On the Awareness, Control and Privacy of Shared Photo Metadata

Benjamin Henne(✉), Maximilian Koch, and Matthew Smith

Distributed Computing and Security Group,
Leibniz Universität Hannover, Hannover, Germany
{henne,smith}@dcsec.uni-hannover.de

Abstract. With the continuously rising number of shared photos, metadata is also increasingly shared, possibly with a huge and potentially unseen impact on the privacy of people. Users often relinquish the control over their photos and the embedded metadata when uploading them. Our results confirm that the concept of metadata is still not commonly known and even people who know about the concept are not aware of the full extent of what is shared. In this work we present two solutions, one to raise awareness about metadata in online photos and one to offer a user-friendly way to gain control over what and how metadata is shared. We assess user interest in options ranging from deletion and modification to encryption and third party storage. We present results from a lab study (n = 43) in which we evaluated user acceptance, feelings and usability of the proposed solutions. Many of our participants expressed the desire for user-friendly mechanisms to control the privacy of metadata. 33 % of them did not simply want to delete their metadata, but preferred to use encryption to share, but nonetheless protect, their data.

1 Introduction

Due to the proliferation of broadband Internet and the wide-spread adoption of mobile devices, the sharing of photos is nowadays booming more than ever: In 2013 Facebook reported more than 350 million photo uploads per day, while Instagram reports an average of 55 million photos per day today.

By uploading their photos, people partially relinquish the control over their personal media. A central problem is that many people may not realize the loss of control induced by sharing their files. Critically, only few people are aware that most of their photos contain more information than the visual content itself, i.e. the image metadata. Besides the visual content, the metadata can amplify or even create threats to the users' privacy. While in the early days of digital imaging, metadata had to be manually—and thus consciously—added to the pictures, current cameras are capable of embedding metadata like GPS coordinates, a camera owner's name or the position of faces into photos automatically. Mobile apps even feature facial recognition that aims to support tagging and might automatically tag individuals with names in the near future. When these photos are uploaded, the metadata is often shared as well.

N. Christin and R. Safavi-Naini (Eds.): FC 2014, LNCS 8437, pp. 77–88, 2014.
DOI: 10.1007/978-3-662-45472-5_6

There has been a lot of work concerning the privacy and security of photos in particular in the context of social media. Prior work mainly focused on privacy, i.e. access control of images [8]. Additionally, specific metadata, like the location of a photo [5] or people linked to photos [1], have been topics of research, but mostly in the scope of services that grant access only to registered users or "friends" [10]. Metadata in general, specifically metadata stored within image files, has received far less attention. One fairly common approach is to simply remove all metadata. However, since metadata can add value for users, this radical solution is not suitable for all situations.

Our work aims at finding a way to maintain the metadata and the users' privacy at the same time. One important aspect of this issue is that people must first become aware of the existence of this "invisible" metadata and thus hopefully gain the desire to use it, protect it or delete it. In this paper we present a Chrome browser extension for raising awareness of metadata when uploading content and while browsing. It also allows users to control what metadata is disclosed. We propose an integrated encryption-based approach to securely share metadata online. Finally, we present results of a lab study (n = 43) on awareness, control and the usability of our solution including a mock-up of metadata encryption.

2 Metadata Problems in a Nutshell

Technical Complexity. Photo metadata stored in files can contain an immense amount of context information. Common metadata standards—such as Exif, IPTC, and XMP—incorporate hundreds of different tags. While many tags address technical details, which are not so relevant for privacy, the scope of privacy-related information should not be underestimated. For instance, the date and time a photo was taken, the name of an image creator or camera owner, a camera's unique serial id, un-cropped preview images, descriptions, and textual or coordinate-based location information can be included. Even person tags with bounding boxes, as known from social networks services can be embedded today. Besides the diversity of the information, its handling poses challenges as well:

- The sheer number of existing tags from different standards and the lack of any overall structure make the identification of specific—in our case privacy-related—information difficult.
- The sets of tags supported by applications differ significantly, so people may unintentionally use one that hides privacy-related information from them.
- Client applications and online services deal with metadata in a bewildering number of ways [7]: Some strip metadata out entirely, others partially or not at all. It is next to impossible for users to find out how each service handles their data without manually trying it out on their own.
- Metadata is stored in different ways; i.e. in local databases, in image files, in sidecar files, or in online services' databases and people may not realize the differences between respective privacy implications.

