

Ahmed, Azam, and Danny Hakim. "Mexico's Hardball Politics Get Even Harder as PRI Fights to Hold On to Power." *The New York Times*, The New York Times, 25 June 2018, https://www.nytimes.com/2018/06/24/world/americas/mexico-election-cambridge-analytica.html

Arrington, Michael. "Facebook Users Revolt, Facebook Replies." *TechCrunch*, TechCrunch, 6 Sept. 2006, https://techcrunch.com/2006/09/06/facebook-users-revolt-facebook-replies/.

Baser, David. "Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?" *Facebook Newsroom*, 16 Apr. 2018, https://newsroom.fb.com/news/2018/04/data-off-facebook/.

Cavoukian, Ann. *Privacy By Design; The 7 Foundational Principles. Privacy By Design; The 7 Foundational Principles.*

Chong, Zoey. "Apple Knocks Facebook with Shutdown over App Privacy Flap." *CNET*, CNET, 31 Jan. 2019, https://www.cnet.com/news/facebook-shuts-down-ios-research-app-it-used-to-access-user-data/.

"EPIC - Facebook Privacy." *Electronic Privacy Information Center*, https://epic.org/privacy/facebook/.

"Explore Your Activity Log: Facebook Help Center." *Facebook*, https://www.facebook.com/help/activitylog.

"Facebook to Be Fined $5bn over Cambridge Analytica Scandal'." *BBC News*, BBC, 13 July 2019, https://www.bbc.com/news/world-us-canada-48972327.

"Facebook Shuts down Beacon." *The Telegraph*, Telegraph Media Group, 21 Sept. 2009, https://www.telegraph.co.uk/technology/facebook/6214370/Facebook-shuts-down-Beacon.html.

Fowler, Geoffrey A. "Goodbye, Chrome: Google's Web Browser Has Become Spy Software." *The Washington Post*, WP Company, 21 June 2019, https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/?noredirect=on.

Fromholz, Julia M. "The European Union Data Privacy Directive." *Berkeley Technology Law Journal*, vol. 15, no. 1, 2000, pp. 461–484. *JSTOR*, www.jstor.org/stable/24115723.

Hall, Mark. "Facebook." *Encyclopædia Britannica*, Encyclopædia Britannica, Inc., 24 Apr. 2012, https://www.britannica.com/topic/Facebook.

Kang, Cecilia. “F.T.C. Approves Facebook Fine of About $5 Billion.” *The New York Times*, The New York Times, 12 July 2019, https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html.

Korosec, Kirsten. “Facebook: What Personal Data It Collects And Shares From Users.” *Fortune*, Fortune, 21 Mar. 2018, http://fortune.com/2018/03/21/facebook-personal-data-cambridge-analytica/.

Kovach, Steve. “Apple Didn’t Just Take the Moral High Ground on Privacy, It Twisted the Knife into Google and Facebook.” *CNBC*, CNBC, 4 June 2019, https://www.cnbc.com/2019/06/04/apple-makes-the-right-move-with-new-private-login-option-on-iphone.html.

LII Staff. “Personal Information.” *Legal Information Institute*, Cornell Law School, 15 June 2015, https://www.law.cornell.edu/wex/personal_Information.

Mayer, Jane. “New Evidence Emerges of Steve Bannon and Cambridge Analytica’s Role in Brexit.” *The New Yorker*, The New Yorker, 18 Nov. 2018, https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit.

Nield, David. “All the Ways Google Tracks You-And How to Stop It.” *Wired*, Conde Nast, 28 May 2019, https://www.wired.com/story/google-tracks-you-privacy/.

Noyes, Dan. “Top 20 Facebook Statistics.” Zephoria Inc., 16 Sept. 2019, https://zephoria.com/top-15-valuable-facebook-statistics/.

“Online Tracking.” *Consumer Information*, Federal Trade Commission, 13 Mar. 2018, https://www.consumer.ftc.gov/articles/0042-online-tracking.

Roessler, Beate. “Three Dimensions of Privacy.” *The Handbook of Privacy Studies: An Interdisciplinary Introduction*, edited by Bart Van der Sloot and Aviva De Groot, Amsterdam University Press, Amsterdam, 2018, pp. 137–142. *JSTOR*, www.jstor.org/stable/j.ctvcmxpmp.7.

Rosenberg, Matthew. “Academic Behind Cambridge Analytica Data Mining Sues Facebook for Defamation.” *The New York Times*, The New York Times, 15 Mar. 2019, https://www.nytimes.com/2019/03/15/technology/aleksandr-kogan-facebook-cambridge-analytica.html.

