Making Rich Media Accessible for Generations:

Trust, Security and Privacy Issues with Personal Media on the Web 2.0

Lothar Fritsch, Knut Holmkvist, Truls Fretland
Norsk Regnesentral – Norwegian Computing Center
Oslo, Norway   www.nr.no

Abstract

The Web 2.0 provides various opportunities to maintain, share and publish personal media collections such as photo or video albums. The collection and sharing of personal media on other parties' platforms requires trust in these platforms and their operators as well as in the other users. In the MARIAGE project, we research the issues under the perspective of long-term availability. With short-term access control to Web 2.0 platforms, and access control policies for social networks, the long-term issue is not sufficiently covered. This article presents trust, security and privacy issues arising when handling personal media objects in the long-term perspective.

1 Introduction

The pre-web Internet had many features: Email, News-groups, Archives (Archie), File Servers (FTP), Finger and so on. Users formed communities where they shared information, discussed common issues and posted and read news. With the introduction of the Web, Internet in addition became a support and trading place. Users can download manuals and software upgrades. Users can buy or book almost anything, books, hotel rooms and clothing.

Although the Web has been commercialised, pre-web type services and applications did not disappear. On the contrary, they prospered in web communities, blogs and resource sharing. This type of services and applications are generally referred to as Web 2.0[1]. Whereas the pre-web Internet was almost totally text based, Web 2.0 is to a high degree dominated by rich media, which however is not well-defined (see page 2 of [2]).

In the project MARIAGE ("Making rich media accessible for generations", Norges forskingsråd project 181819), we primarily address rich media made by non-professionals ("prosumers") but we also consider bought media. As a matter of facts, the idea started out with a question of how young people of today could play their bought music 25-30-50 years from now. How to find and play a music file you bought decades ago?

Some people restrict the Web 2.0 to participation, publishing and sharing. We include the whole "production chain" of private rich media. Prosumers will want to produce and manage their media, share some subsets with limited groups of people and publish other subsets for general consumption. Web 2.0 thereby will include tools for capturing and managing media. Several such tools already exist.

This raises many trust issues. Media will be shared, published, packaged, stored and tagged by various stakeholders on many platforms. From the individual prosumer's perspective, the challenges arise where media objects, their tags and their ownership must be available and usable over a long period of time – spanning his whole lifetime and possible the lifetime of his descendants. The lifetime perspective is yet one of the major weaknesses in the Web 2.0 paradigm – as the average lifetime of online community platforms has been found to be low – one community paradigm loses prosumers to the new paradigms easily, as shown in [2].

1.1 Problem Statement

Lifetime control over personal media objects is a growing problem. Up to now, the complexity of handling family photos was restricted to the number of cardboard boxes with photos, albums and videotapes in them. But today, digital media objects are collected on various physical and virtual media, ranging from memory cards over mobile phones up to remote servers, internet services or other people's computers in peer-to-peer networks. The vision of a "family album" handed down from grandparents to grandchildren has yet to be defined for the digital media world. Problems increase with the ease of producing, moving, copying and distributing digital media. Problem areas are:

1. Long-term storage, tagging, and usage of media objects with meaningful metadata
2. Trusted sharing of media objects with friends and family on the Internet
3. Publication of media objects on publicly available platforms

Three major aspects of personal long-term use of rich media are concerned with future accessibility and usability of rich media objects in the face of:

1. Data formats
2. Rights management
3. User interface

Focusing on the W2Trust workshop scope, this paper identifies long-term implications of digital rights management (DRM) on personal rich media, and the aspects of control of own media objects. This includes, but is not restricted to identification of media, proof of ownership, and expression of policies. We will argue that metadata security is the most relevant topics for trust in Web 2.0 media platforms.

