Preliminary Analysis of Privacy Implications Observed in Social-Media Posts Across Shopping Platforms

Bethany Sumner
Augusta University
Augusta, Georgia
bsumner@augusta.edu

Gokila Dorai
Augusta University
Augusta, Georgia
gdorai@augusta.edu

John Heslen
Augusta University
Augusta, Georgia
jheslen@augusta.edu

ABSTRACT

The widespread activity of hash-tagging, especially among the Gen-Z population, and the impact of social commerce on average consumers raise questions about privacy implications and dangers of anonymous cyberstalking. In this work, we examined the privacy implications observed in hash-tag-based social-media posts (of average users and influencers) by following the trails of online shopping platform(s) product listings, consumer reviews, social-commerce policies, and influencer posts. We have conducted a preliminary analysis considering cyberstalking as one of the avenues that an anonymous stalker may use to impact the social-media user negatively. Further, we have conceptualized the trails behind hash-tagging activities in terms of a privacy threat model, the need for practical data analysis tools, and the lack of mitigation strategies at various layers. Mainly, this paper throws light on the need for more robust user privacy policies and the impact on socio-economic-privacy aspects. This paper also demonstrates the need for expanding the scope of digital investigations and DFIR tools beyond just the devices of individuals (including victims, suspects, perpetrators, and cyber-criminals) and to thoroughly prepare the forensic professionals to consider the online presence of individuals in its *entirety* including anonymous cyberstalking avenues and to raise awareness about the abuse of social networks.

ACM Reference Format:
Bethany Sumner, Gokila Dorai, and John Heslen. 2022. Preliminary Analysis of Privacy Implications Observed in Social-Media Posts Across Shopping Platforms. In *ARES 2022: International Conference on Availability, Reliability and Security, August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3538969.3544457

1 INTRODUCTION

Problem Statement: This paper primarily discusses the privacy implications observed in social-media posts (of average users and influencers). We have conducted a preliminary analysis considering cyberstalking as one of the avenues that an anonymous perpetrator may use to impact the social-media user negatively. Cyberstalking is a modern form of stalking – where perpetrators can constantly and virtually pry on a victim's online life, allowing them to hound their victim no matter the physical distance between them. Our analysis shows the problem of posting on Instagram, where one can see someone's private post if they hashtag a brand. We have also presented a comparison of various popular retail online stores integrating hashtags and user information. Our paper further discusses real-world examples of cyberstalking cases, issues faced by social-media influencers, law enforcement, and the inability of global enterprises to provide privacy-preserving, secure platforms. We have also summarized the most common set of personally identifiable information seen on online shopping websites featuring users' Instagram posts. Finally, we have discussed the need for concrete policies and practices to combat the abuse of social networks and facilitate mitigation strategies to reduce the possibilities of cyberstalking.

Social-media Posts and Influencers: Social media is rapidly becoming a dominating factor in many users' lives, where the realms of entertainment, marketing, and networking are heavily influenced by online posts. While many social media platforms, such as Facebook and Instagram, were more casual in their beginning stages, many use these online platforms to create a branding for themselves, which typically involves curated and carefully planned posts rather than a picture that was quickly taken without meticulous attention to angles and filters. The call for "casual instagram" has recently gained traction from the desire to see more random posts from content creators rather than the highly edited and typically sponsored posts that Instagram's audience has known. Many users can be considered 'influencers' – users with a large following, typically geared towards a niche audience such as fitness fanatics, earnest students, or aesthetic stay-at-home moms. When creating a following based on one's personality and lifestyle, there is the expectation that the followers will see glimpses into the influencers' life– from where they eat, shop, or travel. Having these frequent updates on someone's life can create a parasocial relationship, where the followers feel like they truly know the influencer. This form of relationship is essential for building trust, which is a crucial factor to influencers as their income from social media comes from advertisements and brand deals, which will only be offered as long as the followers trust the influencer's opinion enough to purchase what they suggest.

So, it is a seemingly necessary component of their job to share specific details about their lives, but this causes a need for concern as they are left with little-to-no privacy in their Internet life. Since internet trends and interests change so rapidly, influencers are pressured to keep the updates coming to sustain engagement, meaning they routinely share what they are doing at all points in the day. Although this is hugely normalized in Internet culture,

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3544457

this lack of boundaries puts these users at risk of cyberstalking, the "use of the Internet, e-mail, or other electronic communications devices to stalk another person" [21]. Cyberstalking differs from traditional stalking in that the perpetrator can easily hide behind an online alias, making it challenging to discover their true identity to confront, stop, or persecute them. This makes us think about the landscape and existence of apps that can be used to facilitate stalking anonymously (*insta-stalkers*). Stalking from behind a screen allows the victim's social media pages to constantly be checked on without their knowledge, meaning the user may not know someone is surveying their every move online until it evolves into more advanced cyber harassment and stalking. In 2013, 76% of cyber harassment cases escalated in severity, and cyber harassment can be a predecessor to cyberstalking [17]. About three quarters of cyber harassment cases that begin via social media escalate further[1]. Depending on the user's profile, a potential stalker may be able to obtain where the victim lives, where they go to school/work, places they frequently visit (local restaurants and gyms), and who is in their close social network through bios, photo captions, geotags, and the photos themselves.

In Section 2, we have discussed the related works and cyberstalking issues reported by other researchers. Our conceptualization of the research problem is depicted in Figure 1 followed by a detailed methodology we used to for this research in Section 4. Based on our methodology and preliminary analysis, we have summarized our observations in Section 5. In Sections 6 and 7, we have discussed traditional stalking and cyberstalking, real-world case studies, the effects of stalking on victims, and the lack of intervention policies and tools to adequately address the emerging challenges. Unlike traditional stalking methods; however, the legal system and internet policies are not extensive enough in their measures to protect and defend victims of cyberstalking crimes, and we have discussed these policies in Section 9. Further, the future work and research directions are summarized in Section 10.

2 RELATED WORK

AnonStalk [13] found that public Instagram users are vulnerable to "location disclosure without their consent," where it is possible to predict the location and future location of users through Instagram REST APIs. Although, there is a lack of real-time reporting, it is possible to monitor a target user without their knowledge: if a user is frequently at the locations they post, their future whereabouts are at risk. Baggili et al.'s [3] analysis based on an experimental design and self-reporting of cybercrimes by participants indicates that anonymity manipulation had a prominent effect on self-reported cybercrime engagement.

