WORLD LIBRARIES

Volume 28

No. 1

2024 worldlibraries.dom.edu/index.php/worldlib|

Case Study: Information Privacy & YouTube

Katherine Kozlowski Mitchel

Dominican University

ABSTRACT

Many individuals and organizations in the United States rely on YouTube to publicly share information and/or promote their organization and offerings. However, YouTube has mastered the practice of offering users a false sense of security when it comes to their information privacy. While there are many policies in place within YouTube's privacy standards–and children's personally identifiable information (PII) is rather well protected by the site due to a settlement requiring the site to comply with the Children's Online Privacy Protection Rule (COPPA)–there are little to no true protections for

users when faced with the threat of their information being leaked to bad actors. This does not have to be the case, though, as YouTube has the ability to strengthen their policies to offer more assistance to its users in times where their PII may be used in a malicious way. On the other hand, it is not solely up to YouTube to be responsible in creating new policies surrounding user privacy. The Federal Communications Commission (FCC) is responsible for regulating privacy practices for companies in the United States and has yet to make a groundbreaking move against social media sites like YouTube to protect the information of web users. By instituting regulations that perform similarly to laws like the General Data Protection Regulation (GDPR) of Europe, or the California Consumer Privacy Act (CCPA), the United States can offer consumers better protections in regard to their PII and web safety overall.

INTRODUCTION

Overview

YouTube, being an extension of Google, is no stranger to controversy regarding information privacy and has even faced significant fines and penalties for violating the COPPA guidelines. Further, the strong enforcement of COPPA on YouTube has led users to be extremely cautious about what they are posting in videos for fear they will get flagged for content that the algorithm deems as inappropriate. YouTube doesn't necessarily offer protections for its internet-aged (read: over the age of 13) users when it comes to information privacy. This is largely in part due to Google's tendency to exploit its available data sources and distribute them to other companies for a profit. Further, beyond basic information privacy protections, users face the potential threat of other users by means of doxxing and stalking. In such cases, the individual being attacked is offered no protections by YouTube and is solely responsible for their own safety and prevention of further attacks from future threats.

In an era where many web users are at a heightened risk of attacks from bad actors, now is the best time to bring the topic of information privacy and YouTube to light. This study aims to determine what YouTube does offer in terms of information privacy to its users and in what ways they could become the bastion of social media by making user-centric updates to their policy. By YouTube taking these steps, users will be better protected from the risks caused by a presence on YouTube and can safely manage their channel without fear of their personal information and private data getting into the wrong hands.

Information Privacy Definitions

- California Consumer Privacy Act (CCPA): "If you are a California resident, you may ask businesses to disclose what personal information they have about you and what they do with that information, to delete your personal information and not to sell your personal information. You also have the right to be notified, before or at the point businesses collect your personal information, of the types of personal information they are collecting and what they may do with that information. Generally, businesses cannot discriminate against you for exercising your

rights under the CCPA. Businesses cannot make you waive these rights, and any contract provision that says you waive these rights is unenforceable" (California Attorney General).

- Children's Online Privacy Protection Rule (COPPA): "...prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet" (Code of Federal Regulations).
- Data Protection: "Data protection is the process of safeguarding important data from corruption, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable. Data protection assures that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable legal or regulatory requirements. Protected data should be available when needed and usable for its intended purpose" (Storage Networking Industry Association).
- Doxxing (dox): "To publicly identify or publish private information about (someone) especially as a form of punishment or revenge" (Merriam-Webster).
- Federal Communications Commission (FCC): "The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation" (FCC).
- Federal Trade Commission (FTC): "Protecting the public from deceptive or unfair business practices and from unfair methods of competition through law enforcement, advocacy, research, and education" (FTC).
- General Data Protection Regulation (GDPR): "The GDPR mandates that companies that collect personal data, those must be collected legally with specific restrictions and conditions. Businesses must protect personal data from misuses and exploitations. They must respect the rights of data owners. In cases of violation or failure to comply with GDPR, companies will face penalties and fines" (IM 785 Lecture).
- Internet Protocol Address (IP Address): "An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network. The IP address is the core component on which the networking architecture is built; no network exists without it. An IP address is a logical address that is used to uniquely identify every node in the network. Because IP addresses are logical, they can change. They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives" (Techopedia).

- Information Privacy: “The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Dr. Alan Westin, Privacy and Freedom).
- No Disclosure without Consent Rule: “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains” (Privacy Act).
- Personal Data: “Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data.” (GDPR).
- Personal Information Protection and Electronic Documents Act (PIPEDA): “Organizations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, they must obtain consent again. Personal information must be protected by appropriate safeguards” (Office of the Privacy Commissioner of Canada).
- Personally Identifiable Information (PII): “Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.” (US Department of Labor).
- Privacy Act: “The Privacy Act provides individuals with a means to access government records about themselves” (Privacy Act).
- Virtual Private Network (VPN): “A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network” (National Institute of Standards and Technology).