1.2 The MARIAGE Approach

The MARIAGE project aims at the development of principles, frameworks and demonstrators for life-time media albums. Media types of interest are photographs, videos, music and software-based media such as web pages, flash films, and computer games. MARIAGE focuses on the "prosumer" type of user, a person who is producing and consuming media objects. MARIAGE deals with long-term availability of execution environments, with media format availability in a life-time perspective, with metadata management, and with interoperability between the media album platforms that prosumers use.
Our focus in the Web 2.0 trust analysis are visual media, as digital photography and amateur videography are the dominant media objects on the Web 2.0. There are some issues with text in blogs, but generally the text format conversion, indexing and search problems in text archival and retrieval are researched for more that a decade by the discipline of library science[3].

2 Personal Lifetime Use of Rich Media

In MARIAGE, we performed an examination of current software platforms for personal media management. Platforms examined were mainly in the areas of digital photo and digital video, as we assumed the number of home-produced audio or computer game products to be low compared to the aforementioned media forms. Additionally, we focused on self-produced media handling – objects that are own creations, or that are available for wide uses, e.g. photos provided within a social group, or from public sources. The examined platforms are shown in Figure 1.

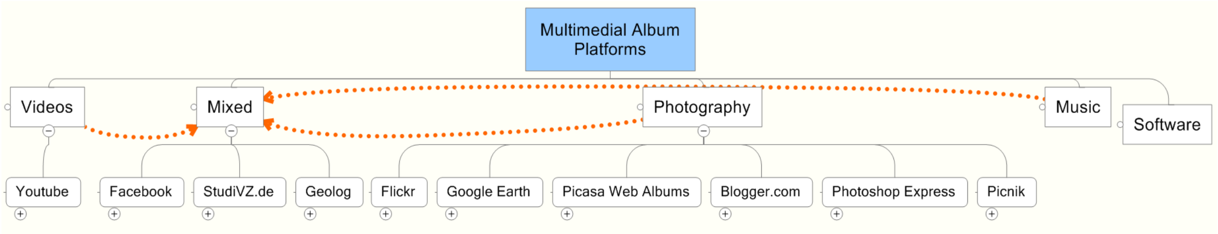

Figure 1: Media platforms examined

Upon analysis and use of publicly available platforms and social networks, the separation of media objects along their ownership or copyright properties became evident. We found important differences between self-produced items, bought items, items obtained with restrictions, and items created and posted by minors. The latter class might need parental approval before it can be published. Figure 2 shows our classification of objects according to ownership rights and copyright. While we focus on self-produced and unlimited-use-objects, it is nonetheless worthwhile to notice that some online platforms request some parts of copyright for their own purposes as soon as people upload their media objects. This is further elaborated in section 2.2.5.

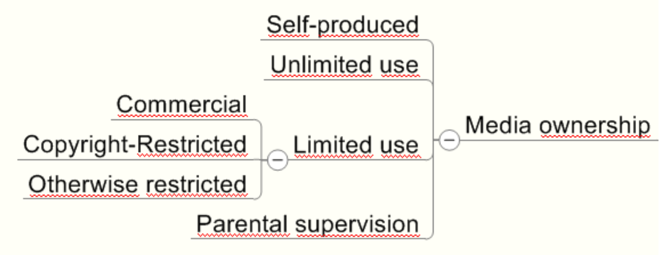

Figure 2: Types of media objects with respect to ownership / copyright

2.1 *Trust Areas & Media Transactions*

This section presents a conceptual model of personal, lifetime media handling. The model is oriented along trust areas. A trust area is a level of trust that is needed in the IT system handling the media objects. We will explain the trust areas, and derive vital media transactions carried out by owners and users of the media objects. From these transactions, we will examine threats for security and privacy and their relevance in the different trust zones.

