

Learning through Videos: Uncovering Approaches to Educating People about Facebook Privacy

Alexa Stein, *Bentley University* Norman Makoto Su, *Indiana University Bloomington*
Xinru Page, *Brigham Young University*

Abstract

This research is an initial step towards identifying an effective way to leverage a popular medium, YouTube videos, in order to educate people about social media privacy risks and how to protect themselves from privacy violations. We report on initial work classifying the current tactics used in YouTube videos to do so. We find that videos fall into three broad categories: Fear Appeals, Reflective Learning, and Technical Literacy. Our work also uncovers how videos utilize different levels of detail to get their message across. We elaborate on how these techniques are employed and suggest how this can be used to inform the design of future online videos as educational interventions to promote user knowledge of social media privacy.

1. Introduction

Social media has been widely adopted in many countries. In the United States alone, it is used by 69% of adults [1]. Although people use social media to facilitate their social, professional, and even civil interactions, 91% of social media users in the U.S. feel they have lost control over their online privacy [2]. Backlash against widely publicized privacy breaches such as with Cambridge Analytica have led many users to feel they must choose between the benefits of social media and completely abandoning it in order to protect their privacy [3]. Rather than leaving users to make such a dichotomous decision, there can be a middle ground of helping them understand the types of privacy risks they face, as well as how to take privacy protecting measures. This study investigates how one form of media, online videos, are being used to educate people about privacy issues on one of the most popular social media platforms, Facebook [1]. We undertook a discourse analysis of videos on YouTube. Namely, we address the following research question:

What methods are currently being used in videos to educate people about Facebook privacy?

Understanding current privacy education approaches can inform the design of future interventions. This paper draws on the broader education literature to discuss the potential

effectiveness of various approaches that we observed in videos. It concludes by sharing implications for designing effective educational intervention videos to educate people about their privacy on Facebook.

2. Background

Social media research reveals how people often do not utilize privacy features, nor change default settings [4]. Studies also point to how readily people disclose their personal information [5]. Indeed, there is much research that investigates the widely cited *privacy paradox* where stated privacy concerns often are not reflected in social media users' behaviors [6]. This has motivated several streams of research, including one stream which investigates methods for increasing privacy awareness to encourage privacy-protecting behaviors. For example, research shows how presenting stories about peers who have been compromised can help users take their privacy more seriously [7]. Other work has focused on explaining privacy in a more accessible way such as through privacy comics [8] or privacy labels [9] (akin to nutrition labels). Scholars have investigated privacy features, behaviors, and coping mechanisms that fall under the broad categories of avoidance, modification, and alleviation [10]. Our research investigates YouTube videos as a vehicle for making privacy education more accessible and persuasive. This analysis of existing Facebook privacy videos is a first step towards that goal.

3. Methods

In August 2019, we performed a YouTube video search conducted by using the keywords "Facebook" + "Privacy" as well as the keywords "Facebook" + "Settings" + "Tutorial". The first author identified video search results that were in English, relevant to Facebook privacy, and relatively short given our goal of accessibility and widespread appeal (we used a generous cutoff of 15 minutes long). This involved analyzing over 5 pages of results, with 40 videos per page, before topic relevance greatly diminished. Following this process produced a final set of 26 videos fitting our inclusion criteria. They were posted between February 2011 and August 2019, with an average length of 4 minutes and 20 seconds long. Our approach follows other studies in human-computer interaction that perform discourse analyses [13] of various popular "texts" (e.g., videos, articles) to glean design insights and opportunities [10,11]. Discourse analysis scrutinizes both the message of a text's content and

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9 -- 11, 2020, Boston, MA, USA.