While some e-commerce websites remove the user's original caption when featuring their post on their gallery, others do not. If a user posted sensitive information through their caption or hashtags, it would also be featured on the website. Zhang et al. [24] developed a "systematic analysis of privacy issues induced by hashtags", and found that a user's precise location can be inferred by learning the associations between hashtags and locations. The Tagvisor system provides recommendations to users if their current caption contains location-revealing hashtags: hiding hashtags, replacing hashtags with semantically similar hashtags, or generalizing hashtags [24]. All of these uphold user privacy and utility, which is vital as hashtags can reveal location, friends, and demographics, as the authors mention. The authors also discuss that human or computer vision may be more likely to identify the picture's location if the post contains photos with a comprehensible background and hashtags, which is the case of some external e-commerce sites featuring consumer Instagram posts.

Previous literature shows that the victims of stalking are primarily women, with only a quarter of stalking victims in a meta-analysis being male [23]. There is a consensus that college-aged women and college students in general, have a higher prevalence of stalking. However, this is attributed to the age range rather than whether a person is either attending college or not [5]. Both a 2003 epidemiological study on the effects of stalking in Germany and its 2018 replicated study found that people who had been stalked had "significantly worse mental well-being than unaffected persons," with most victims facing at least one other health aliment beyond anxiety, such as increased agitation, sleep disorders, and depression [9]. The study also found women to constitute the majority of victims, noting that this is a consistent finding amongst studies on this topic [9].

Since cyberstalking could be carried out virtually, it is easier for perpetrators to remain anonymous, where they may use different Internet Service Providers (ISPs) or screen names to conceal their identity [14, 21]. The accessibility of technology has enabled an increase[2] in offending behaviors. Cheyne and Guggisberg [7] provide examples of cyberstalking actions such as mailbombing, spamming, identity theft, gaining access to the victim's computer, infecting the victim's computer with a virus, posting sexualized content along with the victim's name and contact details on the internet, using GPS to track the victim, and using social media platforms to embarrass, humiliate, and isolate victims. Since a cyberstalker can work from afar, it requires much less effort to engage with victims, meaning they can spam the victim with harassment at no cost and minimum effort [7].

3 CONCEPTUALIZATION

We have conceptualized the trails left behind hash-tagging activities in terms of a privacy threat model and the need for effective data analysis tools and the lack of mitigation strategies at various layers in figure 1.

The trail begins with social commerce and social inspiration, where brands pull from social media users (primarily Gen-Z users) that include the brand's hashtag in their caption. Because the user can post anything that does not go against the platform's guidelines, users can post pictures and captions containing sensitive information that could potentially put them in danger. Privacy policies do not forbid these posts, and the practice of sharing detailed updates of one's life on social media is becoming heavily normalized in the age of influencers. Once the user's post is featured on shopping platforms/listings/reviews or closed community chat rooms (example, the popular Sephora Insider Community [3]), there is a need

[1] http://www.haltabuse.org/resources/stats/2013Statistics.pdf

[2] https://www.fedma.org/wp-content/uploads/2018/05/Global-data-privacy-report-FINAL.pdf

[3] https://community.sephora.com/

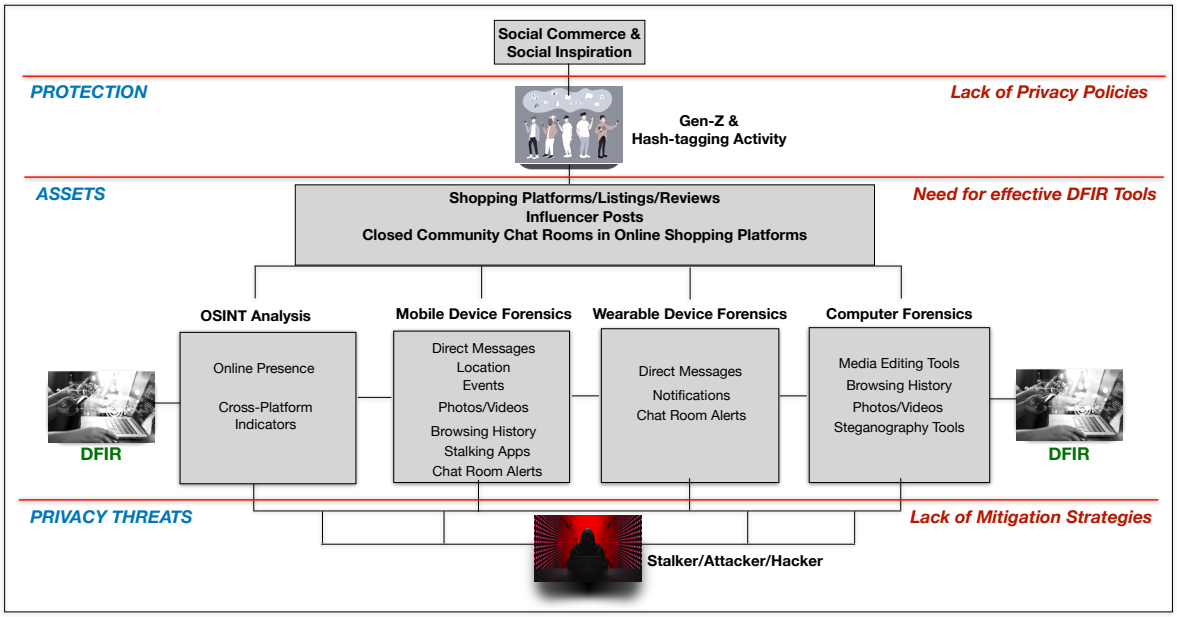


Figure 1: Conceptualizing the Big Picture of Hash-tagging, Cyberstalking, Privacy Threat Model and DFIR

for deeper Digital Forensics and Incident Response (DFIR) tools in the form of mobile device forensics, wearable device forensics, and computer forensics and even Open-source Intelligence (OSINT) analysis. The type of data that can contain evidentiary information in each of these DFIR categories is listed in figure 1.

Although cyberstalking is just one avenue where a user's personally identifiable information can be presented outside of the original social media platform, a perpetrator can use these schemes to harass the victim and advance their harassment. For this reason, it is crucial for effective privacy threat mitigation tools for preventing a privacy attack on these featured users. This is pictured in the form of assets, protection and privacy threats at various conceptual levels in figure 1.

A stalker/attacker/hacker can find ample information on unsuspecting users through a mix of these avenues. Thus, it is essential for mitigation strategies to reduce the threat of the culprit to the victim's safety while possessing compromised sensitive information. As discussed later in the paper, current practices to aid cyberstalking victims are not adequate. Instead, social media platforms, law enforcement, and the legal system dissuade victims from taking their unnerving situation seriously. The effects of cyber harassment on victims cannot be dismissed, and more robust mitigation strategies are needed when privacy policies and DFIR tools are too late to help victims.