2.1.1 Trust Areas

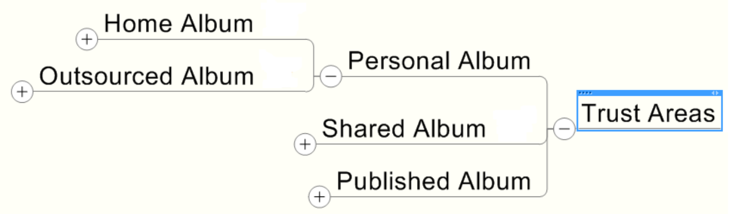

Figure 3: Trust areas in media handling

A personal media album is a prosumer's media storage for long-term use. This can be physically located on one or more home computers, Home media albums, on an Internet service, an outsourced media album, or on a combination of these. An outsourced media album should have the same basic functionality as a home media album, with the exception of added "privacy control". An example is the encryption with Norway's Telenor's data storage service "Telenor Sikker Lagring". This is a storage service where

customers are given a cryptographic key to their content. If the user looses the key he will not get access to the data as Telenor cannot decrypt the data without this key.
A shared media album is where the prosumer give rights, at least access right, to a subset of her media to a limited group of people. A published media album is where the prosumer grants public access and other rights to her media. In both cases "the media" could physically be the media object residing in the personal media archive, or a different copy.

