Editor: Gustavo Rossi • gustavo@lifia.info.unlp.edu.ar

Privacy Concerns for Photo Sharing in Online Social Networks

Kaitai Liang • *Aalto University, Finland*

Joseph K. Liu • *Monash University, Australia*

Rongxing Lu • *Nanyang Technological University, Singapore*

Duncan S. Wong • *City University of Hong Kong, Hong Kong*

As wireless networks flourish, Internet users can access social network platforms (such as Facebook and Twitter) through personal electronic devices anywhere and anytime. However, because users often deploy social network platforms in a public network setting, a common concern remains about how to guarantee privacy for photo sharing. Although most platforms aim to protect such privacy, few are able to reach the goal. This work focuses on an interesting potential privacy risk, called the deletion delay of photo sharing, by pinpointing and investigating the risk's existence in some well-known social network platforms.

As with mobile devices when they reached 3G/4G connectivity, online social networks are now in the middle of a boom. Social network platforms provide a convenient human-machine interface for Internet users, making it simple to share unlimited-format information (such as photos and videos) with friends anywhere and anytime. Additionally, users can enjoy real-time and free chats with others, post the latest status updates/check-ins, and express opinions about current social hot spots. Since social networking's introduction, we've seen several hugely successful platforms emerge (including Facebook, Twitter, and Instagram).

When surfing on such platforms, most users are unaware of the platform's privacy issues, but actually, users' social network privacy is important.[1] Some sensitive information — such as a personal preference, profile, and shared photos — could be leaked to others who aren't granted access rights, if the social media service provider doesn't take great precautions to protect access control. It's undeniable that most social network platforms aim to preserve their clients' privacy as much as they can. For example, Facebook supports personal privacy and security settings so that a user can control which kinds of information others can read or see. However, at least to some extent, most social network platforms are unable to protect users' privacy perfectly.

Thus, in this Spotlight article, we focus on an interesting privacy issue, which we call *deletion delay*, on photo sharing. We investigate some widely used online social network platforms (including Facebook, Instagram, Twitter, Tumblr, Flickr, and MySpace) and show how users indeed suffer from the deletion-delay phenomenon in not only single-platform but also cross-platform settings. In a single-platform scenario, someone can still access a posted photo's URL even after the user deletes the photo. In a cross-platform setting, a photo posted in an initial platform might

 Published by the IEEE Computer Society 1089-7801/15/$31.00 © 2015 IEEE

be shared to a destination platform. However, the photo's access/sharing link that's shown in the destination platform is still available even after the user removes the original photo. Most wouldn't see this deletion delay as a prohibitive problem if the delay was only a few minutes. But actually, what we saw in our investigation is that for some social network platforms, the deletion delay could be a few days or even a few weeks.

Photo-Sharing Deletion Delay

Before we proceed in our investigation of deletion delay, let's look at some basic operations that we might use in an online social network platform.

- *Post/share photo*. A social network platform lets users post photos via their registered accounts by uploading the photos and then clicking the "Post" button. Take Facebook as an example — before posting photos, the photo's owner can manage and access a control list, so that he/she can limit who has access to the photos. If the owner chooses "Friends" in the list, only his/her Facebook friends are granted photo access rights. Most popular social network platforms, such as Instagram, leverage a similar access control mechanism to manage the sharing of photos/posts.
- *Obtain URL of photo*. After someone posts a photo, those with permission to see the photo can copy the photo's URL by right-clicking on the photo and then selecting "Copy image URL." This approach is applicable to lots of social network platforms, including Facebook, Twitter, Tumblr, and MySpace. But for Instagram and Flickr we need to right-click on the webpage containing the photo, and select "Inspect element" to obtain the photo's URL from the HTML source code. It's not difficult to obtain the URL using this approach, because many browsers (for example, Google Chrome) let you access the webpage's source code.
- *Delete photo/post*. The user (poster) can delete his/her photos/posts at any moment by easily clicking the "Delete" button.

Most online social network users think that their photos "disappear" immediately after being deleted. However, this isn't true. According to our investigation, the aforementioned online social network platforms (except Twitter) have a delay of deletion that lets us re-access the deleted photo via either its URL or its sharing/access link.