4 METHODOLOGY

4.1 Hashtag Profiling

In this work, the following steps were adopted for examining the privacy implications observed in hash-tag based social-media posts (of average users and influencers) using the trails left behind by online shopping platform(s) product listings, consumer reviews, social-commerce policies, and influencer posts:

- Identify popular online shopping platforms (accessible in the United States) present on social-media that have created a *hashtag* associated with their brand for consumers to use when posting on social media (while wearing, discussing, or featuring a product from the brand)
- Determine how the brand highlights this hashtag externally (i.e., a gallery on their external shopping website presenting all posts using that hashtag, or including the user's post under the product listing on their website)
- Identify what information from the hash-tagger's original post is visible on the external website (i.e. username, caption (text and hashtags), profile picture)
  - Note: A random user profile search was conducted to check if a user's post is visible on the external website even if they have a private Instagram account, which is the case. The authors of this paper have taken all precautions in place to not to reveal any consumer's/user's personally identifiable information in this publication.
- Identify the landscape and existence of stalking applications in popular mobile app market stores using keyword-based search.

4.2 Analysis of App Markets

Insta Stalker Apps: Instagram stalker apps are a type of application becoming more popular as usage of Instagram has grown. These apps are designed to allow users to be able to track which Instagram users stalk their profile, in particular, those Instagram users who view their profile often. Instagram does not support this use case natively in their application, so third-party apps fill in this role. We scraped two App Stores, the Google Play Store and SlideMe,

which is a third-party Android app store for Instagram stalking apps with varied results. SlideMe was scraped for apps pertaining to the keywords anonymous-stalking, stalking, insta-stalker, stalk, stalker, instagram-stalker, cyber-stalker, and cyber-stalk but found limited results, with most not pertaining to Instagram stalking. The Google Play Store was the other app store we analyzed. It was only scraped for the keyword 'anonymous-stalking' and we found the presence of 350 applications related to Instagram stalking, along with results for stalking other social media applications. Some of these results appeared to be real, but there were countless apps with poor reviews with users claiming that the app did not work.

Next, we have reported our observations based on our preliminary analysis to learn about the intersection of social-commerce, branding and rising demand for social-media influencers.

5 OBSERVATIONS

Diminishing Boundaries: The boundaries between social media and people's personal lives continue to diminish, especially in the era of "online influencers." While most Instagram users have a personal page, where their audience consists of mostly people they know offline, there is a growing number of users who generate an online presence to gain a large following and engagement rate.

Social-commerce and Demand for Influencers: A content creator with a loyal following (which can be seen in consistent engagement such as likes, comments, shares, and reposts) may attract brand deals from companies looking to advertise their products through the growing number of influencers. In recent years, rather than companies solely advertising their business or products on the Internet through their own brand's social media page, many are reaching out to social media influencers to do the job. Depending on the influencer's engagement and the company's budget, the influencer may gain free products or compensation for posting an agreed-upon amount of content for the brand. Here, the brand can spread its product to a wide audience, who will likely trust the influencer's recommendation, with less money and time spent on curating the advertisement themselves.

Branding Linked with Hashtags: Although this new marketing trend has largely been between established influencers and brands with an online presence, there has been a new marketing trend evolving – where the company may be able to gain exposure without providing physical or financial compensation. Likewise to the influencer, brands are hoping for more engagement on their social media pages to routinely come upon more users' feeds and remind them of their product. Engagement can be gained through advertisements and directly interacting with the consumer. The latter has been done through branded hashtags, which is a mechanism that categorizes all posts with the same hashtag in the captions under one feed. Since its early stages, hashtags have been a feature of *Instagram*, and users may use them in their captions to expand on the picture or text in the caption, but companies are now using hashtags to promote their "branding." Some examples of these branded hashtags are Aerie's hashtag AerieREAL, American Eagle Outfitters' AEJeans and AExME, Earthbound's EarthboundTrading, Loft's LOVELOFT, and Rue21's YOUinrue– all of which are American clothing retail stores that have an associated Instagram page for their company.

Public vs. Private Profile Settings: A 'public' Instagram account means that anyone could search the user's Instagram handle and view their pictures, any geotags (a geographic location the user can associate with their post), hashtags, or likes/comments on the post. If User X sets their privacy settings to 'private,' only Instagram users who request to follow them and are accepted by User X can access their pictures and the previously mentioned information. If someone with a private Instagram account posts a picture with the caption "First day at school! Brand'sBack2SchoolHashtag", only their approved followers will be able to see this post on the corresponding hashtag page [2]. Often, tagging a brand in a picture or using their associated hashtag is an effort to potentially gain exposure, such as page views, likes, comments, or followers, from being featured on the corresponding hashtag page.

Potential Exposure due to Reposting: All of the mentioned brands and many others that have a hashtag affiliated with their business promote the chance to be reposted on the brand's Instagram page and/or featured on their external e-commerce website. Depending on the brand, they might feature the user's picture under the listing for the product that the user is wearing/using, or they might have a dedicated gallery on their website to feature social media users who have used the brand's hashtag in an Instagram caption. It is customary for a company to ask for permission to repost/feature the user's picture – either by commenting on the user's post or through direct message. Unlike an influencer's exchange with a brand, an average user does not receive free product or financial compensation for the free advertisement done with their content; however, the user does gain potential exposure for their post and Instagram page, as well as simply the notion of being acknowledged by a brand with a large following. If a user grants permission to use their photo, the picture and accompanying caption is now visible on the user's public profile, the hashtag page(s), and where the brand features the post (i.e., on the company's Instagram page or an external website).

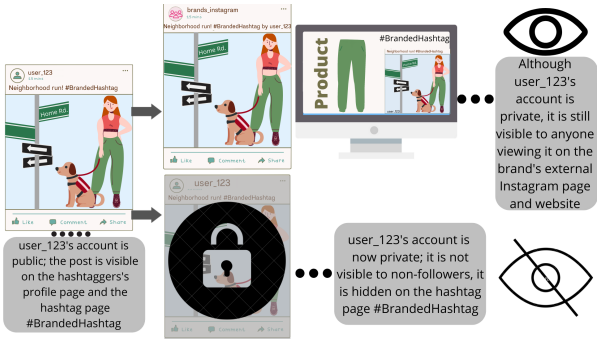


Figure 2: Conceptualizing the Visibility of Private Account Settings on Instagram and External Websites

As seen in figure 2, if a user decides to change their account privacy settings from 'public' to 'private', the post is no longer visible

to other users who do not follow the original poster, and the post is hidden on the hashtag page from non-followers. However, suppose a brand featured the user's post prior to the privacy change. In that case, the post (along with the username and caption) is still *visible* to anyone viewing the brand's Instagram page or external website, despite the original user changing their account settings [16].