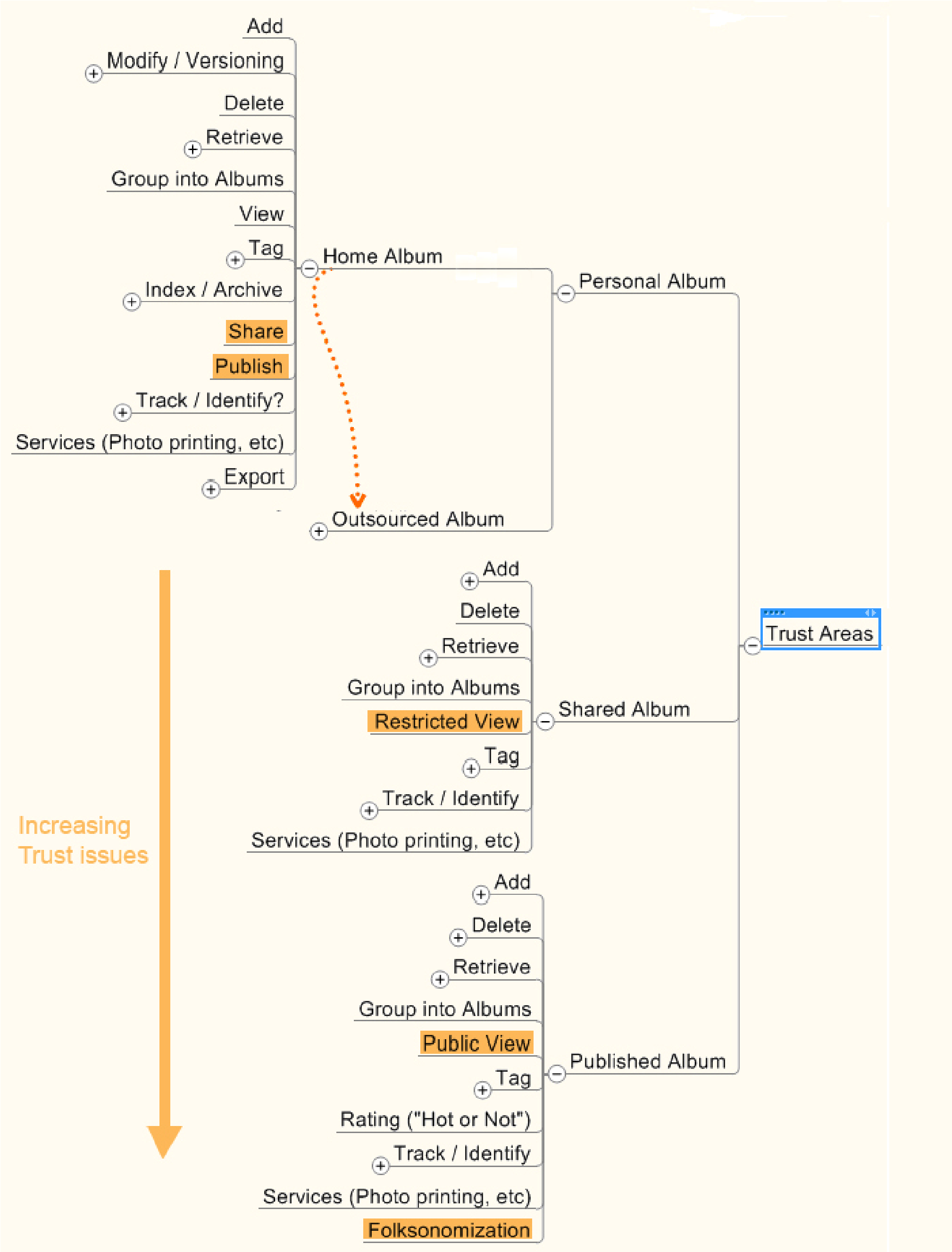

Figure 4: Transactions in media handling

In Figure 3, the four trust areas for media albums are shown. Please note that from top to bottom, the exposure of media to other computer systems or other persons increases, thereby increasing threats and security requirements.
In our conceptualization, in the lifetime perspective a prosumer will administer his personal album, while at the same time use subsets and subversions of his media object collections on various on-line platforms for private use, sharing or publishing. Sets of objects might get lost in the personal album, and can be claimed back after a long time from an on-line service. Our assumption is that a prosumer will collect millions of media objects, such as digital snapshot photos, and might wish to retrieve them many years in the future. For this purpose, upon addition of new objects into the album, tagging operations to add places, keywords and other contextual metadata are absolutely necessary.

2.1.2 Media Transactions

In this paragraph we discuss the transactions or handlings prosumers do on their media, exemplified by photos. Figure 4 summarise these transactions. We start with a set of transactions for the Personal media album, i.e. for Home and Outsourced media album. We assume that for some areas, like image adjustments, the transactions on Shared and Published media album will be a subset these. In other areas, like rights management, transactions not needed in the personal media album will be added.

Basic transactions are addition, versioning and format update, retrieval and removal of media objects from the album.

Viewing transactions deal with showing of media objects and their grouping into albums.

Administrative transactions care for indexing, archival and backup issues, tracking and identification issues, and the export of media objects.

Transfer transactions are those transactions that make media objects available for sharing in a closed group, or for publishing.

Public transactions include rating, folksonomization [4], image identification and services such as printing.

In this paper we concentrate on trust, privacy and security issues. We will not go into detailed on transactions not related to these areas. Note that some of the transactions will have different trust implications depending on what trust area they will be carried out at.

2.2 Trust, Privacy & Security Issues

Here we discuss the transactions related to trust, privacy and security issues.

2.2.1 Access Control

The first concern is access to the media album. Here, access control methods are used over most platforms with an exception of the personal album clients that rely on personal computer access control. Issues here are:

- Person- and group-centric access control in shared albums
- Access to home and on-line personal albums, encryption, long-term security, key recovery
- Revocation of access control over time
- Identify management concepts for a lifetime, e.g. Overcoming access control later in life (forgotten passwords, lost authentication services or identity providers)

Many of today's online platforms provide simple access control mechanisms based on discretionary access control schemes, possibly combined with simple grouping and 2 distinct security levels (private / public). For a lifetime control of access, no concepts of access privilege handling, privilege inheritance and revocation thereof exist.

2.2.2 Ownership, Usage Policy and Tracking

The ownership of digital media objects is an important issue on the Web 2.0. Ownership is important when managing the own personal archive with own and other's media objects in it. It is also important to be able to define policies on media object usage on platforms, where more security issues occur. The main issues we identified were:

- Identifiability of media objects
- Trackability of media objects
- Ownership and IP attribution of media objects
- Use policies upon sharing & publishing

The issue of policy enforcement is similar to the problems and security goals in digital rights management (DRM), where the control over the usage of media objects by other parties is sought to be enforced. However, in managing private media, the main issues are access control to the restricted parts of the album, and the tracking of objects that are taken out of the album and used elsewhere on the Internet. For the private user with its restricted resources for enforcement and legal procedures, we recognize the tracking, identification of trust breaches, and the exclusion of the violator from the shared access to be the best possible measure of protection. This principle was used for example in the "Personal Rights Management" [5], where privacy infringement by mobile phone photography posted to the Web is tackled. For trust management in personal media access control, this implies that the most care shall be exercised in the granting of access privileges to shared albums, and public albums.
Important base technologies for this aspects are watermarking[6], steganography[7], and perceptual image hashing[8].