Deletion Delay on Photo Sharing: Single Platform

After deleting a posted photo in a social network platform, we can still gain access to it by opening its URL in a browser. This might be against a person's will. For example, let's say a friend tags a user in an embarrassing photo, but even after the photo is deleted, others can still access it. Actually, Jacqui Cheng[2,3] and others[4–7] have already reported this type of privacy risk happening with Facebook. Multiple sources[8,9] have noted privacy concerns about deleting posts from Facebook, including Chris Crum,[10] who brought up a general concern about photo deletion in some social network platforms. When Cheng[2] pointed out that this risk existed on Facebook and Instagram, she also reported that a spokesperson for Facebook said it would shorten the delete-delay period to 30 days, and she noted that Instagram had a shorter delete-delay period. However, Cheng only investigated Facebook and Instagram (in a single-platform photo-sharing setting). We've looked at this issue more comprehensively, and in addition to these two platforms, we state that MySpace, Flickr, and Tumblr suffer from the same risk. But as far as we know, Twitter is immune from any deletion-delay problems.

*Table 1. Deletion-delay comparison among different online social network platforms.**

Platforms	No. of days until the deleted photo is unavailable
Facebook	7
Twitter	Immediately
Instagram	3
MySpace	More than 30
Tumblr	More than 30
Flickr	14

* The photos' URLs aren't shown here, but are available upon request.

As others have noted,[2,3,6] these platforms mainly incur deletion delay because of their content delivery networks' (CDNs') complex interactions. It seems that eliminating this "flaw" becomes the technical bottleneck for most existing online social network platforms. With this in mind, later we'll introduce some possible countermeasures for tackling the problem. But first, let's look at the methodology that led to our findings.

Methodology. We set about investigating the deletion delay for the aforementioned social network platforms, to figure out how long a photo "really disappeared" after its deletion. The following is our methodology: first, we post a photo in a platform, copy its URL, and then delete the photo. We further calculate how long the URL is unavailable after the photo's deletion. (We should note here that the purpose of presenting our investigation result is to inspire the social network service providers and their clients to be aware of the deletion-delay problem, rather than trying to deliver a precise scientific calculation.) As Table 1 shows, MySpace and Tumblr suffer from the longest deletion-delay period (note that the URL's availability lasts for at

*Table 2. Comparison of photo sharing in a cross-platform setting.**

Initial platforms	Destination platforms	Shared link	Along with resized photo	Direct copy of photo	Links disable after deletion	Copy/resized photo seen after deletion
Twitter	Facebook	√	√	×	√	√
MySpace	Facebook	√	√	×	×	√
	Twitter	√	×	×	×	⊥
Tumblr	Facebook	×	×	√	⊥	√
	Twitter	√	×	×	√	⊥
Instagram	Facebook	×	×	√	⊥	√
	Twitter	√	×	×	√	⊥
	Tumblr	×	×	√	⊥	√
Flickr	Facebook	√	√	×	√	√
	Twitter	√	×	×	√	⊥
	Tumblr	×	×	√	⊥	√

*√ = yes; × = no; ⊥ = not applicable.

least a month), while Twitter enjoys the shortest delay (in fact, the URL is unavailable right after the photo is deleted).

Deletion Delay on Photo Sharing: Cross Platforms

We experienced a similar deletion-delay problem when a photo posted in one platform is shared to others. To proceed in our investigation, we first need to register six different platform accounts, including Facebook, Twitter, MySpace, Instagram, Tumblr, and Flickr, and next link these accounts together based on their linkage policies.

Photo-sharing mechanism in a cross-platform setting. Most social network platforms enable users to share posted photos from the current platform to others. For example, an Instagram user named Alice can share the photo posted in Instagram to her Facebook timeline. Various platforms employ different mechanisms on cross-platform photo sharing. For instance, if a photo (which is originally posted in MySpace, Twitter, or Flickr) is shared to Facebook, a sharing/access link (of the photo) along with a small-sized original photo will be posted on Facebook's timeline; while when a photo (initially posted on Instagram or Tumblr) is shared to Facebook, a copy of the original photo (a small-sized copy of the original) will be directly shown in the timeline. The photo-sharing mechanism (in the cross-platforms setting) of Twitter is somehow similar to that of Facebook. In Tumblr, a copy of the original photo is directly posted after its sharing, as well. When clicking the copy, we're redirected to the platform (which stores the original photo) to access the photo. This, nevertheless, is undesirable, because even when the original photo is deleted, the photo's copy is still there (in Tumblr's timeline).

Methodology. In this experiment, we post a photo in a platform (that is, the initial platform), and further share it to other platforms (the destination platforms), and finally delete the original photo from the initial platform. From this, we verify whether any information of the original photo is leaked in the destination platforms after it's deleted.