METHODOLOGY

This study uses the method of a case study to determine the current privacy protections in place by YouTube for its users and where there are missing protections and laws. The study relies on organizational theories in order to determine these protections, wherein the protections offered by YouTube are compared to that of federal, state, and private laws and regulations. A case study is a qualitative research method, it requires the collection of data about "...participants, interviews, protocols, tests, examinations of records, and collections of writing samples" (WAC Clearinghouse) to come to a conclusion. There are 4 types of case studies: illustrative, exploratory, cumulative, and critical instance. This research consists of a critical instance case study, meaning that it is set to determine the cause and effect nature of the data collected to study on this topic (WAC Clearinghouse).

Advantages of this type of research method include a large amount of resources available to study and opportunities to utilize reliable sources to reach conclusions on the data collected. Further, there is little to no need to complete research beyond what is found during a search. Disadvantages of this type of research method, on the other hand, are that a narrow scope of data exists that can be collected without directly contacting the organization being studied. Lastly, another disadvantage is that the results of the study are subjective due to the researcher's opinion being the determination of what exactly is the cause and effect. No experiment or study is being held beyond the research sphere to ensure that the conclusions being postured are realistic and impartial.

RESULTS

YouTube, and ultimately its parent company Google, claim to offer transparency over what is collected, why it is collected, and how the information collected and entered into the site can be managed by a user. To a greater extent, they also claim that they do not sell user data and instead, "...use the information we collect to customize our services for [users], including providing recommendations, personalizing search results, and serving relevant ads for [users]" (How Does YouTube Maintain User Privacy). YouTube additionally uses a feature called "Your Data in YouTube" where privacy controls, and information on how YouTube manages user data including search and watch history along with subscription lists are contained. A particular option within this allows users to edit, pause, or clear their watch and search history, along with an Incognito Mode that "lets [users] browse privately in a session so [their] account search and watch history will not reflect whatever [they're] viewing and will not be carried over to [their] logged-in account." (YouTube Privacy Controls). Since Google is the parent of YouTube, there are additional features including the option to view Google-wide controls that track web and application activity, location history, and personalized advertisement settings. YouTube claims that the information is solely shared between YouTube and Google only, however, their AdCenter site indirectly admits that Google is one of the companies who participates in the aggregation of user data and sales by addressing that user data is shared with "sites and applications that partner with Google" (Google Ad Center). Considering YouTube outright states that "YouTube's main source of revenue is

advertising" on its "How Does YouTube Make Money?" page, it is hard to believe that they are not sharing user data in places where the user is not made aware of in the privacy policies.

When it comes to practices that lead to privacy violations of users, YouTube additionally offers spam, deceptive practice, sensitive content, and violent or dangerous content policies within their Community Guidelines. For the spam and deceptive practice policies, YouTube seeks to protect users by having policies that include the usage of external links, spam, deceptive practices, and scams. When it comes to sensitive content, child safety is one of the main components and COPPA is a large part of the protection of children's privacy and the protection of children from being exposed to inappropriate material on the site. In terms of violent or dangerous content, YouTube has policies that are intended to protect users from harassment and cyberbullying. In that vein, when further investigated, anyone who is a target of any threat or harassment is directed to report it to local law enforcement, per YouTube's Harassment and Cyberbullying Policies site. YouTube takes no responsibility for these behaviors occurring on their platform outside of offering an option to report any comments or profiles for the acts and does not actively try to monitor and filter out these types of comments (Harassment and Cyberbullying Policies).

One thing that does come as an advantage from the YouTube Privacy Guidelines is YouTube's clearly laid out stance to enforce their Privacy Guidelines based on how they want them handled and not explicit to each country's guidelines (How Does YouTube Maintain User Privacy?). If a user deletes content or a video that data is permanently deleted from YouTube's servers, offering an option for users to remove any content that may have accidentally included PII, thus ensuring that information remains private after the removal of the content and potentially avoiding the spread of the user's information to a bad actor. If a user discovers their PII including "image or voice, full name, financial information, contact information, or other personally identifiable information" (Protecting Your Identity) on another user's channel and the poster does not comply with requests to take the content down, YouTube offers a "privacy complaint process" where the affected user has an opportunity to have the content taken down.