2.2.3 Metadata Lifecycle & Tagging

Metadata is crucial for finding and understanding media. Metadata contains semantic descriptions, links, ownership and intellectual property information. For photos, EXIF [9] is the standard metadata format. Most digital cameras write EXIF-headers in the photos taken. The camera includes metadata like name and type of camera, use of flash, aperture and "film speed". Other metadata can be added automatic, e.g. position data, or manually, e.g. names of people in the photo. On-line platforms allow the later addition of location metadata, person names, event names or arbitrary tags. The tags are of high importance for later image retrieval from large albums, but there is a difference in tags made and tags needed for later retrieval [10]. When exchanging media objects between several platforms and albums, it is important to manage metadata correctly for several reasons:

- To support life-time retrieval with metadata-based search
- To synchronize several copies and versions of albums
- To preserve privacy by filtering metadata such as names, location or time from the metadata before it is put in public albums
- Preserve and authenticate metadata in the media objects for later re-integration of shared or published material into the personal album

On our survey of platforms of the Web 2.0, we found that mostly tagging is done to apply geographic data, keywords, person names, event names and links to other photos or albums are performed (see Figure 5). Additionally, peer-rating or peer-tagging can occur.

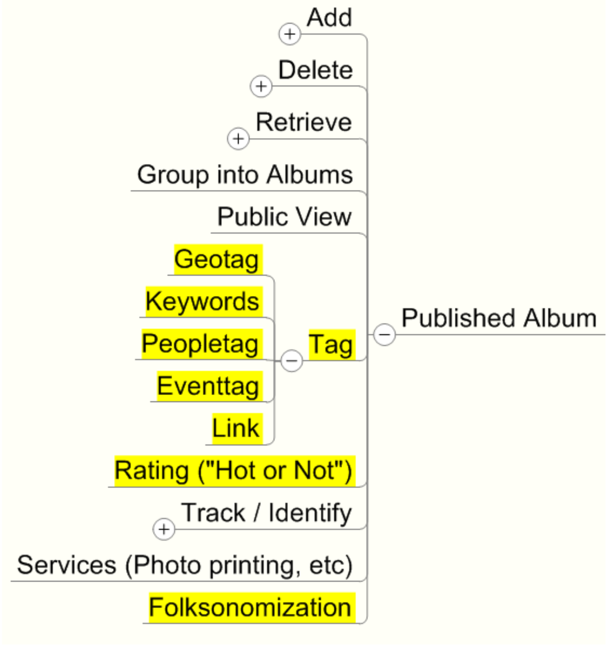

Figure 5: Metadata created through tagging (tags marked yellow)

As this information is essential for finding and understanding photos, this information need to be kept during copy and move transactions. On the other hand, some of this metadata information can reveal private matters, such as information about the used camera model, the names of people in the photos along with the position of the photo shooting in GPS precision, and more. Metadata management faces two major challenges with respect to trust on the Web 2.0:

1. Secure the connection between the media objects and the metadata
2. Manage the flow of - potential sensitive and confidential - metadata information – from the personal album to the shared and public albums

Several occurrences of metadata privacy breaches have occurred. Three examples are shown in Figure 6. The first image shows the display of image EXIF metadata within public Picasaweb albums[1]. The service reads EXIF headers into its album database, and shows their content next to the digital photographs in an album. On the presence of geotags, a map of the photo location is shown. As shown in Figure 6 in the top-left image, such a web album might be an information resource for burglars, revealing camera models, location and photographer activity timing. The second example in Figure 6 shows a risk provided by EXIF thumbnail pictures embedded in digital photos. In the illustrated case, the American journalist Cat Schwarz posted photos of herself on her blog. These photos contained thumbnail images from a larger photo, revealing nude photography to the public[2]. The third trust breach example on the bottom of Figure 6 is a breach of professional secrecy. In February 2006, the Washington Post featured an anonymous young hacker in the article “Invasion of the computer snatchers”[3]. At publishing time, there also was a distorted photo of the hacker published on the web page with the article. As shown in the “Cybercrime law blog”[4] on August 7, 2007, digital cameras can pose a security risk.

