# Analysis of Social Media Privacy Measures

Zachary Hasley
University of Central Florida
Orlando, USA
zachhasley773@knight.ucf.edu

Christopher Gardner
University of Central Florida
Orlando, USA
pigswig@knights.ucf.edu

Cameron Lindsey
University of Central Florida
Orlando, USA
cameronlindsey@knights.ucf.edu

## ABSTRACT

With the rapid growth of the internet social media websites have grown to become a common pastime for almost everyone. The average user does not think about the effects social media has on their personal and private information. It is the responsibility of these websites to protect their customers' information while trying to maintain a profit. The findings of this paper will go into detail on how three major websites collect, protect, and use their customers' information.

## CCS CONCEPTS

• **Security and privacy**;

## 1 INTRODUCTION

With social media websites being one of the top pastimes in the world it is important to understand the potential damages and shortcomings that come with it. Our goal with this paper is to see how three of the top social media websites handle the protection of their users. We want to see how these companies have improved on their privacy protection methods and if they really have the users best interest.

All of these websites are free in some way but at what cost? Over the years we have all heard the words privacy, protection, data, etc. thrown around but how is it really handled and what does it mean to the user? Most people just log on these social media websites and post whatever they want without thinking about the repercussions. Users send messages back and forth thinking only themselves and the intended receiver are the ones with access to these messages but they are wrong.

## 2 BACKGROUND

Reddit, self-billed as "the front page of the internet", is an anonymous site unique for its forum-like approach to content. Reddit allows users to create a forum (called a subreddit, or just "sub") for a topic, which users then post to. This is unlike sites such as Twitter, where a user posts something directly to their own profile, although Reddit has added the option recently. Users can also subscribe to a subreddit, and posts from that subreddit will appear on their homepage, in addition to posts from other subreddits they subscribe to. Reddit uses an "upvote" and "downvote" system for posts, where upvotes show support for a post and downvotes show dislike. Posts with more upvotes show first, unless the user decides to sort posts by another method. As Reddit is considerably more anonymous than most social media sites, its methods of protecting that anonymity made an interesting topic of research.

Facebook is a social media site with a focus on networking. Users can post to their profile, and with permission can post on other's profiles and in groups. Like Reddit's home page, Facebook has a news feed that displays posts from friends and groups the user is in. Additionally, it includes suggestions for the user based on their interests. Facebook employs an emotion reaction system for its posts, with the options of "Like" (a thumbs up), "Love" (a heart), "haha" (a laughing face), "yay" (a smiling face), "wow" (a surprised face), "sad" (a sad face), and "angry" (an angry face). Noticeably, all these reactions push a post upwards on the scale of popularity. For example, a controversial post with 400 haha reactions and 400 angry reactions will be treated with the same priority as a post about a new movie with 800 like reactions in a user's news feed. Facebook has a massive user base and has been the subject of several breaches, which is why we decided to research it for our project.

Snapchat is a popular instant messaging and social media app. Snapchat's main focus is direct messages or snaps which are sent as a video or picture and can be sent directly or posted on a user's story where everyone can see it. Snaps sent directly will expire directly after being opened, and users are alerted if someone takes a screenshot of their snap. One popular feature on Snapchat is the use of filters, which uses augmented reality to overlay or distort the user's face. Snapchat also has a feature to save created Snaps as Memories and view them like a phone's photo gallery. More recently, Snapchat has implemented a Discover section where users can browse through various content and sponsered accounts. Finally, Snapchat also has a feature called Snapmaps where users can opt to share their location and see the locations of their friends. Snapchat's massive popularity in combination with its unique posting method was the reason we chose it for our project.

### 2.1 Related Work

One topic that came up many times during the research of this project was the privacy policy of these social media websites. There were two papers that really highlighted how websites handle privacy policies and how users seem to interpret them. The first of these papers would be TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights. The creators of this paper developed an automated machine learning tool called TLDR which is used to convert privacy policies into a condensed version of itself giving the users less to read with the same useful information. This tool was able to reduce the amount of time it takes to read a privacy policy by an average of 39.14% which makes

*CAP5150, December 4, 2022, Final Paper*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

it more likely for a user to read the policy [1]. This would be useful to social media users as it makes reading the policy less time consuming and gives the users a good idea on what the platforms are doing with their data.
The second would be Measuring the Privacy Dimension of Free Content Websites through Automated Privacy Policy Analysis and Annotation. This paper used the automated tool TLDR mentioned above. They trained it with a dataset to determine the difference between privacy policies in free websites versus premium websites. They found that free websites tend to lack information and use generic privacy policies compared to premium websites [2]. This matters to this paper as most social media websites are free to join and access.