Hashtags/Branding in the U.S. Retail Online Stores: In figure 3, we have shown a summary of the preliminary analysis we conducted to learn about various retail stores and how they integrate hashtags into their online shopping platforms. Various American-based retail stores are featured – all of whom have a designated Instagram hashtag for their consumers to use when posting with one of their products. The six brands featured in the figure were chosen as they are well-known, popular brands (all having an online presence), mainly with a younger population following. Other brands not discussed may also have branded hashtags, and it is suspected that more brands will follow suit and implement this practice in the future.

In the second column, the brand's hashtag is shown; if a consumer wishes to share a picture wearing/using the company's product, the user has an option to use this hashtag in the caption of their Instagram page with the chance for the company to feature the user's post on their retail website. The third column, username, refers to whether the company keeps the consumer's username visible on the featured post once shown on the external website. All of the discussed brands show the user's handle, providing credit to the user except for Pacsun, who will first repost a user's post to their own page. So, in this instance, if a user uses the brand's hashtag on their personal post, Pacsun will repost the picture to its own Instagram page (@pacsun), where the brand may tag the user in the caption. Due to this, when looking at the Pacsun website gallery, all users are Pacsun. The profile picture column refers to if the company features the user's Instagram profile picture on the external website when featuring their post.

Reporting on Variations Observed: In almost all cases, these brands replaced the user's picture with the first letter of their username (so @InstagramUser would have an "I" against a solid-colored background for their profile picture on the external website). American Eagle and Aerie (a sub-brand for American Eagle Outfitters) do not have a profile picture next to the username; instead, it features the Instagram logo. Rue21 removes the profile picture and does not replace it with anything else. When posting to Instagram, users can include a caption and/or hashtags; the fifth column caption/hashtags in figure 3 show whether the brand keeps the user's caption, which may include hashtags, on the featured post on the external website. Out of the brands highlighted, only Loft and Rue21 remove the user's caption, even if a caption is attached to the original post on the user's personal Instagram page. The sixth column, Infinite gallery, refers to the gallery of featured consumer posts on the brand's external website. Those with a checkmark have a dedicated space on their brand's website to showcase everyone featured with their hashtag. The 'infinite' gallery refers to the brand not having a limit on how many posts it will feature so that someone could scroll through all featured posts; even ones reposted years ago. Those who do not have an infinite gallery only showcase a limited number of posts.

Types of personally identifiable information seen on external shopping websites featuring consumer's Instagram post:

- Street signs in neighborhoods and apartment complexes
- Front doors with the apartment number visible
- Distinct location (such as local restaurants, hair salons, and movie theaters)
- Persona and observable traits (such as sports, fitness, art, fashion)

Examples of these identifiers featured on external shopping websites can be seen in the Appendix (Section 12). Various websites are featured, and there are varying levels of personally identifiable information present. For instance, in figure 4 the right example shows a user with an apartment complex and street sign in the background. In figure 5, however, this post on Pacsun's website does not feature much sensitive information. There are two examples in figure 5 of user's sharing a picture featuring their apartment number/neighborhood street sign, which is then featured on brand's external websites without any censoring. The authors of this paper have blurred out these features, but they were clearly visible on the websites.

With the above observations, it is clear that consumers' personally identifiable information can be broadcasted on these websites, and users may not think about the privacy implications before using a brand's hashtag in their caption. As discussed later in the paper, users must be cautious with the information they post online and adequately protect their privacy on each platform their content is featured. Otherwise, having a user's sensitive information, such as their apartment's street sign, can create or escalate cyber harassment, cyberstalking, or even physical stalking.

6 TRADITIONAL STALKING

Before discussing the effects of cyberstalking, it is crucial to understand the means and modes of facilitating traditional stalking, the reported effects of stalking on victims (especially in intimate partner violence (IPV) scenarios), and the primary reasons why stalking cases go underreported, and the response from law enforcement. Since attitudes and laws regarding cyberstalking are largely based on traditional stalking, it is essential to understand the tactics and effects of stalking. Traditional stalking differs in its legal definition from state to state; however, it is generally defined by the National Institute of Justice as "a course of conduct directed at a specific person that involves repeated (two or more occasions) visual or physical proximity, non-consensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear" [1]. Because stalking involves a pattern of behaviors, it can be challenging to discern when situations should classify as stalking, harassment, or just plain annoyance. Additionally, almost all states require the following three claims to be proven beyond a reasonable doubt: first, a course of conduct/behavior, where there are two or more committed acts that present a pattern of behavior; second, the presence of threats that would cause fear in a reasonable person; third, the intent to cause fear in the victim, meaning the stalker must be intentional in their actions (in some states, this requires proof of the desire to

Company	Hashtag	Username	Profile Picture	Caption/ Hashtags	Infinite gallery	Special Notes
American Eagle Outfitters/ Aerie	#AerieREAL #AEJeans #AExME	✓	✗	✓	✓	-
Pacsun	#InMyPac	User sometimes tagged	✗	✓	✗	Pacsun reports all pictures to their page first
Earthbound	#Earthbound Trating	✓	✗	✓	✓	Mix of personal photos and home decor
Rare Beauty	#RareRoutine	✓	✗	✓	✗	Mostly makeup pictures; not many with backgrounds; No separate gallery page (moving pictures across the website instead)
Loft	#LOVELOFT	✓	✗	✗	✓	Clicking on picture does not enlargen it (like other websites do)
Rue21	#YOUinrue	✓	✗	✗	✓	Uses Bazaarvoice to get Instagram gallery

Figure 3: Comparison of Various Retail Online Stores in the United States Integrating Hashtags and User Information

cause fear in the victim; in others, the intent to complete the action suffices) [11].

Stalking and IPV: The legal processing of stalking differs from other crimes in the emphasis on the victims' feelings [7]. Typically, this is not a consideration when prosecuting someone, but stalking can encompass a wide variety of actions that may be considered standard communication or even flattery. The National Intimate Partner and Sexual Violence Survey (NISVS)[4] defines stalking tactics as: "unwanted phone calls, voice or text messages, hang-ups; unwanted emails, instant messages, messages through social media; unwanted cards, letters, flowers, or presents; watching or following from a distance, spying with a listening device, camera, or global positioning system (GPS); approaching or showing up in places, such as the victim's home, workplace, or school when it was unwanted; leaving strange or potentially threatening items for the victim to find; sneaking into victims' home or car and doing things to scare the victim or let the victim know the perpetrator had been there".