Rising Adoption. Due to the evolution of software and devices, the amount of embedded metadata is rising rapidly. A dataset we crawled at Flickr provides evidence for this trend. We crawled 200 k photos, one from each 100 k random users/cameras and from another 100 k users taken by one of 76 popular smartphones. While the portion of geo-tagged images of the 100 k random users rose from 1.5 % in 2006 to 5.1 % in 2012, its portion rose from 0 in 2006 to 39.3 % in 2012 and 42.9 % in 2013 in the subset of 100 k mobile photos. Additionally, we found embedded person tags are now receiving early adoption: 5 % of the mobile photos from 2013 contained unnamed person tags (bounding boxes only) and 0.1 ‰ named person tags. Most photos with unnamed person tags were taken by iOS devices, which tag faces without names automatically since iOS 5.

User Awareness and Actions. In a prior study (n = 414) [6] we analyzed user behavior and perceptions of photo sharing including a section on metadata: In that study 61.1 % of the participants indicated to know the concept of metadata. Those indicating to know metadata made following statements: 29 % generally do not know which additional information is contained in the photos they share; 58 % do not know what their social Web services do with photo metadata; and about 27 % do not think about metadata at all when sharing images on the Web. About 25 % of them do not manually add metadata to photos. About 6 % remove all metadata before sharing, while additional 35 % remove it partially.

To Remove or Not to Remove Metadata. The removal of metadata—either by a service or the user—prevents privacy leaks but also removes information that can be beneficial as well. Metadata is a valuable tool to maintain control of an increasing amount of photos. While most service providers are able to handle big data very well, users are often overburdened keeping track of all their media. In the latter case, metadata can help users to improve the handling of their personal photos. Hence, it can be beneficial to retain metadata in shared files. It can also be desirable to allow others access to the metadata, however the user should be able to consciously choose how and with whom this data is shared. Users should not have to rely on service providers to remove or protect metadata upon upload. Especially because it is impossible for them to check on what a service does with the data.

Summary. Image metadata introduces many benefits, but it also creates diverse challenges for usability and privacy research. We identified two essential objectives that we address in the remainder of this work:

1. Users have to become aware of the existence of metadata, for instance by appropriate visualization [9]. Thus we have to find usable technical solutions that help raising the level of transparency and awareness of metadata in the users' files. This is true both for files already on the Web as well as files currently being uploaded to the Web.
2. Users should have options beyond an all or nothing approach of removing metadata or leaving it unchanged, so they can share metadata with whom they choose without endangering their privacy.

3 Metadata Privacy Browser Extension

To address and study these objectives, we created a Chrome browser extension. The base extension aims to raise awareness about privacy-relevant metadata in shared photos, both for photos that users intend to upload, and for photos that are already on the Web. The extension visualizes metadata with a privacy focus and allows the modification of metadata during upload.

Our extension handles the metadata standards Exif, IPTC, and XMP, based on the Exiv2 C++ library that we integrated using Google Native Client. We also extended the library to support latest in-file person tags as used by Google Picasa, Windows Live Photo Gallery or the current iOS camera app.

While there are already browser extensions for the visualization of online metadata in the Chrome Web Store, those are targeted mainly at photo enthusiasts who actively want to look at metadata. None of them has the goal of informing users of potential privacy issues. Some even send images to a third party web services to extract metadata, creating privacy issues of their own.

In contrast our extension indicates privacy-related metadata passively, thus giving users a chance to see potential issues without having to consciously search for themselves. Our metadata quick indicator icons overlay the actual image as shown in Fig. 1 and thus are right where the focus of the users is when they are paying attention to the image. Maurer et al. have shown that placing security indicators in-context significantly improves their effectiveness [11]. A user can then click on the icons to open an information sidebar to get more information.

3.1 Visualization of Metadata

To visualize and raise awareness about privacy-relevant metadata, our extension groups metadata in the sidebar corresponding to five categories: *people*, *location*, *date & time*, *content description*, and other. For instance, the *people* category includes person tags, names of photographers/artists or unique camera serial ids; *content description* includes the image headline or keyword tags. Each group has its own indicator icon. Wherever possible our extension visualizes the metadata: Coordinate-based locations are shown on a map and bounding boxes of person tags are drawn in a small preview image. For the power-users there is also a button to see full metadata in all its technical glory. One particularly interesting and potentially very harmful piece of metadata is also visualized: The preview image, which is embedded by many cameras and software by default. An example scenario in which this could lead to an unwanted privacy situation is if a somewhat revealing photo is cropped to only show the torso or lower body, but the preview still contains the head of person - thus identifying the person.