When it comes to violations, in September of 2019 YouTube was alleged to have violated COPPA which resulted in a $140 Million settlement with the FTC and more stringent policies from YouTube when it comes to children's personal information and the content marketed towards them (FTC). While its parent company Google has faced its fair share of judgements against it for a variety of privacy practice violations, this was the first major suit against YouTube itself. The case alleged that,

> YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent. YouTube earned millions of dollars by using the identifiers, commonly known as cookies, to deliver targeted ads to viewers of these channels, according to the complaint. (FTC)

As a result of this settlement, and in an attempt to avoid any further violations of COPPA, YouTube was required to include provisions within their site for creators to mark whether or not their content was

geared towards children. Previously, YouTube channel owners had communicated with YouTube directly that their pages were directed toward children or the rating system identified content as "kid-directed" (FTC Compliance Tips). Lastly, in January of 2020, YouTube posted an article titled "Better Protecting Kids' Privacy on YouTube" to their official blog to inform creators and general users on the new policies put into place to protect the privacy of their under-13 user demographics.

When it comes to leadership within the organization, YouTube does not publicly share who is in charge of controlling information privacy-related issues within YouTube. An extensive search did not produce any information on who holds that position. YouTube additionally does not have any plans available to the public in terms of what their current plans are to update their privacy policy. Furthermore, they also do not have any plans available outlining upcoming plans for the organization to add to or change their privacy policy.

DISCUSSION

Even though on the surface it appears that YouTube is doing enough to protect its users from threats to their PII, they have several glaring gaps in their privacy policies that leaves its users vulnerable. For instance, the expectation of users to take on the bulk of responsibility when their PII is shared by another channel without their literal or implicit permission does nothing to truly help someone recover their personal data and resolve the issue. Sure, YouTube offers to step in if the channel sharing the information refuses to take down the content, but they should frankly be running an algorithm that flags data like this when it is shared. If YouTube has a competent enough team of coders who can put together some of the most sophisticated algorithms to make suggestions to users on what videos to watch and others that flag inappropriate content shortly after it is posted, surely, they can gather a team of coders to create an algorithm that catches these incidents and pulls down the content to protect vulnerable users.

In terms of information privacy laws, YouTube has gotten a lot better at adhering to the regulations that were created to fairly manage the practices of social media organizations. As discussed previously, YouTube took the settlement over COPPA with stride and made the necessary changes to meet the requirements of the law and better the platform overall. However, there is still room for improvement for YouTube as a whole. Considering YouTube was adamant about adhering to their own rules for the posting and maintenance of content regardless of a user's home country, it would be easy for the organization to take note of laws like the CCPA and the Personal Information Protection and Electronic Documents Act (PIPEDA) and apply most of the principles to the daily maintenance of the site. Furthermore, YouTube could look to the Privacy Act for guidance, as they could put into place the opportunity for users to access all of their records on YouTube without hassle and without having to jump through hoops to find or request the information. The No Disclosure without Consent Rule within the Privacy Act would also apply in this instance, wherein YouTube would have to both disclose directly to the user their intentions to share their data every time they would want to and request written consent to do so. In some ways, yes, YouTube has managed to adhere to some of the principles of these

acts, but overall most consumers have no idea how to access the data that YouTube collects on them, nor do they know how to opt out of the collection of data from their profile. By taking piecemeal concepts from PIPEDA, CCPA, and the Privacy Act, YouTube can be more transparent in what exact information is collected, require users to give explicit consent or deny the right for YouTube to collect data on them and their usage of the site, and have access to all of the information collected about them with the ability to opt out at any time.

One of the noteworthy components of researching the privacy policies directly through the YouTube site is the survey question pop-up that appeared on most of the pages affiliated with the privacy policies. An example of one of these questions comes from the Ad Settings page, where the pop-up requests the user to answer the following question: “How much do you agree or disagree that the information on this website has improved your opinion that "YouTube protects users from harmful content"?”. The timing and placement of these questions feel a bit sneaky, as though Google and YouTube are trying to manipulate users into a false sense of security in what protections they offer their users. It’s hard to distinguish whether they feel overly confident in the measures they take to protect the personal data of their users or they see their shortcomings and feel that a survey may help give them an idea of what direction they need to take to change course.

RECOMMENDATIONS

Due to the unique circumstances of being an organization in which most, if not all, privacy policies are determined specifically by the regulations imparted on social media and web-based organizations, the recommendations discussed herein will require the discussion of laws and regulations that would apply to all web-based organizations. While some recommendations can be made directly towards YouTube itself, and were mostly addressed during the discussion of this study, it is an unfortunate reality that without laws and regulations put in place on a federal level organization like YouTube will continue to determine loopholes that benefit their bottom line at the end of the day. Users must demand the FCC force a change in the policies of this organization to improve outcomes for its users. There is no avoiding bringing this reality to light, as it is a necessary process to complete to ensure that the unseemly practices of these organizations can and will change.