Reported Effects on Victims: Beyond affecting their physical health, stalking has damning effects on the victim's social realm, as they are pressured to change their routine, where they regularly go, what information they share with others, and choose to stay home more often [7]. Further, a victim's financial and work life can suffer, as the National Crime Victimization Survey found that "more than half of stalking victims lost 5 or more days from work," with an estimated 130,000 victims being fired or asked to leave due to the consequences of stalking on their work-life [4] [5]. Overall, stalking can cause turmoil in various aspects of a victim's life, making it feel like their stalker has a grasp on every part of them.

Underreported Stalking Cases: In addition to the distress caused by their stalker, victims face further turmoil when trying to stop their situation from continuing or escalating further and when trying to prosecute their stalker. The first hurdle for a victim is reaching out for help. Because stalking is a significant umbrella term that can be executed through countless methods, victims are likely to downplay their situation as innocuous, making it improbable they will reach out to law enforcement – as seen by the estimated 50-80% of stalking cases going unreported [5]. Further, the previously mentioned 2003 and replicated 2018 replicated epidemiological studies found that in both years, a high proportion (53.2% in 2003 and 47.9% in 2018) of victims had a dearth of knowledge of the scope of legal action they could take [9].

Limitations to Reporting a Case: When victims do reach out, their list of troubles may increase if they are not taken seriously by law enforcement or do not fall under the protection of the law. In an interview with law enforcement respondents providing their perceptions of the threshold for making reports for stalking victims, one respondee addressed the issue: "Police are looking for that pattern of behavior, 50 texts in one day. 50 voicemails in one day. Something that extreme" – a smoking gun that clearly shows there is an issue [5]. However, even if a police officer does not acknowledge the case as severe enough to make a report, the victim's unrest and anxiety cannot be dismissed.

7 CYBERSTALKING AND LEGAL SYSTEMS

7.1 Offline/Online Anti-Stalking Laws?

Likewise to traditional stalking, after a comprehensive analysis of 53 studies, it was found that females are more likely to be victims of cyberstalking [18]. The United Nations Broadband Commission's Working Group on Gender found that just under three-quarters of women face online violence in the form of threats, harassment, and stalking [15]. Additionally, studies included in this analysis showed that individuals who spent more time on social media were more likely to experience cyberstalking [18], which is concerning with the rise of social media in every aspect of life for both average users and influencers alike.

Although the offender's presence does not physically threaten the victim (unless a scenario of cyberstalking were to escalate into occurring alongside physical stalking), the tactics of cyberstalking must be given the same level of concern and sympathy as if it was a case of offline stalking. The Attorney General recommends that although some cyberstalking activities may not classify as illegal, it is still a serious matter as it may prelude further stalking and violent behavior [21]. Although both users and law enforcement benefit from a safer online environment, there is not as much awareness about the dangers even amongst Internet users, which leads

[4]https://www.cdc.gov/violenceprevention/pdf/nisvs-statereportbook.pdf

victims to not knowing how to address cyberstalking situations. Similarly as discussed earlier with traditional stalking victims, not knowing of the legal resources they could use contributes to this lack of knowledge of how to respond in these situations. If cyberstalking does fall under legal guidance, less than a third of states in the U.S. have "anti-stalking laws that explicitly cover stalking via the Internet, e-mail, pagers, or other electronic communications," which makes it difficult for victims to receive legal justice [21]. As previously mentioned, the ambiguity of defining traditional stalking has hindered sufficient protections being placed for those who have faced or are currently experiencing stalking. This problem is amplified when it comes to digital stalking, as it is much more difficult to prove someone is at fault with an anonymous guise and unknown location.

As cyberstalking does not always give way to physical or in-person violence, there are many incidences of victims not being taken seriously. Without law enforcement having the proper training and awareness, they might not know how dangerous and damaging cyberstalking is to the victim, especially if left unaddressed.

7.2 Criminalizing Cyberstalking

An important distinction between traditional stalking and cyberstalking is the regulations and protections for victims when a case arises. Since cyberstalking is a relatively new phenomenon, compared to traditional physical stalking, some states do not have adequate laws to sufficiently help victims. A daunting issue is that there is no legal standard for cyberstalking, as there is no direct federal law addressing cyberstalking, but rather cyberstalking is prohibited at the federal level due to falling under the umbrellas of 'threatening communication' and harassing, threatening, abusing, annoying anonymous telecommunication which is protected by laws 18 U.S.C. 875(c), 47 U.S.C. 223, and the amended Violence Against Women Act [16]. Although most U.S. states have laws criminalizing cyberstalking, the legal definitions vary among them, meaning a victim's case may be overlooked if it is not considered severe or threatening enough for their state, regardless of the detriment faced by the victim. This was seen in Pickett's case, where the creation of over 500 accounts to harass her was not enough to obtain a restraining order, despite the fact that the perpetrator's identity is known and now lives in the same area as Pickett [16] [8]. Unfortunately, many other victims also do not fall under the legal standing of cyber harassment and cyberstalking, so they are left overlooked and unassisted. Without a standard cyberstalking definition recognized across all states, some victims may find themselves stuck in their situation with no legal guidance to help them get out.

7.3 Legal Ambiguity

For many states, new laws were not created to protect against cyberstalking specifically, but instead, cyberharassment provisions were added to existing harassment and stalking laws. This is a disservice to those suffering from cyberharassment and cyberstalking, as, without clear guidelines specific to the online realm, successful prosecutions are hindered as the laws "unintentionally create difficulties in proving intent, credible threats, and surveillance" [8]. This legal ambiguity leaves victims without the proper resources to end their unnerving situation.

7.4 Collaboration - Lawyers & Technologists

Even in states with strong efforts to systematize cyber victimization, the enforcement of these laws can be difficult if law enforcement agencies are not equipped with proper training and knowledge in combating specifically cyber-related crimes [17]. To victims' dismay, many local police stations solely focus on responding to physical altercations with little concern for online violence, both in the training of their officers and what they decide to spend resources on [19]. This can be seen with Rebecca Watson, a digital journalist who received direct death threats. Police claimed they were unable to help her because the stalker lived in a different state than her [19]. Further, after finding a website containing descriptions of killing women and pictures of Watson herself, she was able to identify his age, location, and name. However, she was still left helpless as the man's local police department directed her to her local police station – who claimed they could not do anything unless he physically acted against her [19]. Unfortunately, this is not the only example of legal authorities dismissing severe threats because they occurred *online*. For instance, Jane Seymour's (American-British actress) daughter Flynn Adams had her family's home address posted online and advertised as a place to fulfill "personal fantasies" (source 4). Adams faced dismissal by the security heads she was in contact with, ranging from legal personnel at the platforms where the harassment took place, to both local and federal law enforcement. Further, the Judge of her case stated Adams should not have a computer if she does not like what people post online. While recounting her experience, she stated the "situation has not been resolved, not in a meaningful way" (source 4). Although the identity of the culprit was identified, she did not gain peace as "law and technology have not caught up with each other yet," comparing her situation to a feedback loop where law enforcement wanted the social media platform to resolve the issue. However, the platform instructed her to go to law enforcement (source 4).