## 3 APPROACH

In our project we used Multi-Source Active Analysis (Figure 1). By pulling from multiple sources, we hoped to grasp the full scope of each site's privacy measures and their effectiveness. For our primary sources, we used the privacy policy of each site and any press release or announcement that came from them. For example, [14] is an official statement by the Reddit admins. For our secondary sources, we used articles written about the site in question. For example, [29] is an article written by a third party, The Verge, about Facebook. Once we had information we needed, we drew conclusions on how each site handled, or mishandled, their users' data.

## 4 TAXONOMY

End to end encryption (E2EE): In end-to-end encryption, a message is encrypted using a public key and can only be decrypted by the intended recipient's private key. This means that upon reaching a server or other intermediary the message is already encrypted, preventing third parties from viewing it. E2EE is secure, as intermediaries never touch the unencrypted message [16].
Hypertext Transfer Protocol Secure (HTTPS): HTTPS is TLS running over HTTP. HTTP is the basic algorithm that sends website data to a client, TLS simply makes sure that this connection is secure [4].
Transport Layer Security (TLS): TLS creates keys to encrypt data, sending them to the client via public key encryption. TLS also requires the server owner to have installed a certificate which identifies them as a trustworthy website, something the client device will ask for upon connecting, providing extra security. HTTPS is used to prevent third parties like ISPs from inserting extra data into a connection, typically in the form of advertisements [5]. Secure Sockets Layer (SSL): The original name of TLS, changed due internal issues in its development. It and TLS are usually used interchangeably, as their functions are nearly identical [5].
Two Factor Authentication (TFA): TFA is a security measure requiring users to input their username and password in addition to performing a third action, usually entering a security code sent as an email or text message. Having TFA enabled prevents attackers from gaining access to user accounts even if they have login information, in addition to alerting the victim to a failed account breach. While helpful, this can be breached, which will be discussed later.

## 5 EVALUATION

### 5.1 Reddit

You can't mention big social media websites without mentioning Reddit. With 52 million daily active users it was ranked the 9th most popular social media app in the US [8]. Reddit has grown to popularity over the past few years and has had to adapt to many different security updates. Reddit has security features for everything from protecting advertisements to protecting their users.
Reddit as a business must try and keep their stakeholders happy by creating a profit. They have a couple different ways of doing this with the main one being advertisements. Of course, to make the advertisements more accurate Reddit collects user data and personalizes some of these advertisements to their users. Because of this it is up to Reddit to protect their user's data in a way that users can trust them as a social media platform.

*5.1.1 Reddit Protections.* Prior to 2015, Reddit was using HTTP as their default application layer protocol. There was the option to use HTTPS, but the user would have to manually enter HTTPS. The average user of the internet would not know to switch to HTTPS so this would leave many users vulnerable [9]. Reddit currently makes this encryption available using TLS v1.2 and TLS v1.3. Other network protection they use would be intrusion detection. This involves controlling the size of the attack as it is happening, detection controls that are activated while data is entered, and technology that handles data as it comes in if potentially dangerous. Cloud services are used to provide network security within services. As data is transferred it is protected with both SSL and TLS [23].
For stored data protection Reddit uses multiple different cloud service providers and uses data centers scattered around the world with the goal of no lost data. Reddit noted that the primary cloud services they use are AWS and occasionally use Google BigQuery [30]. Amazon provides users with many different encryption types to use with their cloud services. Reddit uses multiple provider capabilities with redundant configurations so that nothing slips past and corrupts the data.

*5.1.2 Effectiveness of Protections.* In 2018, Reddit suffered a massive security incident by attackers that were able to hack some employee accounts. Reddit was using TFA with SMS authentication. They learned this was not very secure at all and the attackers were able to intercept the SMS messages. The attacker was able to access a copy of an old database from 2005-2007 containing user information such as usernames and hashed passwords, email addresses, and messages. They were also able to gain access to source code and configuration files. To combat this attack Reddit reported it to law enforcement who launched an investigation. They also added security measures such as more logging, more encryption, and forcing token-based TFA instead of SMS-based, claiming this is the root cause of the leak [14].
It has been found by a Reddit user that passwords, in 2009, are transmitted in clear text. A post on askreddit submitted by a user showed a Wireshark dump of the username and password of the user being sent in plain text [12]. This could be a major problem if the user is trying to access their accounts on a public wifi. Anyone could be using a similar tool to analyze traffic and steal your information. In a study done in 2021 by security.org they found