[1] See picasaweb.google.com, screenshot as of March, 2008.

[2] www.geocities.com/cat_nude/, as of March, 2008.

[3] www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html, as of March, 2008

[4] http://www.cybercrimelaw.org/2007/08/07/digital-cameras-as-a-security-risk/, as of 16-Apr-2008.

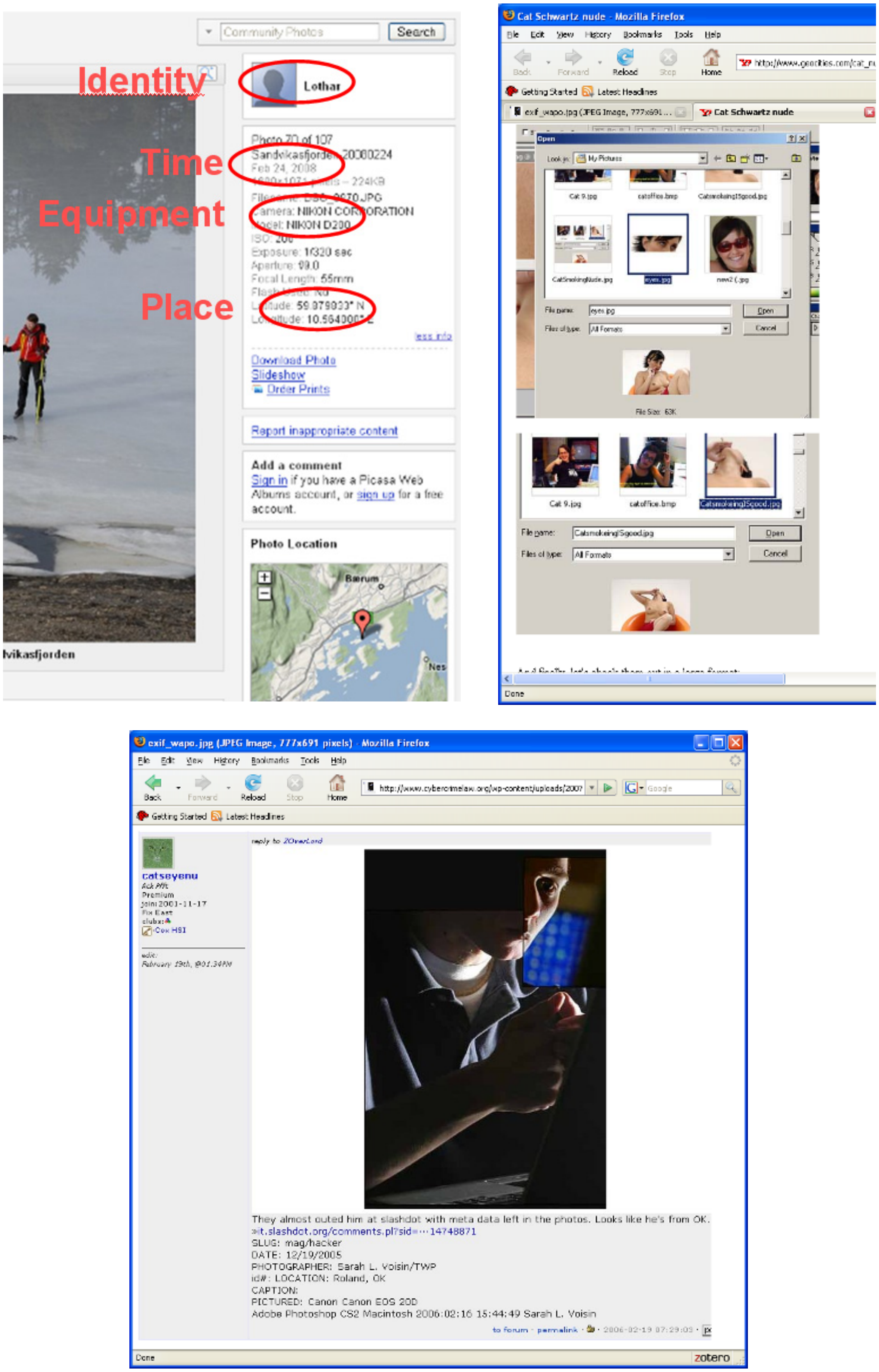
Identity
Time
Equipment
Place
Community Photos
Search
Lothar
lvikasfjorden
Photo Location
Bærum
Nes
Cat Schwartz nude - Mozilla Firefox
exif_wapo.jpg (JPEG Image, 777x691 ...
Cat Schwartz nude
Open
Look in: My Pictures
Cat 9.jpg
catoffice.bmp
CatsmokingI5good.jpg
CatSmokingNude.jpg
eyes.jpg
new2 (.jpg
File name: eyes.jpg
Files of type: All Formats
Open
Cancel
File Size: 63K
File name: CatsmokingI5good.jpg
Done
exif_wapo.jpg (JPEG Image, 777x691 pixels) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Back Forward Reload Stop Home
http://www.cybercrimelaw.org/wp-content/uploads/2007
Google
Getting Started Latest Headlines
zotero