Since the perception of privacy certainly differs between people, generations and countries, we opted to structure presented metadata based on the kind of information instead of attempting to display the most privacy critical information at the top. However, the extension allows assigning a privacy rating to metadata, which then leads to that item being highlighted with a color of choice, such as suggested by Shin et al. [13]. The assignment can be modified by the

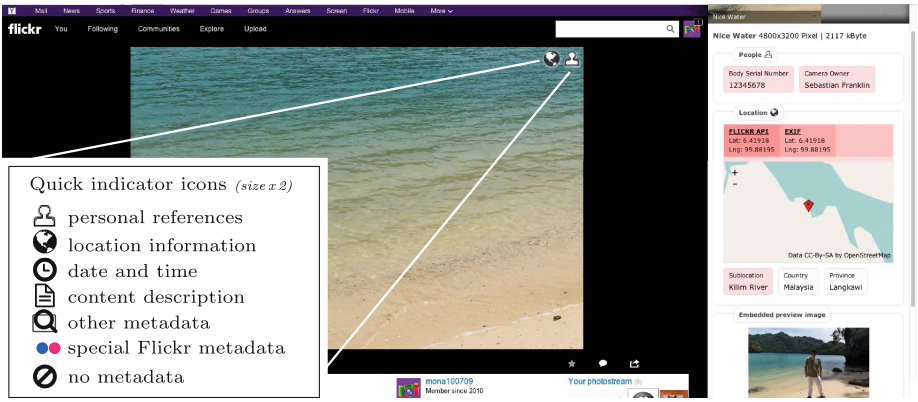

Fig. 1. Photo page at Flickr.com with metadata indicators and information sidebar

users according to their own privacy perception. For the lab study we labeled a selection of items as highly privacy-sensitive and colored them red to test the concept.

3.2 Control of Metadata

We believe unawareness is a major factor for the rare use of applications that enable users to edit or remove metadata before upload. If people do not know what is invisibly stored, they will not take any actions to deal with the issue. However, it is very likely that usability also plays a big role. Most existing tools require at least a moderate level of technical expertise. Additionally, users might not be willing to invest the extra effort of using such tools when their primary goal is to share an image. Our hypothesis is that adding the visual information and easy controls into the upload workflow will raise awareness of potential privacy issues and also give the user easy to use tools to deal with the issues. Thus, we implemented such features with our browser extension.

The prototypical implementation works with all basic HTML upload forms based on re-submission with modified files. When a user uploads a photo via the form, the extension engages in the form submission. An overlay as shown in Fig. 2 appears, and the metadata of all images selected in the file input can be reviewed. The user additionally can modify or remove it from the files.

4 Protecting Metadata

Now that we are able to make people aware of metadata they are about to upload, we need to give them tools to protect that data. As shown above the upload sidebar can be used to easily delete metadata. However, metadata can be useful and it would be desirable to be able to use it without endangering one's privacy by protecting it from unauthorized and unwanted parties.

In-File Encryption of Metadata. One solution for securing metadata would be the encryption of the data in the files. However, this creates several challenges for current metadata standards: Since XMP bases on RDF/XML, we could in principle extend it with secure encryption and even digital signatures. In contrast, the most common Exif and IPTC data is in binary format with restrictions to data length and types. In this case it is not possible to store data in encrypted form without violating the standards or storing additional data somewhere else in the files. When storing additional encryption data in files, it would be hard to keep imaging software from removing it.

Metadata Stores. For online photo sharing, we propose the use of external metadata storage services (metadata stores) for two reasons: First, storing metadata in such a service allows users to maintain and share metadata even for images stored at services like Facebook, which strip off the valuable data in general. Second and related to privacy, the separate storage of metadata allows the implementation of security mechanisms specifically for metadata, while also enabling users to secure images and metadata differently. Data splitting allows much more flexibility for access control as any sharing services allows today [7].

To investigate the idea of metadata stores, we implemented an exemplary test scenario based on Flickr. However, a similar app could be implemented for other services that provide a public API. The Flickr app enables users to upload photos to their photostream. When a user uploads an image with the web app, the user can modify metadata as described before. Finally, the user can choose to upload metadata in the image to Flickr or only separately to the metadata store. When browsing the image, the extension loads metadata from the metadata store and shows them in merged form.