YOUTUBE VIDEO TITLE	MADE BY	APPROACH	SUBJECT AREA						LEVEL OF DETAIL			Date	Likes	Views	
			Pub/ Priva	Appr Shar	Data Coll	Data Perm	Ads	Finan ce	Con text	Feat ure	How- To				
Do you really have a private life online?	Friendly Screens	Literacy	x	x									2011-Feb	<1k	360k
Security on Social Networks	Post Finance	Literacy	x										2013-Mar	<1k	7.8k
Cyber Street- Your Social Media Privacy Settings Need Checking	Cyber Aware	Reflective		x									2013-Dec	<1k	456k
Easy Ways to Stay Safe on Social Networks	Safety in Canada	Literacy	x	x									2014-Feb	<1k	30k
Internet Privacy Prank	Buzzfeed	Reflective	x	x									2014-Apr	15k	809k
How to Make Your Facebook Completely Private	TutoVids	Literacy	x	x	x							x	2014-Jul	11k	92m
Privacy Issues with Social Media	Rita Belloma	Fear								x			2015-Apr	<1k	31k
Social Media Privacy and Security Settings	1800RESPECT	Literacy	x	x								x	2016-Apr	<1k	1.5k
Lesson 26: Social Media and Privacy	Iowa Cyber	Literacy	x	x						x			2016-Aug	<1k	2.1k
Hands-on Privacy on Your Social Media	ITRC San Diego	Fear	x	x									2016-Dec	<1k	21k
Facebook Privacy Settings Tutorial 2017	Anson Alexander	Literacy	x								x	x	2017-Apr	<1k	70k
			<i>Before 2018:</i> 82% 73% 9% 0% 0% 0% 18% 9% 27%												
Public Revelation of Cambridge Analytica Incident															
How to protect your privacy and data on social media?	Parameswaran R	Literacy			x		x			x	x		2018-Mar	<1k	2k
5 hidden Facebook settings you should change right now!	Beebom	Fear		x	x		x				x		2018-Mar	8.4k	176k
How to check your Facebook privacy settings and other	PBS NewsHour	Literacy			x		x				x	x	2018-Mar	<1k	11k
Facebook announces new privacy settings	ABC News	Literacy				x							2018-Mar	<1k	15k
Weekend Update: Mark Zuckerberg on Cambridge Analytica	SNL	Reflective			x	x				x			2018-Apr	16k	1.7m
Anthony-Confident Facebook is moving past the data privacy i...	Aegis Capital	Literacy			x				x				2018-Oct	<1k	<1k
Full way of set privacy setting on Facebook account	Hassan Nizamani	Literacy	x								x	x	2018-Nov	<1k	<1k
Data cop says Facebook isn't protecting people's privacy	Wochit News	Fear			x								2018-Nov	<1k	<1k
Today we are going to find out what Facebook is?	Info. Channel	Literacy	x	x						x			2018-Nov	<1k	<1k
How to Locked Facebook Profile Facebook Profile is Locked	RaRe iTech	Literacy	x								x		2019-Jan	33K	2.4m
This could change Facebook forever	The Verge	Fear	x			x	x	x				x	2019-Mar	4K	174K
Watch Mark Zuckerberg Outline Facebook's New Privacy Appr...	Tech Insider	Reflective	x	x	x	x						x	2019-Apr	1K	56K
Report: Emails may prove Mark Zuckerberg knew about Faceb...	CBS News	Literacy			x				x			x	2019-Jun	<1K	7K
FTC fining Facebook \$5B over privacy and user data sharing	Fox Business	Fear	x		x		x	x				x	2019-Jul	<1K	29K
Facebook unveils new data privacy tool	Newsy	Fear			x		x	x				x	2019-Aug	<1K	<1K
			<i>2018 and on:</i> 40% 20% 67% 27% 40% 33% 20% 33% 47%												
			<i>All years:</i> 58% 23% 19% 42% 15% 42% 19% 23% 38%												

Table 1 Videos included in analysis

the tactics by which such content is rendered persuasive [13]. Each video was carefully reviewed – its script, video techniques, and the YouTube metadata (e.g., the YouTube descriptor written by the content creator) were subjected to a close reading and discussed by our research team to identify patterns in discourse. Codes corresponding to these patterns were created and used to categorize the videos (see Table 1 columns Approach, Subject Area, and Level of Detail for codes and see Results section for description of each code).

4. Results

Through discourse analysis of the YouTube Videos, we identified the privacy topics that were presented, the level of detail used to describe these topics, as well as the method used to persuade the viewer to protect their privacy. Table 1 shows this information and lists each of the videos by creation date, noting when the Cambridge Analytica scandal occurred. We elaborate on our findings in this section and present trends on the type of content presented in each of the persuasive approaches.

4.1 Privacy Topics

We identified six subject areas that were presented in the videos. The subject areas and a brief description are presented below.

Public/Private. Explains who can see what content, especially pertaining to Facebook posts and profiles.

Appropriate Sharing. Discusses what content is appropriate to share on one's Facebook page.

Data Collection. Describes the data that Facebook collects about its users.