Roose, Kevin, and Cecilia Kang. “Mark Zuckerberg Testifies on Facebook Before Skeptical Lawmakers.” *The New York Times*, The New York Times, 11 Apr. 2018, https://www.nytimes.com/2018/04/10/us/politics/zuckerberg-facebook-senate-hearing.html.

Rubinstein, Ira S., and Nathaniel Good. “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents.” *Berkeley Technology Law Journal*, vol. 28, no. 2, 2013, pp. 1333–1413. *JSTOR*, www.jstor.org/stable/24119897.

Schulze, Elizabeth. “Mark Zuckerberg Says He Wants Stricter European-Style Privacy Laws - but Some Experts Are Questioning His Motives.” *CNBC*, CNBC, 1 Apr. 2019, https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html.

Singer, Natasha. “Facebook’s Push for Facial Recognition Prompts Privacy Alarms.” *The New York Times*, The New York Times, 9 July 2018, https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html.

V, Ramzeen A. “72 Facebook Acquisitions.” *TechWyse*, 5 Sept. 2019, https://www.techwyse.com/blog/infographics/facebook-acquisitions-the-complete-list-infographic/.

Wagner, Kurt. “Here’s How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users.” *Vox*, Vox, 17 Mar. 2018, https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

“What Is Privacy?” *Privacy International*, https://privacyinternational.org/explainer/56/what-privacy.

Zuckerberg, Mark. “The Facts About Facebook.” *The Wall Street Journal*, Dow Jones & Company, 25 Jan. 2019, https://www.wsj.com/articles/the-facts-about-facebook-11548374613.

TOPIC B: OPEN SOURCE INVESTIGATION

WHAT IS OPEN SOURCE INVESTIGATION?

Open source investigations (OSINT) involve the collection and verification of open source intelligence. Anything that can be found publicly constitutes open source intelligence, such as public government records or public information posted online. In the modern day, social media plays an important role as being a medium in which researchers can look for open source intelligence. For example, if protests are occurring in a certain region and human rights monitors are concerned that the human rights of individuals may be threatened, human rights monitors may live monitor activity in the region through Twitter and Facebook. Through Twitter, one can use TweetDeck to search for keywords that have been posted in a period of time and look at different twitter timelines in one dashboard. Through Facebook, human rights investigators can search for relevant pages and keywords and monitor activity on those pages such as status and photo updates. As well, Facebook profiles include the option of indicating the city one is from and his/her job description, which is information that can be used in investigations (Human Rights). After open source intelligence—the content of posts from Twitter, Facebook, etc—has been collected, investigators then attempt to verify the intelligence, as not everything that people post on the Internet is true or original content. If there is an image depicting a potential human rights or legal violation, investigators can reverse image search the photo to see where the original image comes from. If there is a text based post that indicates a potential violation, investigators can search the text of the aforementioned post to see if it appears anywhere else on the internet as well as verify if the content of that text can be substantiated (Research Methodology).

It is important for investigators to archive any of these posts as soon as they see them because users can delete their posts, or if these posts are reported by other users, Facebook and Twitter could take them down. As there is a growing movement to limit the circulation of fake news, hate speech, and disturbing graphic materials on the Internet, there results a catch-22. The circulation of fake news, hate speech, and graphic images can propagate persecution and violence towards a certain group, which is why people argue for these materials to be taken down. However, on the other hand, the existence of these posts can become evidence for investigators to use in legal cases. Thus, it becomes a little more complicated for tech companies to decide and define how the public benefits or does not benefit from the existence of certain posts online (Warner).

Open Source Intelligence is still quite a young field, so it is still developing and improving all the time. On a macro scale, the field's capabilities for providing high quality, relevant, and useful intelligence are constantly increasing because more and more of daily life is conducted through the internet. Since the amount of data that exists online is growing exponentially year to year as cyberspace develops, the internet is a constantly growing source for OSINT (Benes). In addition, as the number of people who conduct OSINT has grown, organizations like Bellingcat have sprung up as hubs for this new form of investigation (About).

On a micro scale, open source intelligence is being helped by increased mobility and availability brought about by technology (Benes). One example is mobile journalism, a growing practice in which mobile phones are used in order to capture live information about an ongoing crime, news event, or disturbance. There are more than six billion phones in the world today, enabling people around the world to take journalism and investigation into their own hands (How Mobile…).

ACTIVISM ON FACEBOOK - 2011 CLEAN WATER CAMPAIGN

Facebook enables activism on its platform through its Campaign feature, which allows users to create funding pages, informational summaries, and discussion forums. Facebook also has Groups, which creates collective spaces where users can post messages to all other group members. These features are certainly useful, but are quite minimalist, and rely on the users to facilitate activism.