Metadata Encryption. So as not to create a privacy problem by storing metadata in plain text the data needs to be encrypted so that the store and other unauthorized parties cannot access it. Storing metadata at a service makes encryption easier: It is possible to encrypt the metadata without the restrictions discussed before. As a first step, we propose encrypting all metadata en bloc, since encrypting separate parts creates additional usability challenges.

The big crux with most encryption solutions is that key management creates so many usability problems that users do not bother to use encryption or can't use it correctly [12]. For our use case the *Confidentiality as a Service* (CaaS) paradigm proposed by Fahl et al. [3] would be applicable to encrypt stored metadata. Its usability has already been evaluated in the context of Facebook messaging [4]. CaaS removes the need for user-based key management by splitting the trust between a service provider and the CaaS provider. Applying Caas-encryption, a user additionally chooses the sharing audience and enters his CaaS password when uploading. If the audience is public the metadata is uploaded unencryptedly. Otherwise the user selects contacts from his friends list and thus defines the ACL for CaaS-encryption. When selecting a group like *friends*, every user in the group is added. To prevent pre-binding attacks only users can be added who are already registered with CaaS. Once the metadata has been encrypted by the CaaS provider, it is uploaded to the store. When someone is browsing a photo

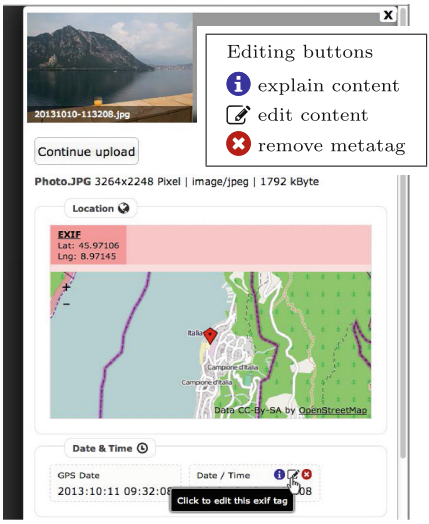

Fig. 2. Upload sidebar allows modification before final submission

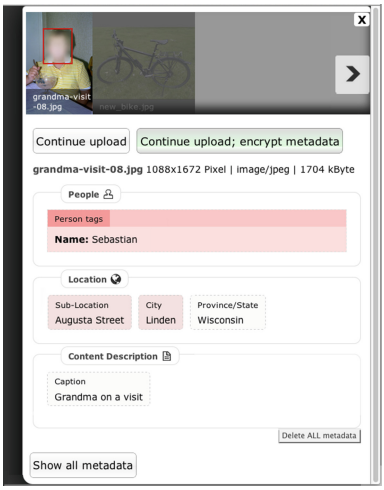

Fig. 3. Upload sidebar with option to store metadata encryptedly—multiple file upload with two photos

for which metadata was escrowed in a store, the extension loads the metadata. If metadata is encrypted and the user is on the recipients lists, the extension asks for the user's password and decrypts the data.

5 User Study

To assess user benefits and the usability of our browser extension, we conducted a lab study. We invited students from our university mailing list for study participation. 62 people filled out the online survey we used to outline our study, of which 43 attended and completed the lab study without any issues. The participants received a compensation of € 5. 62.8 % of the participants were female and 37.2 % were male. Their average age was 24 ± 4. The participants were guided by a rough task description and answered 22 questions in a paper survey while completing their tasks. Since we were mainly looking for feedback on the usability of our solution and the amount of interest the new features could illicit, we opted to openly state what we were attempting to study. Thus, we briefly explained that we want to examine two new privacy features of the web browser Chrome: the possibility to modify or delete metadata while uploading photos and a metadata viewer with metadata indicator icons. We did not mention that we are the authors of the extension, but rather portrayed it as new browser features.

Before our participants started their tasks, we asked them how much they think about if, where, and how they disclose personal information on the Web.

On the 5-point scale from (1) *not at all* to (5) *very much*, they answered with a mean and mode value of 4 (sd = 0.9) with 9 % of answers being in the lower two items. Additionally, we asked them to rate their feeling of control of what they disclose about themselves when sharing photos on the Web. On the 5-point scale from (1) *not at all* to (5) *absolutely* they reported their feeling about control with a mean value of 2.7 (sd = 1) with 20 % in the upper two items. The answers showed a clear feeling of lack of control that we try to address with our work.