Sharing photos from MySpace to Facebook. We post a photo in MySpace, and next share it to Facebook. In Figure 1ai, we see that a piece of news appears on the Facebook timeline after we share the photo. We then delete the original photo posted in MySpace. However, the link shown in Facebook still lets us access the photo (see Figure 1aii), and meanwhile, the small-sized photo tagged with the link is visible.

Sharing photos from Twitter or Flickr to Facebook. After we remove the original photo (posted in Twitter), the sharing link shown in Facebook is unavailable immediately, but we can still see the small-sized photo (see Figure 1b). The same phenomenon exists in photo sharing from Flickr to Facebook.

Sharing photos from Instagram or Tumblr to Facebook. Instagram/Tumblr directly shares a copy of the original photo to Facebook (see Figure 1c). Even when we delete the original photo from Instagram/Tumblr, its copy still shows on the Facebook timeline.

Sharing photos from MySpace, Flickr, or Tumblr to Twitter. When we share a photo posted in MySpace, Flickr, or Tumblr to Twitter, a sharing/access link of the photo shows on the Twitter timeline. If we remove the original photo posted in Flickr or Tumblr,

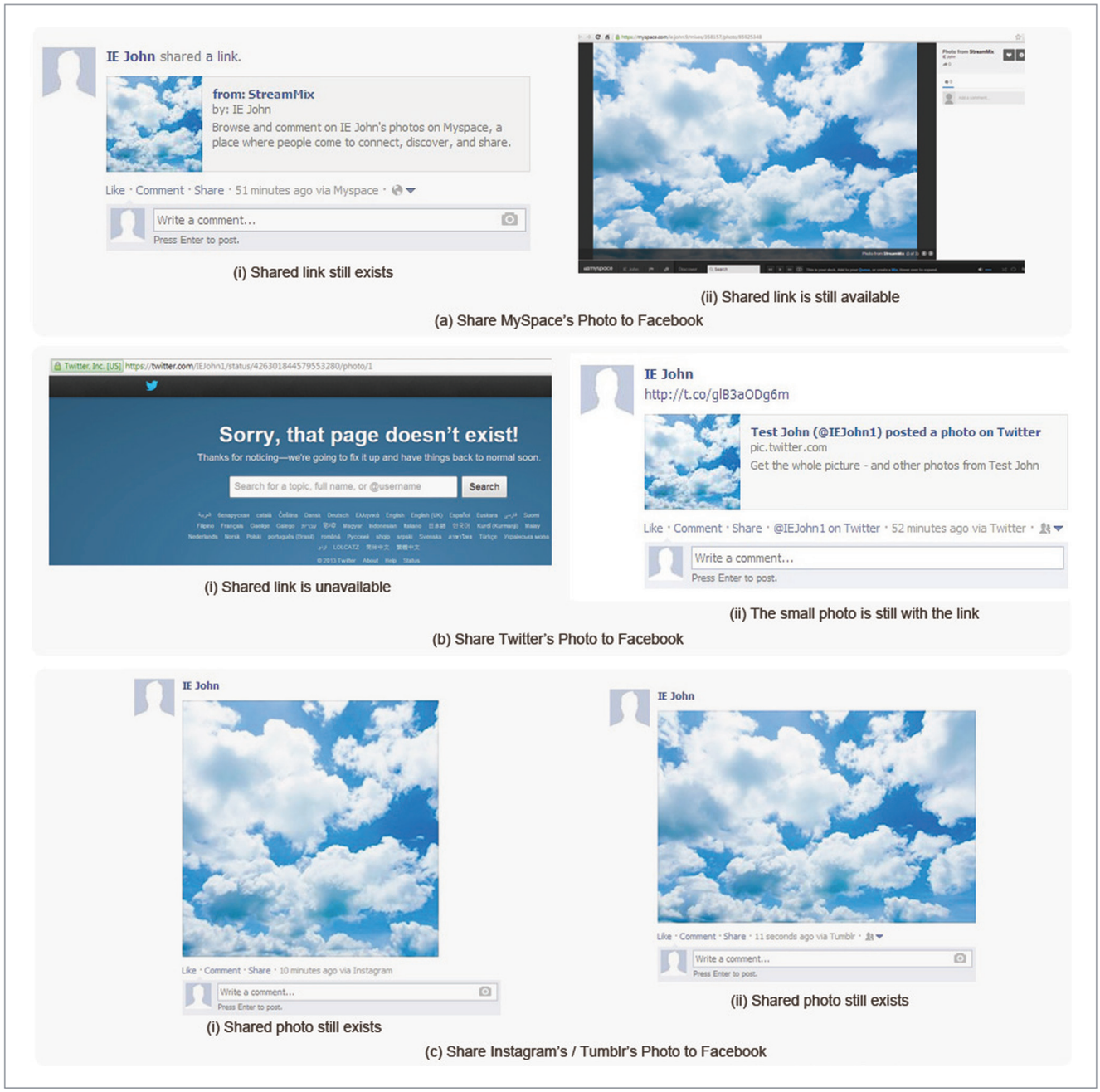

Figure 1. Photo sharing from (a) MySpace, (b) Twitter, and (c) Instagram/Tumblr to Facebook. In many cases, after deleting the photo from the initial platform, vestiges of the photo and/or its data still exist in the destination platform.