In 2009, the Italian government passed a water privatisation law that required that the water supply was more privately funded. Specifically, it established the regulations that in all companies managing water, private investors should own at least 40% of the company, while local government should have less than 30%. Proponents of this law claimed that the privatisation would increase the efficiency of Italy's water system. However, many protested the idea that water, a universal right, would now be influenced by the forces of the free market (The Campaign).

In 2011, the Forum Italiano dei Movimenti per l'Acqua began a grassroots campaign to overturn the aforementioned law. Facebook became a vital tool - initially many groups and pages were created, and they coalesced into one as the movement gained traction. Facebook became a legitimate alternative to mainstream media, who were mostly ignoring or opposing the campaign. One key characteristic of this movement was extremely individualized communication - users of Facebook would directly reach out to their friends and mobilize them, harnessing Facebook's web of friendships for social good. Another unique feature of the campaign was massive mobilization of Italy's younger generations - the media began labeling them 'popolo di Facebook', or people of Facebook, and they made a significant impact in the movement (The Campaign).

In the end, the campaign amassed over 1.4 million signatures in favor of a referendum to overturn the law. The referendum also passed by an overwhelming majority of 95%-5%. This case was an overwhelming success, and opened the world's eyes to the power of Facebook's platform for social good (The Campaign).

Social media has several key benefits when used for social activism. It enables new forms of online protest, from sharing infographics to organizing protests. Features like Facebook's Campaigns allow movements to sustain a common identity and maintain a history of the key events of the activism. The interconnected nature of social media makes it much easier to mobilize new people - people are much more likely to read a post from one of their friends than a flyer on a street. In addition, a lack of centralized communication doesn't necessarily entail poorer organization - instead of acting as figureheads, leaders act as connective directors, enabling others to lead in their own form of protest (Poell).

At the same time, social media and specifically Facebook have many drawbacks. There are significant privacy and control risks for activists, as compared to traditional activism. Additionally, Facebook can lead to an "echo chamber", in which we are only connected to those with similar opinions as us - in such cases, there can be a big difference between Facebook and reality - activism on Facebook could incorrectly or incompletely address issues it aims to fix. Specifically for Facebook, data access is extremely closed - data is Facebook's competitive advantage over other social media companies and its source of revenue, and so they are extremely reticent to give unrestricted public access. Users are also generally reluctant to allow research groups to use their personal data. Communication on Facebook can also be too fragmented to ever come together - this issue is exacerbated by Facebook's lack of a powerful search engine for research (Poell).

CONTENT MODERATION

When content is uploaded to Facebook, it undergoes a multi-stage moderation process which attempts to keep out posts which Facebook deems as inappropriate for the site. Disallowed content can range from fairly innocuous lies about other people or pictures posted without consent, to serious and damaging content like hate speech and gore. Content moderation is a necessity for all social media platforms because such sites are partially responsible for the content that they host, even if it is user-generated. Legally, they are protected by the Common Decency Act of 1996, but their public reputation can be seriously damaged by unsuitable content.

The first layer of content moderation involves a complex system of artificial intelligence and classification. Facebook utilizes the latest and greatest algorithms in order to classify pictures, videos, and text - these classifications are then used to decide whether or not a piece of content is allowed or not. Importantly, such systems are not able to distinguish categories intelligently, and instead are answering what images probably are (Newton).

WHAT THE TECH?: MACHINE LEARNING

Machine learning is an incredibly powerful and hot field in technology, and has quickly become very widely used and talked about. Many understand machine learning as allowing computer programs to make more intelligent decisions, but few understand exactly what the field is. In this section, I'll give a high level overview of machine learning and some of its applications so that you, the delegates, have context for how it can be used in addressing crises.

Machine learning is fundamentally about data analysis. In general, machine learning algorithms take in an enormous amount of data, and use complicated math to create generalized rules for any new data it receives. Suppose, for example, there is a machine learning program which tries to tell if a picture is of a cat or not. After seeing a few hundred examples, the program might be able to create rules like: Does it have ears? Does it have whiskers? Are its eyes feline? For a human, these rules look like math equations, so it is not always possible to understand why a program makes the predictions that it does. In general though, the more examples a program is able to "train" on, the more accurate its predictions will be.

Machine learning can be used for image recognition, financial predictions, understanding human speech, and much much more. If you end up trying to incorporate machine learning into a solution for a crisis, try to answer the questions: What data are we using for training? What are we predicting? Could our algorithm make a decision that negatively impacts the company?