Photo 70 of 107
Sandvikasfjorden 20080224
Feb 24, 2008
1600x1071 pixels – 224KB
Filename: DSC_0970.JPG
Camera: NIKON CORPORATION
Model: NIKON D200
ISO: 200
Exposure: 1/320 sec
Aperture: f/9.0
Focal Length: 55mm
Flash Used: No
Latitude: 59.879833° N
Longitude: 10.564000° E

less info

Download Photo
Slideshow
Order Prints

Report inappropriate content

Add a comment
Sign in if you have a Picasa Web Albums account, or sign up for a free account.

reply to 2OverLord

catseyenu
Ack Pfft
Premium
join: 2001-11-17
Fix East
clubs:
Cox HSI

edit:
February 19th, @01:34PM

They almost outed him at slashdot with meta data left in the photos. Looks like he's from OK.
»it.slashdot.org/comments.pl?sid=···14748871
SLUG: mag/hacker
DATE: 12/19/2005
PHOTOGRAPHER: Sarah L. Voisin/TWP
id#: LOCATION: Roland, OK
CAPTION:
PICTURED: Canon Canon EOS 20D
Adobe Photoshop CS2 Macintosh 2006:02:16 15:44:49 Sarah L. Voisin

to forum · permalink · 2006-02-19 07:29:03 ·

Figure 6: Examples for metadata privacy risks. Detailed information in a public album (upper left), full exposure in an EXIF thumbnail (upper right), betrayal of journalistic source through location metadata on a digital newspaper photograph (bottom).

The photographer was filling her photos with EXIF headers, and coded the photo location into the photo of the hacker. This was a very small village. The location name was available in the EXIF headers on the Washington Post web page, thereby betraying the hacker's anonymity in the article – and exposing him to prosecution threats with anti-hacking laws.

2.2.4 Media and Digital Rights Management

Digital Rights Management (DRM) aims at controlling the use and distribution of digital media objects. DRM systems generally encrypt media, and rely on trustworthy software and services for decryption and use of the media objects. In our report on the state of the art in DRM [11], we examined and classified contemporary DRM systems. We classified DRM systems according to their basic type (active or passive), their restrictiveness on media usage, and the dependency of media objects on the full functioning of the DRM infrastructure. Clearly, restrictiveness and dependency are two crucial properties for long-term usability of media objects. Figure 7 summarizes our classification.