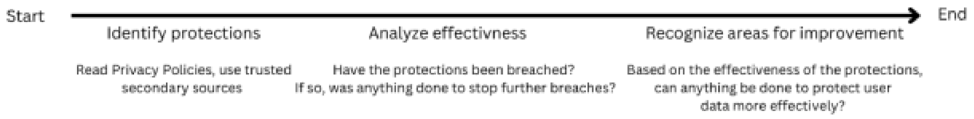

Start
Identify protections
Analyze effectivness
Recognize areas for improvement
End
Read Privacy Policies, use trusted secondary sources
Have the protections been breached? If so, was anything done to stop further breaches?
Based on the effectiveness of the protections, can anything be done to protect user data more effectively?

**Figure 1: Multi-Source Active Analysis Pipeline**

that 68% use the same password for different accounts [27]. This shows how important it is for users to use different passwords on these websites. A user could be connecting to public wifi anywhere and 68% of them have the chance of their password to all of their accounts being leaked.

*5.1.3 Possible Improvements.* Like most social media websites, Reddit collects information on their users to help target advertisements, protect users from scammers, and provide customer service. Of course this is all according to their privacy policy so they would make it sound much better than the truth. Reddit does allow users to fine turn some of their personal data collection. They collect information such as your location via GPS or bluetooth, IP addresses associated with accounts, any content from private messages to posts [22].

Reddit does allow users to subscribe to Reddit premium which gives the users an ad-free experience. An improvement here would be not collecting data on these types of users as they have no need for personalized advertisements. This makes me think that while Reddit does not show these premium users advertisements, they are still collecting their data and selling it to customers to increase profits.

## 5.2 Facebook

With 2.9 billion monthly active users, Facebook is the biggest social media platform in the entire world [15]. Nearly 3 billion users a month means that Facebook servers have a lot of data going through them, and given the nature of the site, a significant amount of it is personal. Here is a look at the data Facebook collects on its users, the steps it takes to protect it, and what they do with it.

Facebook collects a wide range of data on its users. This includes personal information about a user, who they interact with and how, the device they use to connect, their education level, their political views, their health, how they interact with advertisements, their location, and much more. Before making judgements, there is nuance to this. Data like political beliefs and health are given some protections by law, and some data Facebook keeps, like credit card information, can remain out of their hands should a user decide not to share it. In addition to the data collected on users, Facebook collects data on those who do not use their products. Should a user post about how their sibling who doesn't use Facebook enjoys a hobby, Facebook will collect that information [18].

This data is mainly used in two ways: product improvement and targeted advertisements. Facebook uses the data it collects to test new products and programs in addition to gauging user feelings on those already released. They also allow advertisers to easily target their most effective audience. When signing up for Facebook, a user provides information about themselves such as age, gender, and location, which advertisers use to reach their intended audience most effectively. Further use of Facebook gives advertisers information about a user's interests, which in turn can be used to target their advertisements even more effectively [18].

With all of this personal data, it is important that Facebook's protections can resist attacks in order to protect the privacy of its users. Additionally, Facebook must be responsible with what data they allow advertisers access to, again to protect user privacy.

*5.2.1 Facebook Protections.* Facebook possesses two messaging services: WhatsApp and Facebook messenger, both of which offer E2EE. On WhatsApp it is used for all communications, while on Facebook messenger it is a toggleable option, currently disabled by default [13]. Facebook messenger having encryption turned off by default likely leaves many users' messages open for third parties, as it is likely many users' do not understand E2EE or are simply not aware of the option. In addition, E2EE must be enabled on a per-chat basis, meaning a forgetful user may also leave some of their messages unencrypted. Facebook appears to agree that the off by default model is unsafe, as it has expressed interest in changing this default in 2023 [29]. A welcome change.