When Facebook's algorithms are unsure about their classifications, they pass reports onto the massive content moderation staff responsible for upholding Facebook's terms of use. Facebook currently employs around 15 thousand people around the world as moderators - their daily job is reviewing reports and deciding how to handle the sensitive content. Decisions on how to respond to different types of content are determined at Facebook's Content Standards Forum, and slowly trickle down to the human moderators (How Social-Media…).

A rising issue in the Open Source Intelligence community is that content on Facebook is deleted by its moderation system before it can be used to investigate human rights abuses. In 2014, several pictures documenting the violent war in Syria were removed from Facebook for violating Community Guidelines - such content, although violent and gory, could have proved invaluable in investigating the atrocities of the conflict (Burrington). However, once "moderated", there is no way to recover the pictures, even if they could provide evidence in a legal trial. Julian Nicholls, a lawyer in the International Criminal Court, said "It's something that keeps me awake at night, the idea that there's a video or photo out there that I could use, but before we identify it or preserve it, it disappears." (Asher-Schapiro). Facebook is in a unique position to enable open source investigations through its platform because of its global user base, social connectivity, and huge trove of data - however, enabling such investigations would require a significant restructuring of how its content moderation system operates.

CASE STUDY: ETHNIC CLEANSING IN MYANMAR

Human rights investigators at the Human Rights Center at UC Berkeley and at Reuters worked together to collect information on anti-Rohingya sentiment in posts on Facebook circulated by users in Myanmar (Why Facebook…). In April 2018, Mark Zuckerberg responded to public backlash that the crisis in Myanmar was being fueled by hate speech and propaganda posted on Facebook against the Rohingya and Muslim communities in Myanmar by calling for greater review of posts posted in the Burmese language (Roose). Although posts on Facebook that promote hate speech towards certain ethnic or social groups are in violation of Facebook's terms of service, over a thousand posts/comments/materials involving hate speech against Rohingyas/Myanmar Muslims were found by Reuters and the Human Rights Center. This is attributed to the fact that Facebook did not have many individuals who spoke Burmese reviewing posts written in Burmese. These posts in Burmese do not auto-translate very coherently, which may explain why many of these posts with dehumanising language were not taken down by Facebook.

The Reuters report claims that when Facebook became widely available to users in Myanmar in 2013, after telecommunications were deregulated, violence against Myanmar Muslims and Rohingyas began to steadily increase. As well, although Twitter is less used in Myanmar than Facebook, many posts on Twitter also perpetuated hate speech against these groups and did not get flagged or taken down. Thus, this case study shows how social media can be a medium to encourage hate speech and human rights violations if posts are not adequately reviewed by tech companies. In this situation, having these posts exist on the evidence did not benefit the public by serving as evidence as to the perpetrators of certain violations, but these posts may have actually just encouraged violations to occur through the spread of hate speech.

GOVERNMENT INVOLVEMENT

Open Source Investigation is an incredibly powerful tool for national law enforcement forces around the world. In 2009, the European Union attempted to create a platform for open-source intelligence called Virtuoso. This project allowed police forces to easily navigate online sources of information and created opportunities for large-scale data collection by the government. However, the project may have been ahead of its time, and was ended in 2013. Despite this, the Virtuoso project highlighted the need for governments around the world to leverage the internet and the power of big data to combat crime (VIRTUOSO).

At the same time, governments have shown suspicion towards the legitimacy of open-source intelligence. In 2018, evidence of the use of chemical weapons in Syria began to surface across the internet. Despite this, Emily Thornberry, who was the Foreign Secretary of the United Kingdom, warned the UK government against "open source intelligence provided by proscribed terrorist groups." Thornberry received significant backlash, but was also supported by other members of parliament. Without any way to verify the validity of a particular piece of evidence, it is highly likely that governments will continue to undervalue open source investigation because information over the internet can often lie contrary to the truth (Don't Rely…).

KEY COMPANIES

Twitter is a popular social network based around "tweets", which are essentially short blog posts which are published to all of a user's followers. Twitter's cultural influence over the past decade cannot be understated - it has become a virtual soapbox for anyone and everyone, from President Donald Trump to Syrian refugees, to publicly broadcast their opinions on. Additionally, it is also widely considered one of the most powerful tools for open source investigation - for example, in June 2019, there was an investigation into Saudi Arabian twitter campaigns against Jeff Bezos (Sen).