Data Permanence. Conveys the idea that once data is posted on Facebook, it may always be out there. It is impossible to guarantee that it can be deleted from the internet.

Ads. Explains how targeted advertisements are shown to users on Facebook and the settings for controlling ads.

Finance. Discusses the financial cost of the public perceptions of Facebook's privacy violations.

While we make no claims to causation, we observed that the latter three themes (data permanence, ads, and finance) did not appear until March 2018, which coincides with the publicizing of the Cambridge Analytica scandal. These three themes have to do with the relationship between the individual and the Facebook organization, highlighting how Facebook is perceived as a possibly untrustworthy entity. Earlier videos focus almost exclusively on interpersonal privacy between individuals.

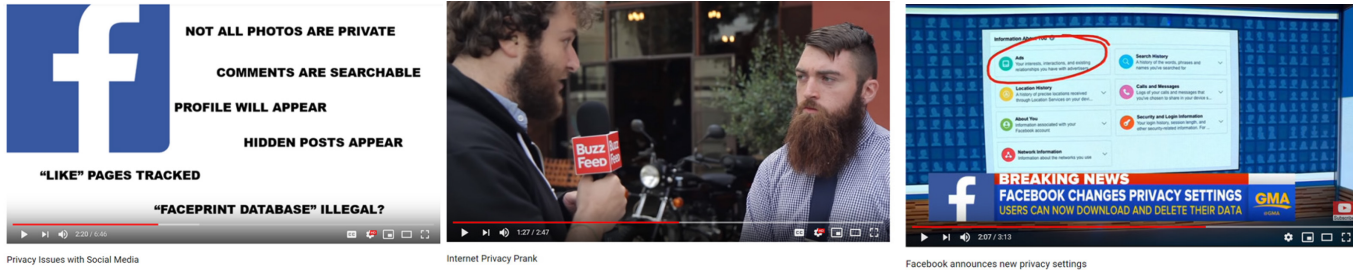


Figure 1. Examples of each approach: Fear Appeals warn about scary consequences (left), Reflective Learning surfaces one’s past behavior (middle), Digital Literacy educates the viewer about how Facebook works (right)

4.2 Level of Detail

The privacy topics were described using different levels of detail in the video. These different levels varied in the type of information they presented to describe the topic, as well as the goals they accomplished. They are as follows:

Context. Discusses the context surrounding Facebook use such as regulatory factors, societal shifts, and trends in user adoption. This explains to the user the real-world constraints and loopholes that pose privacy risks to people.

Feature. Explains what settings and features exist, what actions can be performed on the platform (e.g. post, like), and other information about how Facebook functions. Understanding a specific functionality helps the user see exactly how and what information is shared that could cause a privacy violation.

How-to. Shows how to change a given setting or perform a specific task on Facebook. This empowers users to control the functionality of Facebook such as changing defaults and selectively sharing information.

As we describe in the next section, these levels of detail were utilized to different extents by the different persuasive approaches.

4.3 Persuasive Approach

Most significantly, we found that the videos fell into three categories, which each align with interventions used in the field of education. We discuss each of these approaches and give examples of how they are integrated into the videos. While all privacy topics were subject matters in each of the three approaches, we identify gaps in how level of detail is used in each approach.

Fear Appeal. This category of videos educates users through fear of potential privacy violations – scaring users by illustrating the negative ramifications of not protecting their privacy. This approach is often used in the health literature to promote healthy behaviors by communicating the negative consequences of particular behaviors (e.g., smoking cessation, safe sex; see [18,20]). The effectiveness of such approaches is debated – in the field of education, fear

appeals lead to lower test scores compared with positive appeals to do well [15].

In our dataset, these types of videos frighten viewers by presenting scenarios of users falling victim to nefarious parties that access their data. Videos described contextual information such as the Cambridge Analytica scandal and discussed the functionality of Facebook that could lead to privacy violations. They discussed topics such as what if your information could be stolen and what could go wrong if your data is released and available to the internet. For example, several videos attempted to motivate users to action by pointing to Cambridge Analytica, a company whose access to user data may have unduly influenced voters in the U.S. 2016 presidential election. Figure 1 shows an example of how fearful, negative, and threatening language are used in these types of videos.