When browsing, Facebook uses HTTPS to secure the connection between the user and the server. Unlike E2EE on Facebook messenger, this is always on [20]. While HTTPS is generally standard for large sites, every security measure counts. Like most sites, Facebook employs a two-factor authentication system, should the user enable it [19]. Facebook hashes its passwords using a 7 step program in an attempt to ensure the secrecy of user passwords. It begins with a md5 hash, which is followed up by a salt and hash. The result of these hashes is sent over to Facebook, who then hashes the data again using a secret. Finally, a scrypt is used to slow down breaching attempts, and the hash is compressed for storage purposes. [28]

*5.2.2 Effectiveness of Protections.* Facebook has had more than a fair share of data breaches, for a variety of reasons. Knowing about these breaches, and why they occurred, is critical in understanding the effectiveness of Facebook's privacy measures. To begin, in May 2010 it was discovered that Facebook was giving its advertisers the user name and IP address of users that clicked on their ads. This 'privacy loophole' allowed Facebook to sell advertisers the data needed to track a user without the user's consent [26]. In response to this, Facebook closed this version of the loophole. However, that did not end Facebook's problem with sharing user data without permission. In 2018, Facebook was revealed to be allowing 150 other companies access to private information with the justification that these other companies were "extensions" of Facebook. Said other companies had varied levels of access: while Bing was only allowed to see a given user's friend list, Netflix and Spotify could see 'private' messages between users [7]. There does not appear to be any concrete information as to if Facebook ever stopped sharing this information.

Facebook has a share of breaches aside from mismanagement of its own data. In 2012, a bug in Facebook's contact manager allowed unauthorized users access to others' phone number and email. If a user attempted to download contact info from another, their phone number and email would be included regardless of the targeted users privacy settings. This breach is particularly notable because it took a year to be found and patched, although it was stated that no one used the bug for a malicious purpose. 6 million users were stated to have been affected [25]. In May 2018 a bug made private profiles viable to anyone. 14 million users were affected [17]. Finally, in September 2019 a bug in the "view as" feature allowed attackers access to other users' access tokens. Between 50 million and 90 million users were affected [24].

Finally, there is arguably the biggest data breach of the 2010's: the Cambridge Analytica scandal. In 2018, Cambridge Analytica, a political consulting firm, was revealed to have access to 87 million users' private data. A quiz app on Facebook allowed the creator, Aleksandar Kogan, access to the users' personal data. It also gave him access to the data of every single user on the quiz takers friends list. While Facebook admittedly forbids the selling of data like this in its terms of use, that did little to stop them. For a time it was believed that the data gathered may have influenced the 2016 presidential election, but as of 2022 nothing has ever been proven [3]. The majority of Facebook's technical protections appear to work as intended: The encryptions they use to protect private messages have not been breached, their two-factor authentication is effective, and their password hashing has resisted outside attacks. All of the breaches have been the fault of the humans running Facebook, not the protections they use.

*5.2.3 Possible Improvements.* This is not a complete list of Facebook's data breaches by any means, but it is enough to draw conclusions. The main threat to user safety seems not to be outside attackers, but Facebook itself. Be it features that leave exploits in the system, ill-vetted quiz apps, or them directly violating the law to sell access to the data they collect, Facebook's privacy issues are a direct result of either incompetence or greed. These shortcomings undermine any privacy measures that they put in place, and unless Facebook begins to more strictly self-moderate this will continue. With a 15 year history of mistakes, it remains doubtful they will ever improve.

## 5.3 Snapchat

As one of the largest social media platforms in the world with 319 million daily users [11], many of them being minors, security is a large focus. In Snapchat, users communicate by taking short videos or pictures called snaps, and sending them to other users, these snaps can usually only be opened once before disappearing after a short amount of time. Snapchat also has a feature called Snap Maps where users optionally share their locations and can view the locations of their friends. Snapchat also collects user information such as name, date of birth, phone number, and email. In addition to the data that you provide, Snapchat stores the details of all users' communications, usage statistics, ad views, and publicly available content created on the app.

*5.3.1 Snapchat Protections.* Snapchat does provide a decent amount of control over user information, they do allow you to edit and access all account information from the app. Snapchat also provides users with the option to download their data including conversation history, location data, and other logging information. You also can allow or deny Snapchat access to your pictures, camera, microphone, and location data. You may also choose to delete your Snapchat account at any time and Snapchat states they will remove your sent pictures and videos from their servers. You also choose what other users can contact you and are able to block and report other users.

Snapchat keeps your personally identifiable information indefinitely unless you decide to modify or remove those records. Location tracking data is kept for an unspecified amount of time. Snapchat states that sent 'snaps' are deleted from their servers after they have been opened or if they have expired.

In Snapchats' terms and conditions they state that they do not sell personal information, however they do provide personal information to 3rd parties for targeted advertising [10], however users can opt out of this. Snapchat has also complied with law enforcement requests to share data collected from a user if that user is suspected of being guilty of some serious crimes. Snapchat's terms and conditions do not explicitly state their methods for securing their data, both in transit and when being stored on their servers.