5.1 Awareness and Control at Photo Upload

In the first task the participants were instructed to upload five photos at a basic photo-sharing service: One image without metadata and four containing different metadata including location data, (un)named person tags, a camera owner's name, a camera serial id and technical details. The visual content and location had slight relation to our university and students' life.

After the participants had encountered the upload dialog and the metadata for the first time, we asked them if they knew that the information just visualized by the browser was stored in (their) photos. 19 % of them answered *no*; 23 % answered *yes*. 58 % of them stated that they knew that some metadata is embedded, but did not know which kind of data. Additionally, 20 % of those answering with yes wondered about some kind of data being embedded later on in the study. This emphasizes that even if people know about metadata in general, most people probably do not know what is really embedded and shared.

After all uploads we asked our participants how much the new feature improved their awareness about what is shared with their photos. On a 5-point scale from (1) *not at all* to (5) *very much* they answered with a mean value of 4.5, with 69 % answering *very much*. This is an encouraging result. When we asked the same question about control of what is shared, participants answered with a mean value of 4.3 with 55 % of participants having chosen the top answer. Only a single participant stated in a comment that he still does not feel that he has an overview of what exactly he shares on the Web. However, a large majority of our participants stated that the new feature increased awareness and control.

During this task overall 11 participants selectively deleted metadata of a mean of 2.4 photos; 15 participants used the delete all button for other photos (mean 2.5 photos), while 9 of them first deleted selectively, but deleted all embedded metadata in the end. When we asked the participants in the debriefing if and why they removed metadata in this task (42 % of them affirmed deletion), some explained that they had not removed metadata because it was only a study or not their own photos. Interestingly, a participant reported to have deleted metadata for the same reason. She stated that she did not want to disclose data of other people, even though she did not know them.

We also investigated first contact perception and usability. After the participants had used the upload feature for the first time, we asked them if they intuitively understood the new functionality. On a 5-point scale from (1) *not at all* to (5) *absolutely*, they answered with a mean score of 3.8 (sd = 1.1).

Using the *system usability scale* (SUS) score [2], participants rated the upload feature with 73.5 of 100 points, which indicates a good usability.

We questioned our participants how they perceived the integration of the metadata modification dialog in the upload process. On the 5-point scale from (1) *unfunctional/obstructive* to (5) *very functional/very good*, they answered with a mean value of 4.3 with 58 % in the top item and only 5 % in the lower two items. When asking how often they would like to use the new features at home using the 5-point scale from (1) *never* to (5) *always* with (3) as *from time to time*, they answered with a mean value of 4.2 ($\text{sd} = 1, \text{mode} = 5$) in case of the visualization of uploaded metadata. Concerning the possibility of removing metadata, they answered with a mean value of 4 ($\text{sd} = 1, \text{mode} = 5$). In contrast, the mean answer of 3.7 ($\text{sd} = 1.1, \text{mode} = 4$) was given in case of the modification of metadata. Participants significantly preferred viewing (Wilcoxon test: $Z = -3, p < .05$) and visibly preferred deletion ($Z = -1.7, p = .08$) to changing values. When asked for missing features, some participants requested easier removal of groups of metadata, or a default option to delete all metadata on upload. Others asked for the ability to add metadata (person tags, location, and copyright information). Finally, one participant asked for the option to encrypt metadata in files.

5.2 Awareness of Metadata on the Web

In the second task participants started to browse on a prepared web page showing some public images with links to source pages to allow the images to be viewed in their original context. The images contained all kinds of metadata discussed before including an example of a face cropped in the image, but with the complete preview embedded. In addition, they could browse the Flickr page of recent iPhone 4S uploads and another public photo-sharing community that preserves metadata. Participants were free to decide where they browse and could choose when to proceed with the questionnaire. On average they visited 3 external pages and viewed the metadata details of 4 photos over a timespan of roughly 5 min before going on to the questionnaire.

When we asked them how helpful they perceived the indicator icons that show what information is stored in the images, participants answered with a mean value of 4.1 ($\text{sd} = 1.1, \text{mode} = 5$) on the 5-point scale from (1) *not at all helpful* to (5) *very helpful* with 9 % of answers in the bottom two items. We also asked how much the icons annoy them during browsing using the scale from (1) *not at all annoying* to (5) *very annoying*. They responded to this question with a mean value of 1.5 ($\text{sd} = 0.7$) with only one answer in the upper two items. Most of the participants perceived the indicators as helpful to very helpful and hardly anyone felt annoyed. However, both these values must be taken in the context of the task focus participants had. Particularly the annoyance question will have to be re-evaluated in a field study.