Users can make some small changes for themselves that would assist in preventing some risks involved with a web presence on sites like YouTube, and YouTube itself could encourage users to take the adequate steps to protect themselves, as well. By pushing users to utilize services like VPNs, YouTube could ensure that the IP address of its users would be better protected due to the masking of location and, therefore, result in less overall risk for acts like doxxing from bad actors on the site. However, the main key to imparting change from YouTube and its fellow social media organizations is by action of the FCC. The FCC needs to put its foot down and protect the consumers that use social media sites regardless of whether they pay for the services or not. Consumers can exist within free services, as at any point in time they may become a paying customer. With that in mind, the FCC can study the success

of international regulations like the GDPR and learn how to flesh out and/or adopt the ideas held within it to better the information privacy of all social media users within the United States.

LIMITATIONS

This study includes multiple limitations, much like most case studies tend to do. As the writer of the study is the individual who determines the results and missing factors, the results are subjective and solely up to the discretion of the writer. Differing opinions can, and will, occur surrounding this topic and this study only imparts one perspective in regards to the subject at hand. Additionally, case studies allow for a narrow scope of research and do not delve deeply into the subject matter through different methods including interviews, contacting the organization directly, and similar thorough practices. Furthermore, the information available regarding the topic of information privacy and data are constantly evolving and the information discussed within this study is limited to the time in which it was written. Tomorrow, next week, or next year the information discussed herein may become outdated and new laws and regulations may be passed that deems this data collection moot. Due to that reasoning, there is a limitation to timeliness surrounding this study.

CONCLUSIONS

The Universal Declaration of Human Rights, Article 19 put the essence of YouTube into a nice package, “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers” (United Nations). This also applies well to the concept of information security in relation to YouTube, as users should be granted the right to “seek, receive, and impart information and ideas” that pertain to their PII “regardless of frontiers”. Or, in this case, regardless of the web-based privacy threats in front of them. While it is difficult to suggest to large social media organizations massive changes that would benefit the users over the bottom line of the company, it is imperative that further regulations are put into place on the site to protect the users and their PII. It does not matter if YouTube organically determines the practice of updating their policies to better protect users or if the FCC creates rules similar to the GDPR or PIPEDA. Regardless of who puts the wheels in motion on changing the policies at YouTube, it is a necessary act to complete. There is also a definitive need for further investigations and more complex research to be completed in regards to this topic, especially when it comes to social media as a whole. If users feel safer and their privacy can be better protected on the site, YouTube could be the first social media organization to maintain its loyal users indefinitely. In a world where many people don’t feel safe using any social media and fear or sometimes even find their information getting into the wrong hands, it would be a smart move for YouTube to change that and perhaps even spread awareness to other social media organizations who in-turn could change their policies. It does not need to be a perfect world for organizations like YouTube to take the consumer into full consideration and change outcomes of data privacy for the better.

REFERENCES

California Attorney General. (n.d.). *California Consumer Privacy Act (CCPA)*. https://oag.ca.gov/privacy/ccpa

Code of Federal Regulations. (n.d.). *Children's Online Privacy Protection Rule (COPPA)*. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Storage Networking Industry Association. (n.d.). *Data protection*. https://www.snia.org/education/dictionary/d

Merriam-Webster. (n.d.). *Doxxing*. In *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/doxxing

Federal Communications Commission. (n.d.). *About the FCC*. https://www.fcc.gov/about/overview

Federal Trade Commission. (n.d.). *Protecting America's consumers*. https://www.ftc.gov

Techopedia. (n.d.). *Internet Protocol Address (IP Address)*. https://www.techopedia.com/definition/5366/internet-protocol-address-ip-address

Office of the Privacy Commissioner of Canada. (n.d.). *PIPEDA and your personal information*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

U.S. Department of Labor. (n.d.). *Personally Identifiable Information (PII)*. https://www.dol.gov/general/privacy/

National Institute of Standards and Technology. (n.d.). *Virtual Private Network (VPN)*. https://csrc.nist.gov/glossary/term/virtual_private_network

United Nations. (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Google Ad Center. (n.d.). *Ad settings*. https://adssettings.google.com

YouTube. (n.d.). *Privacy controls*. https://support.google.com/youtube/answer/10364219

YouTube. (2020). *Better protecting kids' privacy on YouTube*. https://blog.youtube/news-and-events/protecting-kids-privacy-on-youtube

YouTube. (n.d.). *Harassment and cyberbullying policies*. https://support.google.com/youtube/answer/2802268

YouTube. (n.d.). *How does YouTube make money?*. https://support.google.com/youtube/answer/9243352

YouTube. (n.d.). *Community guidelines*. Retrieved from https://www.youtube.com/howyoutubeworks/policies/community-guidelines/

Federal Trade Commission. (n.d.). *Compliance tips for COPPA*. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

Zamir, H. IM 785 Lecture. (2022). *General Data Protection Regulation (GDPR)*. [Lecture material]