*5.3.2 Effectiveness of Protections.* Unfortunately, Snapchat has seen issues with security breaches in the past. In 2014 Snapchat's API was exploited to obtain user's private data through their 'Find My Friends' feature, which initially users could not opt out on. This allowed data skimming to extract personal data such as names, phone numbers, and usernames. They responded to this by making that feature optional, but were criticized for their late patch of this exploit.

In 2017, a phishing attack was executed where compromised accounts would send links to users that would redirect to a web page mimicking Snapchats login screen. Many social media apps have link screening functionality that check for links to malicious content before allowing the user to proceed, however this overlook caused over 50,000 users accounts and passwords to be compromised [21].

*5.3.3 Possible Improvements.* While Snapchat's password encryption methods are secure enough against common adversaries, still this does not fully protect against user's with insecure passwords either leaked in another site's data breach or easily guessed based on that user's public information. Requiring multi-factor authentication would be a step in the right direction to help protect user's accounts against unauthorized access.

While Snapchat's terms and conditions state that users must be at least 13 years old, little - if anything - is done to validate a new user's age. Requiring some form of identification or confirmation from an adult with verified identification would be beneficial to help protect younger users from creating accounts and would also help limit bot and spam account creation.

## 6 DISCUSSION

While it appears these websites are moving in the right direction there's still more room to improve. With leaks still happening it can still cause worry knowing the customer's data is not one hundred percent safe. More code reviews could reduce the risk of this data being breached.

It is understanded that these companies must profit somehow but alternatives would be nice. Some people might say they would like to pay a fee to use these websites instead of having their data collected without a choice. This seems like a good idea as it allows the companies to still profit while the users can have a peace of mind knowing their data is more private. In short, alternative methods of monetization would allow companies to survive without collecting and selling user data, making it easier to protect from hackers.

More recently, there have been reports of Snapchat's employees spying on user accounts [6]. Snapchat's internal tool 'SnapLion' is used as a sort of admin tool which provides employees access to user accounts and allows employees to view user's messages and data saved onto Snapchat's servers. While the tool is used officially to comply with law enforcement requests and reset user's passwords if they are locked out, there are reports of employees abusing the tool to view user's private information.

## 7 WORK DISTRIBUTION

As for work distribution each team member contributed to proofreading other's works. Chris researched Reddit and added the problem statement and introduction. Zach researched Facebook and added the taxonomy, as well as creating figures. Cameron researched Snapchat and contributed to the initial discussion as well as did final paper formatting.

Chris' estimated time worked would be 14 to 15 hours. Cameron's estimated time worked would be 13 to 15 hours. Zach's estimated time worked would be 15 to 16 hours.

## 8 CONCLUSION

Generally, the protections placed by companies are secure. There are exceptions to this rule, as seen in Reddit's TFA breach, but external forces usually do not have unauthorized access to data by cracking an encryption or hash. However, illy vetted code and the desire for profit place a user's data at risk no matter the protections enacted. Spotify's API was abusable on launch, and Facebook allowed a quiz app that stole data from a user and everyone on their friends list, despite it being explicitly against their privacy policy.

User data will always be at risk, no matter the privacy measures put in place. As developers are humans, exploits will always be found. But these risks can be mitigated, through better coding practices and better monetization methods.

# REFERENCES

[1] Ülkü Meteriz-Yildiran Abdulrahman Alabduljabbar, Ahmed Abusnaina and David Mohaisen. 2021. TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights. *ACM Workshop on Privacy in the Electronic Society (WPES'21)* (2021).

[2] Abdulrahman Alabduljabbar and David Mohaisen. 2022. Measuring the Privacy Dimension of Free Content Websites through Automated Privacy Policy Analysis and Annotation. *Companion Proceedings of the Web Conference* (2022).

[3] Alvin Chang. 2018. The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram. *Vox* (2018). https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

[4] Cloudfare. [n.d.]. What Is HTTPS? https://www.cloudflare.com/learning/ssl/what-is-https/

[5] Cloudfare. [n.d.]. What Is Transport Layer Security? https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

[6] Joseph Cox. 2019. Snapchat Employees Abused Data Access to Spy on Users. *Motherboard Tech* (2019). https://www.vice.com/en/article/xwnva7/snapchat-employees-abused-data-access-spy-on-users-snaplion

[7] et al Dance, Gabriel J.X. 2018. As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. *The New York Times* (2018). https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html

[8] Brian Dean. 2022. Reddit user and Growth Stats. *Backlinko* (2022). https://backlinko.com/reddit-users