Since the sidebar includes different aspects to improve the understanding of information, we asked our participants how they perceived those aspects using the 5-point scale from (1) *useless* to (5) *very helpful* with (3) as *neutral*. In case of

grouping data, showing very private data with red background, visualizing locations on a map and the detailed view of all metadata the participants answered with a mean score of 4.1 ($\text{sd} = 1, \text{mode} = 5$). In case of person tag previews showing names when hovering over bounding boxes, the average score was 3.9 ($\text{sd} = 1, \text{mode} = 4$), and in case of tag descriptions the average answer was 3.8 ($\text{sd} = 1.2, \text{mode} = 5$). So, none of the features were regarded as useless.

To assess the awareness gain based on the metadata visualization, we asked our participants how effectively the new feature improves their awareness of what is embedded in photos that they and others shared. On the 5-point scale from (1) *not at all* to (5) *very effectively* participants answered with the mean value of 4.6 ($\text{sd} = 0.8, \text{mode} = 5$), indicating an appreciable improvement.

When we asked them how often they would like to use the new visualization features at home using the 5-point scale from (1) *never* to (5) *always* with (3) as *from time to time*, over 60 % answered in the top two items and no one answered *never*. Our participants slightly preferred (Wilcoxon test: $Z = 1.7, p = .09$) using metadata indicators on the average with a mean value of 4.2 ($\text{sd} = 0.9, \text{mode} = 5$) to showing details in the sidebar with a mean value of 4 ($\text{sd} = 1, \text{mode} = \{4, 5\}$).

Based on the SUS score, participants rated the visualizations feature's usability with 76.9 of 100 points, which indicates a good usability.

5.3 Metadata Privacy and Usefulness

In the last task of the study the participants were instructed to upload one of the initial photos again. To test whether users would be able to use the proposed encryption mechanisms and to a small extent also test whether they would be interested in it, the corresponding upload page was extended to support storing metadata in a pre-configured metadata store. On this upload page our mock-up of encryption was automatically enabled. When uploading a photo, participants now were presented two buttons in the sidebar: *Continue upload* and *Continue upload; encrypt metadata* as shown in Fig. 3. When selecting encryption, metadata was removed from the image file and stored in the service. On submission the user was asked for the sharing audience corresponding to Flickr groups *family*, *friends*, *only me*, and some people from the user's role-playing contact list. Subsequently users had to enter their encryption password and the image was uploaded. Viewing the uploaded image, the extension recognized the image and asked for password once to decrypt the metadata from the store.

While the participants were primed to upload an image, we did not elaborate on the encryption. We only provided them a password in the task description with which they could encrypt their metadata if they want. We did not give them any task which explicitly required them to do that though. When executing the task, 56 % of the participants encrypted metadata of an uploaded image.

In the survey we asked them whether they consider metadata as (1) a *threat to privacy* or as (5) *useful and meaningful* information on a 5-point scale. In the case of sharing photos on the Web, they stated that they consider it as a threat with a mean rating of 1.7 ($\text{sd} = 1, \text{mode} = 1$). When sharing photos with single persons for instance via email, they rated metadata to be more meaningful with

a mean value of 3.9 (sd = 1, mode = 4). For private use, they rated it with a mean value of 4.6 (sd = 0.9) to be meaningful and useful data.

Finally, we asked our participants to rank different ways to secure metadata sharing and hence preserve their privacy. In their answers, 40 % of the participants indicated to mostly prefer the removal of all metadata, while 33 % stated to prefer encryption to restrict access to it. We found this to be surprising. Considering how unpopular email encryption is and the fact that we only mentioned the possibility to use encryption but did not task them to use it, we did not expect so many participants to list this as their preferred option. 26 % prefer to share metadata publicly after selectively removing some information and only one participant stated he wanted to share the metadata completely as is the current standard. On the second rank, 53 % of the participants chose the selective removal; 23 % encryption; and 19 % the complete removal. Sharing metadata as it is was the last choice for 86 % of participants. Participants' answers show an appreciable willingness to encrypt metadata, which allows securing it while retaining the data for a restricted audience.