However, these videos failed to acknowledge the relational and informational benefits people gain in using social media [14]–[16] that might motivate them to continue heavy use of Facebook. Indeed, in lieu of any solutions, the videos seem to suggest the only recourse would be to terminate use of social media. In fact, each video does not provide more than one level of detail and so viewers who are educated thoroughly on the **context** that leads to privacy threats, do not know exactly how this is done technically through Facebook **features**. Those who learn about how **features** work are not provided with a **how-to** guide on how to change that behavior. Thus, even if the fear appeal is effective in bringing about awareness and concern, without providing guidance on how to protect their privacy, it is uncertain whether viewers would go to the opposite extreme and completely avoid social media.

Reflective Learning. This approach involves reflecting on and becoming more aware of one’s past choices and actions [3]. This is in order to encourage viewers to make more informed choices in the future (which might be incongruous with their past choices). A Reflective Learning approach has been shown to produce positive learning outcomes in the education literature where students review their past mistakes and improve going forward [10].

In the videos we analyzed, this approach took the form of uncovering actual past disclosures that the user might now regret sharing. This was in an attempt to change their attitudes and behavior for future disclosures. For example, in one video (Figure 1) an interviewer asked pedestrians to give their name for a supposed interview. Based on this one piece of information, the video showed behind-the-scenes staff members quickly searching publicly available social media posts about the pedestrian. They surreptitiously fed information to the interviewer through an earpiece. Pedestrians grew uncomfortable as the interviewer brought up personal information such as inquiring about their parents by name or asking whether they liked the grits that they ate for breakfast. Upon revealing what staff members had done, interviewees were astonished at how what they had disclosed publicly could be used by strangers and vowed to change their posting behaviors.

Like Fear Appeal videos, Reflective Learning videos each only utilized one level of detail at most. Furthermore, none of the Reflective Learning videos in our dataset explained how Facebook worked at a functional level and so interviewees did not get **feature**-level descriptions of why their information was publicly available. Even if Reflective Learning approaches motivate behavioral change, they may leave a gap in user understanding of how these undesirable results come about, or an understanding of **how-to** change settings still leaves a gap in understanding which ones should be changed and why.

Digital Literacy. This category of videos aimed to empower users by educating them to be more digitally literate. While the Fear Appeal and Reflective Learning videos tried to make an emotional appeal to viewers, this type of video attempted to make users feel more knowledgeable about Facebook privacy.

Scholars vary widely in their definitions of the skills and abilities associated with digital literacy. Definitions usually include the ability to understand and use digital information [2]. Many also emphasize the technical ability of users, such as tool literacy [19]. Research that uses general measures of digital literacy (including technical ability) to predict privacy-related online behaviors have had mixed results and which vary based on personal characteristics [17].

Drawing on these various definitions of digital literacy, we define videos in this category as attempting to educate people about 1) how information is used or produced on the Facebook platform (i.e., understand and use digital information), and/or 2) how to use Facebook features or settings (tool literacy). Figure 3 shows an example of a digital literacy video that teaches people what information is being collected about them and how to view and change that.

This was the only category of videos where we observed videos utilizing more than one level of detail. However, no one video drew on all three levels-of-detail, nor covered all topics. Several videos explained how information flows on the platform and how to change it, but did not provide the larger context of why this is important and what are the social and privacy ramifications. Thus, no one video seemed set up to provide an end-to-end privacy education intervention. Figure 1 shows an example of a video that uses the digital literacy approach.

5. Design Implications and Conclusion

Based on our analysis, we observed that existing videos range in content, level of detail provided, and their persuasive approach. The biggest gap we observed was that there is no end-to-end solution that paints the full picture of why privacy is important (*context*), what happens on the platform to endanger this (*feature*), and how to protect oneself (*how-to*). These are all necessary components in persuading one to act and enabling them to carry out that action. Certainly, the lack of such YouTube videos may point to the challenge of creating a succinct video that satisfies all these components but is still fit for YouTube consumption.

However, we see a possible design opportunity to create videos (or sets of videos) that (as a whole) integrate these three levels of detail into their explanations. Furthermore, further research is needed to evaluate how such a video could be designed – for example, it is unclear what the relative effectiveness of fear appeal, reflective learning, and digital literacy approaches are to motivating privacy-changing behavior. It is also possible that some approaches may be more effective for specific topics. For example, some YouTube genres exist for “candid-camera” which could be effective as a reflective-learning approach and perhaps the most useful for interpersonal privacy between Facebook users. Viewers could more easily anticipate threats to their relationship with others through this genre. More indirect privacy threats, such as Facebook collecting data about its users, may require a fear appeal to make clear the risks and perhaps could draw on the newscasting genre that is used in videos to heighten awareness around risky situations. Furthermore, the interplay between persuasive approaches and level of detail is another dimension that needs to be investigated.