7.5 Cybercrimes and Costs

There have been calls from academic scholars to put more significant effort into preventing cyber victimization, looking toward both the effects on the victims and the cost of resolving cybercrimes as motivations. Cumulatively, cybercrime costs Americans millions of dollars, with cyber victimization having "severe financial and emotional repercussions" [17]. The American Journal of Criminal Justice points to an altered Gang Resistance Education and Training Program that highlighted cyberbullying and cyberstalking, which could educate police officers and hopefully reduce these behaviors and the cases that get directed to the courts [17]. Further, improvements must be made even in stations with a foundation for combating cybercrime at their stations. Often, a sole officer, or only a small group of them, receives training on cybercrime investigation and management [17].

In order to help those facing a cyberstalking threat, it is crucial for all officers to cover these topics in basic training; however, this can seem like an expensive investment for communities with already straining budgets, and this solution will take time to catch

up with what is needed from law enforcement. Note that funding is a critical issue, recognizing that it may take a high-profile case for a community to recognize the dangers and prompt public officials to enact preventative measures [20]. Further, the Police Executive Research Forum[5] notes how staffing is an essential part of creating a cybercrime unit, with the possible need to hire outside of the current agency while recognizing that funding is stretched for many units. The Forum[6] suggests making a case to their community to raise the operating budget (which can be challenging to do proactively in a community where they have not seen the dangers of cyberstalking yet), grand funds, or forfeiture funds . Although the increased focus on cybercrimes in many police departments is desperately needed, this cannot be relied on to help those in danger currently. With the increased social media activity by the Gen-Z population and the lack of sufficient proactive privacy-preserving measures by corporates, the dangers of cyberstalking can explode if not mitigated soon. Technology-facilitated private online chat rooms and insider communities are harder to track unless social media platforms and insider community platforms enforce stricter content moderation and privacy-preserving platform architecture.

7.6 Awareness

Beyond law enforcement, there must be a greater awareness amongst all social media users (and those frequently on other forms of the internet) of how seemingly harmless posts can heavily compromise personal information. Further, cyberstalking victims must not dismiss their own experiences, as 41.6% of victims did not contact the police due to: fear of escalation, guilt/sympathy, and self-blaming (in a 2011-2014 sample of 305 individuals (274 of whom have experienced online harassment) [2]. With further awareness about the seriousness of cyberstalking, victims may acknowledge what they are experiencing rather than push it aside. Even what victims see as seemingly minor grievances can heavily affect their lives or escalate further. Ideally, cyberstalking practices can be slowed or entirely prevented with users' having a high degree of comprehension of how malicious users can use the information present on their social media posts. Although determined stalkers can scour the internet for sensitive information even with high caution and awareness, the current attitude of what is acceptable to share online makes the perpetrators' job even easier.

7.7 Recent Cyberstalking Incidents

With the boundaries between social media and people's personal lives continuing to diminish, sharing personal identifying information on the internet with little thought given to personal safety and security is commonplace. A study conducted by the Global Data and Marketing Alliance (GDMA)[7] found that 77% of people classify themselves as pragmatic or unconcerned about sharing their data. Recently, an American celebrity[8] endured cyberstalking by a registered sex offender, who began harassing her on her Instagram by leaving disturbing comments. In the Facebook Watch's Red Table Talk cyberstalking episode, the celebrity commented that the stalker checked the geo-tags on her photos (an Instagram mechanism that allows a user to connect a geographic location with their post), which allowed him to see all of her daily actions and get her patterns down. His online harassment and cyberstalking later led to physical stalking. A social media influencer[9] experienced cyberstalking and faced challenges in receiving a restraining order, where her stalker created over 500 fake social media accounts to leave harassing comments and direct messages.

8 DISCUSSIONS

According to the Cyber Crimes Division of the Massachusetts Attorney General's Office[10], cyberstalking can occur between individuals with a prior relationship, or between two strangers where victims have posted a "treasure-trove of personal identifying data on social networking sites including their age, phone numbers, personal interests, and photographs." As seen in the photos collected from various e-commerce websites that share consumer pictures through Instagram hashtags, some users do not hesitate to share pictures with self-identifying backgrounds, such as apartment complexes, street signs, and places they may frequently visit. Most of the consumer Instagram pages featured on these websites have their privacy setting set to public, meaning anyone who searches their username can see their entire profile. However, if a user with a public profile allows a brand to repost or feature their picture on an external website but then changes their profile settings to private, the picture will still be visible on that external network[11], even if it no longer shows up under the hashtag's Instagram page.

Special Agent Siobhan Johnson[12], with the Federal Bureau of Investigation, recommends making "social media accounts private and NOT oversharing personal information," and that if cyberstalking has already been taking place, he recommends erasing their digital footprint. However, if consumer privacy is important to an e-commerce business, there should be precautions when reposting or featuring their customer's photos. 51% of consumers said, "trust was key in their decision to share information with a company,"[13] but as seen in previous examples, a brand may not analyze a customer's privacy when reposting for business exposure. Since access to a user's information is what gives power to cyberstalkers, there is a need for a privacy-preserving framework that can throttle anonymous cyberstalking.

Officials recommend that consumers take it into their own hands when protecting their privacy online; however, with the rise of social media, it is becoming normalized to broadcast personal information on the Internet. The use of social media, such as Instagram, can let stalkers track their targets virtually by studying their pictures, captions, and any hashtags or geo-tags. There are many cases of cyberstalkers gaining their information through social media;

[5]https://www.iacpcybercenter.org/wp-content/uploads/2018/06/Starting-a-Cyber-Crime-Unit.pdf
[6]https://www.iacpcybercenter.org/wp-content/uploads/2018/06/Starting-a-Cyber-Crime-Unit.pdf
[7]https:/ /www.fedma.org/wp-content/uploads/2018/05/Global-data-privacy-report-FINAL.pdf
[8]https://nypost.com/2021/10/07/willow-smith-says-pedophile-stalker-broke-into-her-home/
[9]https://www.facebook.com/redtabletalk/videos/cyberstalking-how-to-protect-yourself/548778832852755/
[10]https://www.mass.gov/info-details/cyber-crimescyber-stalking-
[11]https://help.instagram.com/164895810321211
[12]https://abc7chicago.com/cyberstalking-prevention-prevent-how-to/5990204/
[13]https:/ /www.fedma.org/wp-content/uploads/2018/05/Global-data-privacy-report-FINAL.pdf

however, there is a lack of studies focusing on the potential dangers of external websites featuring users' posts, where their privacy settings are ignored. Although there is a focus on protecting one's information on the user's individual page, there are not enough safeguards to ensure the brand does not feature posts with potentially sensitive, identifiable information on their website.