[9] Lorenzo Franceschi-Bicchierai. 2015. Reddit Switches to Encryption By Default. *Motherboard Tech* (2015). https://www.vice.com/en/article/kbzj7y/reddit-switches-to-https-encryption-by-default

[10] Snap Inc. [n.d.]. Privacy Policy. https://snap.com/en-US/privacy/privacy-policy

[11] Snap Inc. [n.d.]. Snap Inc. Announces Fourth Quarter and Full Year 2021 Financial Results. https://investor.snap.com/news/news-details/2022/Snap-Inc.-Announces-Fourth-Quarter-and-Full-Year-2021-Financial-Results/default.aspx

[12] Jonathan_the_Nerd. 2009. Why does reddit transmit my password in cleartext? https://www.reddit.com/r/AskReddit/comments/90rhn/why_does_reddit_transmit_my_password_in_cleartext/

[13] Gail Kent. 2020. Hard Questions: Why Does Facebook Enable End-to-End Encryption? *Meta* (2020). https://about.fb.com/news/2018/05/end-to-end-encryption/

[14] KeyserSosa. 2018. We had a security incident. Here's what you need to know. https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/

[15] Alfred Lua. 2022. 21 Top Social Media Sites to Consider for Your Brand. *Buffer Library* (2022). https://buffer.com/library/social-media-sites/

[16] Madelyn Lutkevich, Ben. Bacon. 2021. What Is End-to-End Encryption (E2EE) and How Does It Work? *SearchSecurity* (2021). https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE

[17] Louise Matsakis. 2018. Facebook Bug Made up to 14 Million Users' Posts Public for Days. *Wired* (2018). https://www.wired.com/story/facebook-bug-14-million-users-posts-public/

[18] Meta. [n.d.]. Facebook Privacy Policy. https://www.facebook.com/privacy/center/

[19] Meta. [n.d.]. Login Alerts and Two-Factor Authentication: Facebook Help Center. https://www.facebook.com/help/909243165853369/?helpref=hc_fnav

[20] Meta. 2022. Does Facebook Use Secure Browsing (HTTPS)? https://www.facebook.com/help/156201551113407

[21] Casey Newton. 2018. A phishing attack scored credentials for more than 50,000 Snapchat users. *The Verge* (2018). https://www.theverge.com/2018/2/16/17017078/snapchat-phishing-attack-klkviral-dominican-republic

[22] Reddit. [n.d.]. Reddit Privacy Policy. https://www.reddit.com/policies/privacy-policy

[23] Reddit. [n.d.]. Reddit Security Measures. https://redditinc.force.com/helpcenter/s/article/Reddit-Security-Measures

[24] Aja Romano. 2018. Facebook Says 50 Million User Accounts Were Exposed to Hackers. *Vox* (2018). https://www.vox.com/2018/9/28/17914598/facebook-new-hack-data-breach-50-million

[25] Gerry Shih. 2013. Facebook Admits Year-Long Data Breach Exposed 6 Million Users. *Reuters* (2013). https://www.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed-6-million-users-idUSBRE95K18Y20130621