By uncovering different types of content and approaches to educating people about Facebook privacy, this work reveals opportunities for evaluating and creating more effective privacy interventions.

References

- [1] A. Smith and M. Anderson, "Social Media Use in 2018," *Pew Res. Cent. Internet Sci. Tech.*, Mar. 2018, Accessed: Jul. 27, 2018. [Online]. Available: <http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/>.
- [2] L. Rainie, "Americans' complicated feelings about social media in an era of privacy concerns," *Pew Research Center*, Mar. 27, 2018. <http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/> (accessed Sep. 16, 2018).
- [3] A. Perrin, "Americans are changing their relationship with Facebook," Pew Research Center, 2018. Accessed: Sep. 26, 2018. [Online]. Available: <http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/>.
- [4] B. Krishnamurthy and C. E. Wills, "Characterizing Privacy in Online Social Networks," in *In WOSN: Workshop on Online Social Networks*, p. 37.
- [5] R. Gross, A. Acquisti, and I. I. I. H. John Heinz, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA, USA, 2005, pp. 71–80, doi: 10.1145/1102199.1102214.
- [6] L. Baruh, E. Secinti, and Z. Cemalcilar, "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review," *J. Commun.*, vol. 67, no. 1, pp. 26–53, Feb. 2017, doi: 10.1111/jcom.12276.
- [7] E. A. Watkins, F. Roesner, S. McGregor, B. Lowens, K. Caine, and M. N. Al-Ameen, "Sensemaking and Storytelling: Network Security Strategies for Collaborative Groups," in *2016 International Conference on Collaboration Technologies and Systems (CTS)*, Oct. 2016, pp. 622–623, doi: 10.1109/CTS.2016.0118.
- [8] B. P. Knijnenburg and D. Cherry, "Comics as a Medium for Privacy Notices," Denver, CO, Jun. 2016.
- [9] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing privacy notices: an online study of the nutrition label approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, Georgia, USA, Apr. 2010, pp. 1573–1582, doi: 10.1145/1753326.1753561.
- [10] K. E. Caine, "Exploring everyday privacy behaviors and disclosures," *Dr. Diss. Ga. Inst. Technol.*, Dec. 2009, Accessed: Feb. 07, 2019. [Online]. Available: <https://smartech.gatech.edu/handle/1853/31665>.
- [11] L. S. Liu, J. Huh, T. Neogi, K. Inkpen, and W. Pratt, "Health Vlogger-viewer Interaction in Chronic Illness Management," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2013, pp. 49–58, doi: 10.1145/2470654.2470663.
- [12] N. M. Su, "Street Fighter IV: Braggadocio off and On-line," in *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, New York, NY, USA, 2010, pp. 361–370, doi: 10.1145/1718918.1718981.
- [13] N. Phillips and C. Hardy, *Discourse Analysis: Investigating Processes of Social Construction*. SAGE, 2002.
- [14] N. B. Ellison, C. Steinfield, and C. Lampe, "The Benefits of Facebook 'Friends': Social Capital and College Students' Use of Online Social Network Sites," *J. Computer-Mediated Communication*, vol. 12, no. 4, pp. 1143–1168, 2007, doi: 10.1111/j.1083-6101.2007.00367.x.
- [15] P. Wisniewski, H. Xu, H. Lipford, and E. Bello-Ogunu, "Facebook apps and tagging: The trade-off between personal privacy and engaging with friends," *J. Assoc. Inf. Sci. Technol.*, vol. 66, no. 9, pp. 1883–1896, Sep. 2015, doi: 10.1002/asi.23299.
- [16] M. Burke, R. Kraut, and C. Marlow, "Social Capital on Facebook: Differentiating Uses and Users," in *Proc. CHI 2011*, 2011, pp. 571–580, doi: 10.1145/1978942.1979023.
- [17] Y. J. Park, "Digital Literacy and Privacy Behavior Online," *Commun. Res.*, vol. 40, no. 2, pp. 215–236, Apr. 2013, doi: 10.1177/0093650211418338.