9 SUMMARY - LAW AND POLICIES

Unlike traditional stalking methods; however, the legal system is not extensive enough in its measures to protect and defend victims of cyberstalking crimes. This fact, along with the reality that even when cyberstalking is reported, which is rare; law enforcement agencies are generally ill-equipped to investigate them This significantly compounds the problem of successfully prosecuting these types of crimes [22]. Chang [6] notes three major challenges of law enforcement in investigating cyber stalking. First, law enforcement personnel are challenged by a lack of understanding and awareness of cyberstalking because it is a relatively new type of crime and they may choose not to investigate complaints as they can underestimate their seriousness. Second, given the global reach of the internet, law enforcement can easily run into jurisdictional problems, especially if the crime is committed in another state or country. Finally, law enforcement personnel may lack the expertise to properly identify or gain access to the online accounts of cyber stalkers, especially if anonymizing tools were used to make attribution more difficult [6].

Additionally, there has been an issue within the United States regarding how cyberstalking is conceptualized and prosecuted by individual states, although most states take one of two approaches. In the first approach, states would make modifications to existent laws against traditional stalking and update them by including the various digital means a stalker may use to conduct the crime (e.g., internet applications such as Facebook or Instagram). The second approach used by fewer states was to create new laws specifically aimed at preventing stalking using digital means that were not just extensions of existing laws [12]. Although this second approach seems more effective in catching the various nuances and modalities of stalkers who use information and communication technologies to commit their crimes, it is problematic in the sense that the added nuance prevents the establishment of a nationally agreed upon definition of cyberstalking [10] or a widely accepted national rubric for sentencing laws.

10 FUTURE WORK

The research conducted in this study primarily focuses on the dangers of personally identifiable information present on external shopping websites that feature Instagram user's posts. Although Instagram seems to be the primary social media platform for brands directly interacting with users, other platforms (such as Facebook, Twitter, TikTok, etc.) should be reviewed in regards to companies wanting to work with both average users and influencers. While it has been shown this is an issue between Instagram users and brands, it is unknown how frequently this occurs on other social media platforms. Instagram hashtags appear to be the central way of engaging with consumers, but this does not minimize the threat and dangers of users' privacy being overlooked on other platforms. Future works should quantitatively show the frequency and prevalence of users' posts on all of these social media platforms featured on external websites that reveal personal information, risking their safety and privacy.

Additionally, a major analysis of the problem should be conducted in which the data of all public posts featured by brands on an external website can be pulled automatically through scripting. This paper has identified several concerning features seen on these websites (street signs, distinct local locations, home identifiers such as pictures in front of their house/neighborhood and apartment numbers), but it is currently unknown how extensive this issue is in a quantitative way. The percentage of these occurrences would help motivate and inform the need for action, which is something the authors are interested in looking into.

11 CONCLUSION

The similarities between traditional stalking and cyberstalking are seen in the demographic of victims and attitudes towards victims. Although traditional stalking has been a well-known issue for much longer than cyberstalking, it still faces setbacks in law enforcement and the laws protecting victims. These grievances only deepen when a victim is faced with cyber-harassment or cyberstalking, as many cyberstalking laws are amended to physical stalking legislature. The foundation of these laws can leave traditional stalking victims unhelped, and without direct laws addressing these cybercrimes, victims of cyberstalking are dismissed or left abandoned in ending their problem.

The abuse of social networks calls for comprehensive policies and practices to ensure social media users are protected and thus less at risk of a potential cyberstalker. Practical DFIR tools are crucial in combating the abuse of publicly sensitive information, even when the user's profile settings are set to private. Forensic professionals must be aware of the various new avenues perpetrators can obtain information, such as OSINT analysis, mobile device forensics, wearable device forensics, and computer forensics.

Without these needed efforts, victims are left vulnerable as their information is visible, and there is insufficient help from law enforcement, the social media platforms, and global enterprises. As sharing every aspect of one's life becomes more normalized, it becomes more urgent to place these protections and mitigation strategies to fruition. With 350 mobile applications related to Instagram stalking and other social media platform stalking, it is apparent that readily available stalking tools are a current and growing issue. Although many apps have reviews claiming the apps are not functional, there is a high demand for cyberstalking services, allowing perpetrators to further prey on their victims with ease.

ACKNOWLEDGMENTS

The authors would like to thank Prof. Ibrahim Baggili, Professor, Computer Science at Louisiana State University - Center for Computation and Technology for his valuable suggestions and insightful comments on this work, and Seth Barett, Undergraduate Research Assistant, School of Computer & Cyber Sciences for helping in the mobile stalking app analysis. The authors would like to acknowledge National Science Foundation (NSF) (Award number: 2131509) for supporting this project through supplemental funding.