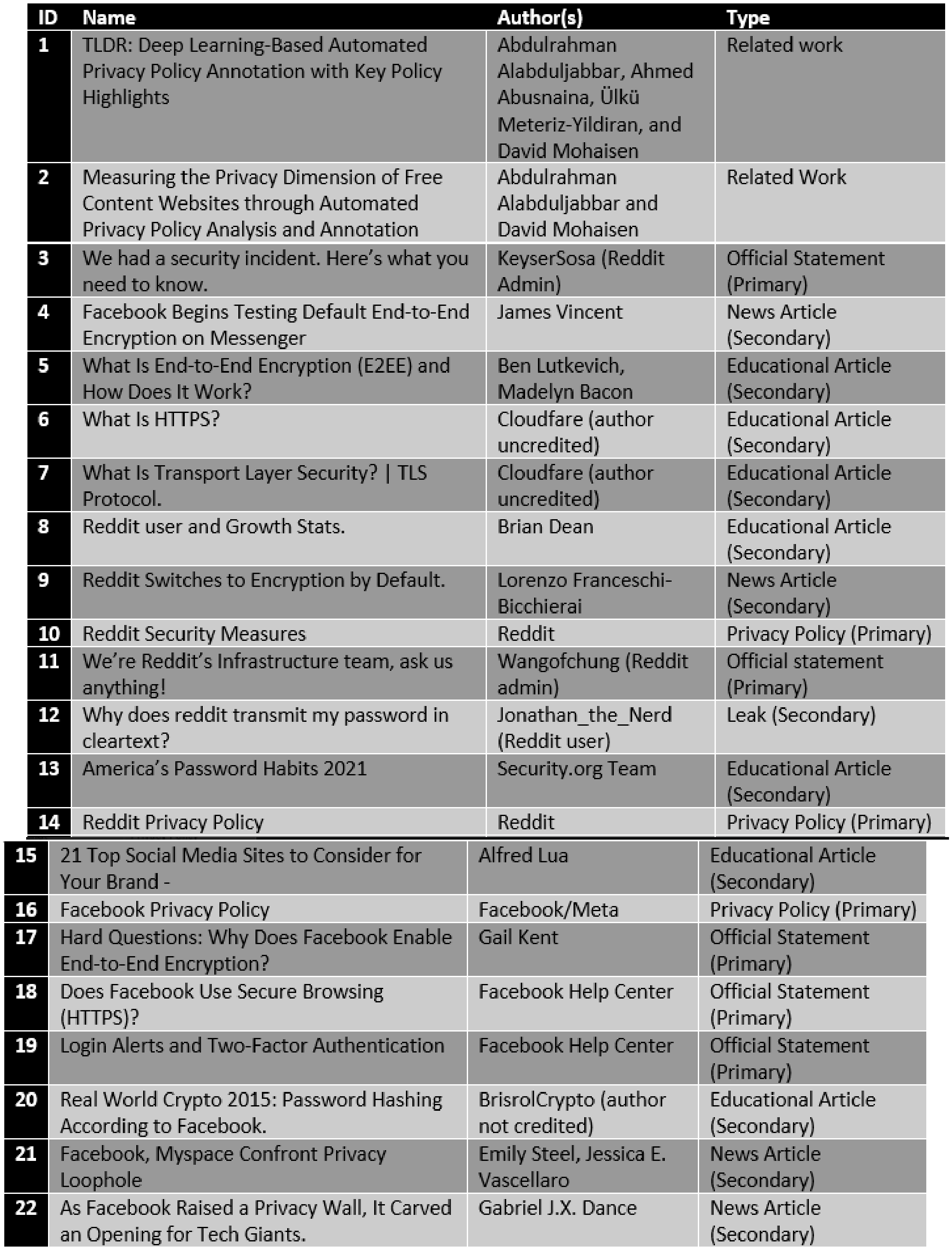
[26] Emily Steel and Jessica E. Vascellaro. 2010. Facebook, Myspace Confront Privacy Loophole. https://www.wsj.com/articles/SB10001424052748704513104575256701215465596

[27] Security.org Team. 2022. America's Password Habits 2021. https://www.security.org/resources/online-password-strategies/

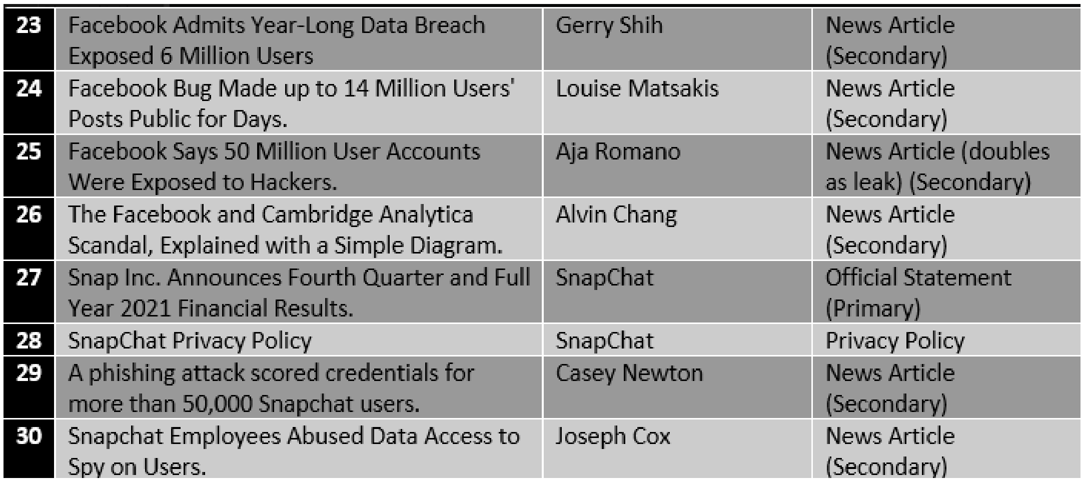
[28] Unknown. [n.d.]. Real World Crypto 2015: Password Hashing According to Facebook. https://bristolcrypto.blogspot.com/2015/01/password-hashing-according-to-facebook.html