the shared link shown on Twitter's timeline is immediately unavailable. Nonetheless, the case of sharing photos from MySpace to Twitter is an exception, whereby the link is still available. Note that a resized photo won't show along with the access link on the Twitter timeline unless we share a photostream from Flickr to Twitter.

Sharing photos from Instagram to Twitter. Sharing a photo posted on Instagram to Twitter is privacy-preserving. After we share the photo, a sharing/access link shows only on the Twitter timeline. If we delete the original photo from Instagram, the link is unavailable immediately.

Sharing photos from Instagram/Flickr to Tumblr. If we share a photo posted on Instagram or Flickr to Tumblr, a copy of the photo shows on Tumblr's timeline, where the copy has a sharing/access link as well. If we delete the original photo, we can still see the copy of the photo but its redirection functionality is disabled.

Comparing cross-platform photo sharing. We summarize the investigation's results in Table 2. As you can see, Twitter yielded adequate privacy-preserving photo sharing in a cross-platform setting. It doesn't show a resized photo or a copy of a photo in its timeline, and moreover, its sharing/access link is disabled immediately after we remove the original photo from the initial platform. But for Facebook and Tumblr, they reserve either a resized photo or a copy of a photo in their timelines, regardless of whether you deleted the original photo. In addition, Table 2 indicates the photo-sharing policies of the social network platforms: we can share photos from other platforms to Facebook and Twitter, while MySpace, Instagram, and Flickr have stricter photo-sharing regulations.

Some Possible Countermeasures

As far as we know, there's no direct and efficient approach to tackle the deletion-delay problem. Therefore, we only introduce some possible countermeasures for the problem, and hope these solutions might inspire future research.

One possible solution[5] is for social network service providers to shorten the photo-deletion time from the CDN. However, this approach's efficiency relies on the data storage structure and data locating/searching mechanism that a social network platform employs. Nowadays, a platform's storage back end is able to store at least hundreds of thousands of users' data, so that it might not be very efficient to locate and then delete a photo from a great amount of data within a short time interval. Therefore, we might choose to consider other methods.

Another possible solution is to combine an encryption mechanism with the help of a trusted (third) party. A social network user might choose to encrypt photos before posting in a platform by employing some encryption mechanisms, such as attribute-based encryption.[11–13] Here, the photos are stored in an encrypted format, and the URLs now are only associated with the encrypted photos. The user may then upload the photos' decryption keys to a trusted party (either the platform server or a trusted third party), so that the party can locate the encrypted photos, and next display the photos by using the keys for those users granted access rights.

Finally, social network service providers could take some privacy-preserving solutions for users' information/profiles into account. For example, we might extend the existing access/privacy control or privacy-enhanced technology, as detailed in other works,[14–16] to solve the deletion delay of photo sharing.

In investigating the issue of social networks' deletion delay in single- and cross-platform photo sharing, our goal is to bring awareness of the privacy risks involved. Hopefully the countermeasures that we proposed act as helpful solutions. We also brought this issue to light in the hopes that social network service providers (and their users) will be more conscious of this issue, thereby fostering more research and developments that protect social network users' privacy. ◻

Acknowledgments

This work took place during Kaitai Liang's internship with the Institute for Infocomm Research in Singapore. This work was supported by a grant from the Research Grants Council (RGC) of the Hong Kong Special Administrative Region (HKSAR), China (project CityU 121512). Joseph K. Liu is the corresponding author of this work.