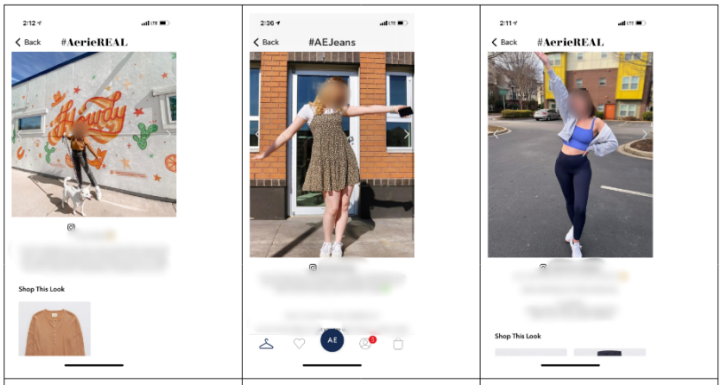
REFERENCES

[1] Women Act. 2007. Domestic Violence, Stalking, and Antistalking Legislation. (2007).
[2] Haider M Al-Khateeb, Gregory Epiphaniou, Zhraa A Alhaboby, James Barnes, and Emma Short. 2017. Cyberstalking: Investigating formal intervention and the role of Corporate Social Responsibility. *Telematics and Informatics* 34, 4 (2017), 339–349.
[3] Ibrahim Baggili and Marcus Rogers. 2009. Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity. (2009).
[4] Katrina Baum. 2011. *Stalking victimization in the United States*. Diane Publishing.
[5] Tim Boehnlein, Jeff Kretschmar, Wendy Regoeczi, and Jill Smialek. 2020. Responding to stalking victims: Perceptions, barriers, and directions for future research. *Journal of family violence* 35, 7 (2020), 755–768.
[6] Wei-Jung Chang. 2020. Cyberstalking and law enforcement. *Procedia Computer Science* 176 (2020), 1188–1194.
[7] Nicola Cheyne and Marika Guggisberg. 2018. Stalking: An age old problem with new expressions in the digital age. *Violence against women in the 21st century: Challenges and future directions* (2018), 161–190.
[8] Cassie Cox. 2014. Protecting victims of cyberstalking, cyberharassment, and online impersonation through prosecutions and effective laws. *Jurimetrics* (2014), 277–302.
[9] Harald Dreßing, Peter Gass, Katharina Schultz, and Christine Kuehner. 2020. The prevalence and effects of stalking: a replication study. *Deutsches Ärzteblatt International* 117, 20 (2020), 347.
[10] Aimee Fukuchi. 2011. A balance of convenience: The use of burden-shifting devices in criminal cyberharassment law. *BCL Rev.* 52 (2011), 289.
[11] Mary Graham. 1996. *Domestic Violence, Stalking, & Antistalking Legislation: An Annual Report to Congress Under the Violence Against Women Act.* DIANE Publishing.
[12] Steven D Hazelwood and Sarah Koon-Magnin. 2013. Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology* 7, 2 (2013), 155–168.
[13] V Kanakaris, K Tzovelekis, and DV Bandekas. 2018. Impact of AnonStalk (Anonymous Stalking) on users of Social Media: A Case Study. *Journal of Engineering Science & Technology Review* 11, 2 (2018).
[14] Puneet Kaur, Amandeep Dhir, Anushree Tandon, Ebtesam A Alzeiby, and Abeer Ahmed Abohassan. 2021. A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change* 163 (2021), 120426.
[15] Priya Kumar, Anatoliy Gruzd, and Philip Mai. 2021. Mapping out Violence Against Women of Influence on Twitter Using the Cyber–Lifestyle Routine Activity Theory. *American behavioral scientist* 65, 5 (2021), 689–711.
[16] Mirela Loftus. 2016. The Anti-Social Network: Cyberstalking Victimization Among College Students. *Journal of the American Academy of Child & Adolescent Psychiatry* 4, 55 (2016), 340–341.
[17] Catherine D Marcum and George E Higgins. 2019. Examining the effectiveness of academic scholarship on the fight against cyberbullying and cyberstalking. *American journal of criminal justice* 44, 4 (2019), 645–655.
[18] Catherine D Marcum and George E Higgins. 2021. A Systematic Review of Cyberstalking Victimization and Offending Behaviors. *American Journal of Criminal Justice* (2021), 1–29.
[19] Emma Marshak. 2017. Online harassment: A legislative solution. *Harv. J. on Legis.* 54 (2017), 503.
[20] Christa Miller. 2006. Cyber stalking & bullying: What law enforcement needs to know. *Annotation* (2006).
[21] US Dept of Justice. 1999. Cyberstalking: A New Challenge for Law Enforcement and Industry: A Report From the Attorney General to the Vice President. (1999).
[22] Nicolle Parsons-Pollard and Laura J Moriarty. 2009. Cyberstalking: Utilizing what we do know. *Victims and Offenders* 4, 4 (2009), 435–441.
[23] Brian H Spitzberg. 2002. The tactical topography of stalking victimization and management. *Trauma, Violence, & Abuse* 3, 4 (2002), 261–288.
[24] Yang Zhang, Mathias Humbert, Tahleen Rahman, Cheng-Te Li, Jun Pang, and Michael Backes. 2018. Tagvisor: A privacy advisor for sharing hashtags. In *Proceedings of the 2018 World Wide Web Conference*. 287–296.

12 APPENDIX

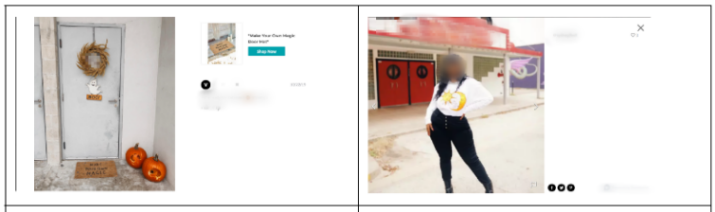
A EXTERNAL WEBSITES AND INSTA POSTS

Examples of external websites featuring users' Instagram posts with personally identifiable information are reported in two parts as Figures 4 and 5.



Post featured by Aerie using the hashtag #AerieREAL. The user is posed in front of a barber shop with a distinct wall, where the Instagram handle for the barber shop is painted on, which has been blurred. A simple Google search of the barber shop's name, or looking up the barber shop's Instagram using the tag on the wall, is a fast way to determine the location where this picture was taken, despite there not being any geo-tagged (An Instagram feature to tag photos based on location, where users can search or click on geotags and have a map with a pin in that location) information on the external website. The user does have the picture geo-tagged on her personal Instagram page, but this is not featured on Aerie's external website.	Post featured by American Eagle Outfitters using the hashtag #AEJeans. The background is a building with the building number shown. If this is a place the user frequently visits, this is sensitive personal information that is public when viewed through American Eagle's featured #AEJeans gallery. It is interesting to note that the user has their Instagram privacy settings set to private; however, since this post has been shared to an external network, anyone can have access to their post [43] through this gallery.	Post featured by Aerie using the hashtag #AerieREAL. The user is posed in front of an apartment complex, with a street sign and car in the background. Although it is not clear if this is the user's car, the street sign and apartment complex, where the original user may or may not live/visit frequently, reveals potentially personal, sensitive information.

Figure 4: Instagram Posts with PII found in External Websites



A featured post from Earthbound Trading Co. with the user's Instagram profile picture removed, although the username and caption is visible. The picture shows an apartment door, with the room number visible, which has been blurred out.	A featured post on Rue21's website gallery #YOUinrue. The user is posed in front of a movie theater, which has been blurred due to the text having the theature's name/location. As seen, the user's Instagram profile picture and caption (along with any potential hashtags or geotag) are removed.
A featured post on Pacsun's website, which has been reposted by Pacsun on Instagram and then featured on Pacsun's external website. The caption is visible and the user is tagged in the caption of Pacsun's post.	A post featured on American Eagle Outfitters, where the user is posed in a neighborhood, in front of a house and street sign. The street sign is visible and legible, and although the user has the picture geotagged on her original Instagram picture, which can be seen since her privacy is set to public, American Eagle has removed this. The original caption is still visible, but her profile picture has been removed.

Figure 5: Instagram Posts with PII found in External Websites