[29] James Vincent. 2022. Facebook Begins Testing Default End-to-End Encryption on Messenger. *The Verge* (2022). https://www.theverge.com/2022/8/11/23301275/facebook-messenger-end-to-end-encryption-default-test-e2ee-privacy-security-plans

[30] Wangofchung. 2019. We're Reddit's Infrastructure team, ask us anything! https://www.reddit.com/r/aws/comments/ecf5i3/comment/fbb4gk1/?utm_source=share&utm_medium=web2x&context=3



| ID | Name | Author(s) | Type |
|---|---|---|---|
| 1 | TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights | Abdulrahman Alabduljabbar, Ahmed Abusnaina, Ülkü Meteriz-Yildiran, and David Mohaisen | Related work |
| 2 | Measuring the Privacy Dimension of Free Content Websites through Automated Privacy Policy Analysis and Annotation | Abdulrahman Alabduljabbar and David Mohaisen | Related Work |
| 3 | We had a security incident. Here's what you need to know. | KeyserSosa (Reddit Admin) | Official Statement (Primary) |
| 4 | Facebook Begins Testing Default End-to-End Encryption on Messenger | James Vincent | News Article (Secondary) |
| 5 | What Is End-to-End Encryption (E2EE) and How Does It Work? | Ben Lutkevich, Madelyn Bacon | Educational Article (Secondary) |
| 6 | What Is HTTPS? | Cloudfare (author uncredited) | Educational Article (Secondary) |
| 7 | What Is Transport Layer Security? \| TLS Protocol. | Cloudfare (author uncredited) | Educational Article (Secondary) |
| 8 | Reddit user and Growth Stats. | Brian Dean | Educational Article (Secondary) |
| 9 | Reddit Switches to Encryption by Default. | Lorenzo Franceschi-Bicchierai | News Article (Secondary) |
| 10 | Reddit Security Measures | Reddit | Privacy Policy (Primary) |
| 11 | We're Reddit's Infrastructure team, ask us anything! | Wangofchung (Reddit admin) | Official statement (Primary) |
| 12 | Why does reddit transmit my password in cleartext? | Jonathan_the_Nerd (Reddit user) | Leak (Secondary) |
| 13 | America's Password Habits 2021 | Security.org Team | Educational Article (Secondary) |
| 14 | Reddit Privacy Policy | Reddit | Privacy Policy (Primary) |
| 15 | 21 Top Social Media Sites to Consider for Your Brand - | Alfred Lua | Educational Article (Secondary) |
| 16 | Facebook Privacy Policy | Facebook/Meta | Privacy Policy (Primary) |
| 17 | Hard Questions: Why Does Facebook Enable End-to-End Encryption? | Gail Kent | Official Statement (Primary) |
| 18 | Does Facebook Use Secure Browsing (HTTPS)? | Facebook Help Center | Official Statement (Primary) |
| 19 | Login Alerts and Two-Factor Authentication | Facebook Help Center | Official Statement (Primary) |
| 20 | Real World Crypto 2015: Password Hashing According to Facebook. | BrisrolCrypto (author not credited) | Educational Article (Secondary) |
| 21 | Facebook, Myspace Confront Privacy Loophole | Emily Steel, Jessica E. Vascellaro | News Article (Secondary) |
| 22 | As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. | Gabriel J.X. Dance | News Article (Secondary) |



| | | | |
|---|---|---|---|
| **23** | Facebook Admits Year-Long Data Breach Exposed 6 Million Users | Gerry Shih | News Article (Secondary) |
| **24** | Facebook Bug Made up to 14 Million Users' Posts Public for Days. | Louise Matsakis | News Article (Secondary) |
| **25** | Facebook Says 50 Million User Accounts Were Exposed to Hackers. | Aja Romano | News Article (doubles as leak) (Secondary) |
| **26** | The Facebook and Cambridge Analytica Scandal, Explained with a Simple Diagram. | Alvin Chang | News Article (Secondary) |
| **27** | Snap Inc. Announces Fourth Quarter and Full Year 2021 Financial Results. | SnapChat | Official Statement (Primary) |
| **28** | SnapChat Privacy Policy | SnapChat | Privacy Policy |
| **29** | A phishing attack scored credentials for more than 50,000 Snapchat users. | Casey Newton | News Article (Secondary) |
| **30** | Snapchat Employees Abused Data Access to Spy on Users. | Joseph Cox | News Article (Secondary) |