References

1. National Children's and Youth Law Centre, "Privacy (Online)," *Lawstuff*, 12 Nov. 2013; www.lawstuff.org.au/wa_law/topics/privacy.
2. J. Cheng, "Three Years Later, Deleting Your Photos on Facebook Now Actually Works," *Ars Technica*, 16 Aug. 2012; http://arstechnica.com/business/2012/08/facebook-finally-changes-photo-deletion-policy-after-3-years-of-reporting.
3. J. Cheng, "Over 3 Years Later, 'Deleted' Facebook Photos Are Still Online," *Ars Technica*, 6 Feb. 2012; http://arstechnica.com/business/2012/02/nearly-3-years-later-deleted-facebook-photos-are-still-online.
4. D. Cohen, "Facebook Finally Fixes Photo-Deletion Issue," *Social Times*, 16 Aug. 2012; www.adweek.com/socialtimes/photo-deletion-issue-fixed/400681.
5. H. Collis, "Facebook Finally Deletes Millions of Embarrassing Pictures from Its Servers after Years of Keeping Them Against Users' Wishes," *The Daily Mail*, 26 Aug. 2012; www.dailymail.co.uk/news/article-2193805/Facebook-updates-deleted-photos-gone-forever.html.
6. Z. Whittaker, "Facebook Does Not Erase User-Deleted Content," 2010, ZDNet, 28 Apr. 2010; www.zdnet.com/blog/igeneration/facebook-does-not-erase-user-deleted-content/4808, 2010.
7. S. Jacobsson Purewal, "Deleted Facebook Photos Still Accessible Online, Years Later," *PCWorld*, 7 Feb. 2012; www.pcworld.com/article/249433.
8. S. Colaner, "Think Your Deleted Facebook Posts Are Really Deleted? Guess Again," Hot Hardware, 3 July 2013; http://hothardware.com/News/Think-Your-Deleted-Facebook-Posts-Are-Really-Deleted-Guess-Again/#!beG7UK.
9. F. Bea, "Turns out Delete Doesn't Quite Mean the Same Thing to Facebook as It Does to You," *Digital Trends*, 2 July 2013; www.digitaltrends.com/social-media/deleting-facebook-posts-fail/#!beG7qM.
10. C. Crum, "Are Your Social Network Photos Really Being Deleted? Are You Sure?" Web Pro News, 28 May 2009; www.webpronews.com/are-you-social-network-photos-really-being-deleted-2009-05.
11. V. Goyal et al., "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," *Proc. ACM Conf.*

Computer and Comm. Security, 2006, pp. 89–98.
12. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE Symp. Security and Privacy*, 2007, pp. 321–334.
13. R. Baden et al., "Persona: An Online Social Network with User-Defined Privacy," *Proc. ACM SIGCOMM*, 2009, pp. 135–146.
14. T. Reynaert et al., "Pesap: A Privacy Enhanced Social Application Platform," *Proc. IEEE Conf. Social Computing and Privacy, Security, Risk, and Trust*, 2012, pp. 827–833.
15. M. Shehab et al., "Access Control for Online Social Networks Third Party Applications," *Computers & Security*, vol. 31, no. 8, 2012, pp. 897–911.
16. K. Singh, S. Bhola, and W. Lee, "xbook: Redesigning Privacy Control in Social Networking Platforms," *Proc. USENIX Security Symp.*, 2009, pp. 249–266.

Kaitai Liang is a postdoctoral researcher in the Department of Computer Science at Aalto University, Finland. His primary research interest is applied cryptography; in particular, cryptographic protocols, encryption/signature schemes, and RFID. He's also interested in cybersecurity, such as network security, privacy-enhanced technology, Big Data security, and security in cloud computing. Liang has a PhD in computer science from the City University of Hong Kong. Contact him at kaitai.liang@aalto.fi.

Joseph K. Liu is a senior lecturer in the Faculty of Information Technology at Monash University, Australia. His current technical focuses are cybersecurity in physical systems, including cloud computing environments, Internet of Things, transportation systems, and smart city infrastructures; lightweight security; and privacy-enhanced technology. Liu has a PhD in information engineering from the Chinese University of Hong Kong. Contact him at ksliu9@gmail.com.

Rongxing Lu is an assistant professor in the School of Electrical and Electronic Engineering at Nanyang Technological University, Singapore. His research interests include computer network security; mobile and wireless communication security; and Big Data security and privacy. Lu has a PhD in computer science from Shanghai Jiao Tong University, China, and another PhD (where he was awarded the Canada Governor General Gold Medal) in electrical and computer engineering from the University of Waterloo, Canada. He's a member of IEEE. Contact him at rxlu@ntu.edu.sg.

Duncan S. Wong is an associate professor in the Department of Computer Science at the City University of Hong Kong. His primary research interest is cryptography; in particular, cryptographic protocols, encryption/signature schemes, and anonymous systems. He's also interested in other topics surrounding information security, such as network security, wireless security, database security, and security in cloud computing. Wong has a PhD in computer science from Northeastern University. Contact him at duncan@cityu.edu.hk.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.