The main reason that Twitter is so effective at enabling open source investigation is its commitment to openness and freedom of expression. One lesser known product, TweetDeck, allows for extensive and fine-grained searching and analysis of any user's history on Twitter. It also has powerful tools that archive sensitive content and make it easy to view the history of trending hashtags. In the investigations against Saudi Arabia, "by looking at their Twitter output [investigators] can see what hashtags they are pushing, why they are pushing them, how they are segmenting their audience, how they are pushing different messages in response to real world events, and [investigators] can also understand what is important to them and what is not." (Sen). Though there are a few situations in which Twitter will impede an investigation or simply delete a sensitive account, its track record for enabling OSINT should be a standard for other social media networks (Kumar).

QUESTIONS TO CONSIDER

1. To what extent should Facebook allow access to its data to those who wish to conduct open source investigation?
2. What are some shortcomings of Facebook's suite of apps when it comes to open source investigations?
3. How can Facebook improve the way it moderates its content?
4. Does Facebook have an obligation to activists to allow access to internal data?

WORKS CITED

"'Don't Rely on Intelligence from Terrorists': Thornberry Warns Govt over Any Syria Chemical Attacks." *RT International*, 11 Sept. 2018, https://www.rt.com/uk/438161-idlib-syria-thornberry-chemical/.

"About." *Bellingcat*, https://www.bellingcat.com/about/.

Asher-Schapiro, Avi. "YouTube and Facebook Are Removing Evidence of Atrocities, Jeopardizing Cases Against War Criminals." *The Intercept*, 2 Nov. 2017, https://theintercept.com/2017/11/02/war-crimes-youtube-facebook-syria-rohingya/.

Benes, Libor. "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm." *Journal of Strategic Security*, vol. 6, no. 3, 2013, pp. 22–37. *JSTOR*, www.jstor.org/stable/26485053.

Burrington, Ingrid. "Could Facebook Be Tried for Human-Rights Abuses?" *The Atlantic*, Atlantic Media Company, 21 Dec. 2017, https://www.theatlantic.com/technology/archive/2017/12/could-facebook-be-tried-for-war-crimes/548639/.

"How Mobile Phones Are Changing Journalism Practice in the 21st Century." *Reuters Institute for the Study of Journalism*, 4 Mar. 2014, https://reutersinstitute.politics.ox.ac.uk/risj-review/how-mobile-phones-are-changing-journalism-practice-21st-century.

"How Social-Media Platforms Dispense Justice." *The Economist*, The Economist Newspaper, 6 Sept. 2018, https://www.economist.com/business/2018/09/06/how-social-media-platforms-dispense-justice.

"Human Rights Investigations Lab." *Human Rights Investigations Lab*, UC Berkeley, 2016, https://humanrights.berkeley.edu/programs-projects/tech/investigations-lab.

Kumar, Ankit. "No, India Did Not Bully Twitter into Banning OSINT Accounts." *India Today*, 21 June 2019, https://www.indiatoday.in/india/story/twitter-ban-osint-accounts-india-america-british-students-dmca-1553731-2019-06-21.

Newton, Casey. "The Secret Lives of Facebook Moderators in America." *The Verge*, The Verge, 25 Feb. 2019, https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona.

Poell, Thomas & Van Dijck, José. (2017). Social media and new protest movements.

“Research Methodology: Syrian Archive.” *Syrian Archive*, https://syrianarchive.org/en/tools_methods/methodology/.

Roose, Kevin, and Paul Mozur. “Zuckerberg Was Called Out Over Myanmar Violence. Here’s His Apology.” *The New York Times*, The New York Times, 9 Apr. 2018, https://www.nytimes.com/2018/04/09/business/facebook-myanmar-zuckerberg.html.

Sen, Ashish Kumar. “Open Source Information as a Tool in Exposing Authoritarian Regimes.” *Atlantic Council*, 21 June 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/open-source-information-as-a-tool-in-exposing-authoritarian-regimes.

“The Campaign for Water on Facebook.” *Social Media Activism: Water as a Common Good*, by Matteo Cernison, Amsterdam University Press, Amsterdam, 2019, pp. 165–202. *JSTOR*, www.jstor.org/stable/j.ctvc77nv5.11.

“VIRTUOSO Project.” EUROSINT FORUM, https://www.eurosint.eu/virtuoso-project.

Warner, Bernhard. “Tech Companies Are Deleting Evidence of War Crimes.” *The Atlantic*, Atlantic Media Company, 9 May 2019, https://www.theatlantic.com/ideas/archive/2019/05/facebook-algorithms-are-making-it-harder/588931/.

“Why Facebook Is Losing the War on Hate Speech in Myanmar.” *Reuters*, Thomson Reuters, 15 Aug. 2018, https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/?utm_source=twitter&utm_medium=Social.