5.4 Debriefing and Summary

In the debriefing of the study, we asked the participants what they had learned by using the extended browser and if they thought this would have any effect on their thinking or future behavior. 88 % of our participants answered affirmatively. About one quarter of them stated that they will (try to) think about metadata or even modify it when sharing photos in the future, while others stated that they are now more aware about the topic after having seen metadata in the wild. This shows that once informed about the existence of metadata there is a desire for change. Thus, it should be our goal to raise awareness in the wild and give users tools with which to control and protect their metadata. More than 10 % commented that they underestimated the amount and kind of stored information. Even people who thought that they know what is stored were surprised about some data like embedded previews or in-file person tags.

Before we could debrief them on the fact that the extension was developed by us about one quarter of the participants asked when or where they could get the browser with the new features. Even after they were informed that the extension is still a prototype some were interested in getting an early version.

6 Conclusion and Future Work

In this work we presented an extension for the Google Chrome web browser that aims to assist users in seeing and controlling photo metadata. Our lab study showed that users reacted very positively to the capability of seeing and being able to control the metadata they upload. The usability evaluation received very good results and set the stage for the next phase of our research. In this study we did not obfuscate the fact that we were studying the visualization and control of metadata. Thus, we could only study the usability of our approach and not

the awareness and desire raising effect this technology can have in the wild. The next step in our work is to conduct a field study to see how effective the upload window, the metadata indicators and sidebar are without any priming or task focus. Based on a mock-up implementation of the encryption service we proposed, our study's results showed that one third of our participants opted for the encryption approach. This surprising result also bears further research.

References

1. Besmer, A., Richter Lipford, H.: Moving beyond untagging: photo privacy in a tagged world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pp. 1563–1572. ACM (2010)
2. Brooke, J.: SUS: a quick and dirty usability scale. In: Jordan, P.W., Weerdmeester, B., Thomas, A., Mclelland, I.L. (eds.) Usability Evaluation in Industry. Taylor and Francis, London (1996)
3. Fahl, S., Harbach, M., Muders, T., Smith, M.: Confidentiality as a service - usable security for the cloud. In: 2012 IEEE 11th Int'l Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 153–162 (2012)
4. Fahl, S., Harbach, M., Muders, T., Smith, M., Sander, U.: Helping johnny 2.0 to encrypt his facebook conversations. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, pp. 11:1–11:17. ACM (2012)
5. Friedland, G., Sommer, R.: Cybercasing the joint: on the privacy implications of geo-tagging. In: Proceedings of the 5th USENIX Conference on Hot Topics in Security, HotSec'10, pp. 1–8. USENIX Association (2010)
6. Henne, B., Smith, M.: Awareness about photos on the web and how privacy-privacy-tradeoffs could help. In: Adams, A.A., Brenner, M., Smith, M. (eds.) FC 2013. LNCS, vol. 7862, pp. 131–148. Springer, Heidelberg (2013)
7. Henne, B., Szongott, C., Smith, M.: Snapme if you can: privacy threats of other peoples' geo-tagged media and what we can do about it. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '13, pp. 95–106. ACM (2013)
8. Klemperer, P., Liang, Y., Mazurek, M., Sleeper, M., Ur, B., Bauer, L., Cranor, L.F., Gupta, N., Reiter, M.: Tag, you can see it!: using tags for access control in photo sharing. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '12, pp. 377–386. ACM (2012)
9. Mahmood, S., Desmedt, Y.: Usable privacy by visual and interactive control of information flow. In: Christianson, B., Malcolm, J., Stajano, F., Anderson, J. (eds.) Security Protocols 2012. LNCS, vol. 7622, pp. 181–188. Springer, Heidelberg (2012)
10. Mahmood, S., Desmedt, Y.: Poster: preliminary analysis of google+'s privacy. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11, pp. 809–812. ACM (2011)
11. Maurer, M.E., De Luca, A., Kempe, S.: Using data type based security alert dialogs to raise online security awareness. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS '11, pp. 2:1–2:13. ACM (2011)
12. Sheng, S., Broderick, L., Koranda, C.A., Hyland, J.J.: Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium on Usable Privacy and Security (2006)
13. Shin, D., Lopes, R.: An empirical study of visual security cues to prevent the SSLstripping attack. In: Proceedings of the 27th Annual Computer Security Applications Conference, pp. 287–296 (2011)