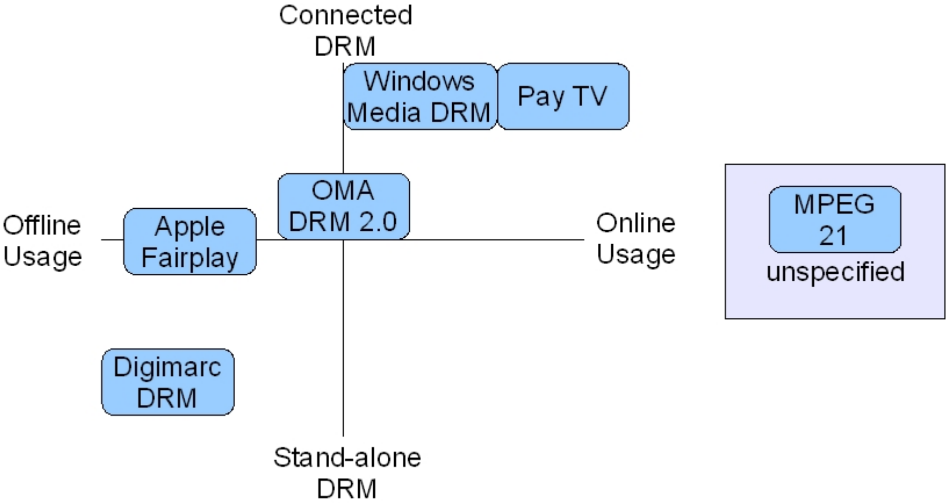

Figure 7: DRM classification in MARIAGE

We found that passive DRM systems – that enable media tracking and accountability – are generally less restrictive and less dependent. In Web 2.0 systems, the long-term aspect of DRM should be taken serious within the trust model, as with raising competition any Web 2.0 operator is very dependent in keeping customer trust.

2.2.5 Challenges of the "Web 2.0"

2.2.5.1 Publicity

The inherent publicity of media objects on the Web 2.0 creates various issues. Two areas can be distinguished:

- Information revealed by own actions
  Personal metadata, social networks, photo locations, names of friends and other information can leak out to the public.
- Information revealed by others' actions
  Cross-tagging, as possible on several platforms, enable other users of the Web 2.0 service to tag and comment a prosumer's media objects, thereby revealing information that has been kept secret by the owner of the media object.

A strong challenge of the Web 2.0 is the enabling of trust in confidentiality and privacy in networked, tagged and shared media objects.

2.2.5.2 Eternal memory

With reference to the previous section, the eternal memory of search engines and on-line archives poses a problem when personal data leaks out. As of today, it is considered impossible to revoke information that was publicly available in Internet information systems. The long-term use of personal media objects in Web 2.0 communities requires consideration of this. A wishful development would be that of revocation possibilities or the enforcement of restrictive archival and indexing policies.

2.2.5.3 Terms & conditions

In the case of the early Photoshop Express photo album and manipulation platform, Adobe caused some irritation among photographers in March and April 2008 by claiming unlimited licences of photographs published to the public on their platform. An update of the terms of use on April 10, 2008 reduces this unlimited license to the license to use content on the Photoshop Express platform together with Adobe's partners, and in advertising and advertising revenue generation. As some platform providers of the Web 2.0 target at harvesting prosumer contributions for their own commercial purposes, a clear policy and intellectual property situation is advisable. Sources: Adobe.com terms of use, version April 10, 2008, https://www.photoshop.com/express/terms.html paragraph 8 and 10:
Modified by: Adobe Photoshop Express Additional Terms of Use Effective April 10, 2008, https://www.photoshop.com/express/pxterms.html

3 Research challenges in lifetime multimedia

From the issues, threats and challenges described above, we present the main research challenges for the lifetime handling of media objects by prosumers. In Figure 8, we summarized the major trust, security and privacy issues for lifetime multimedia handling on the Web 2.0

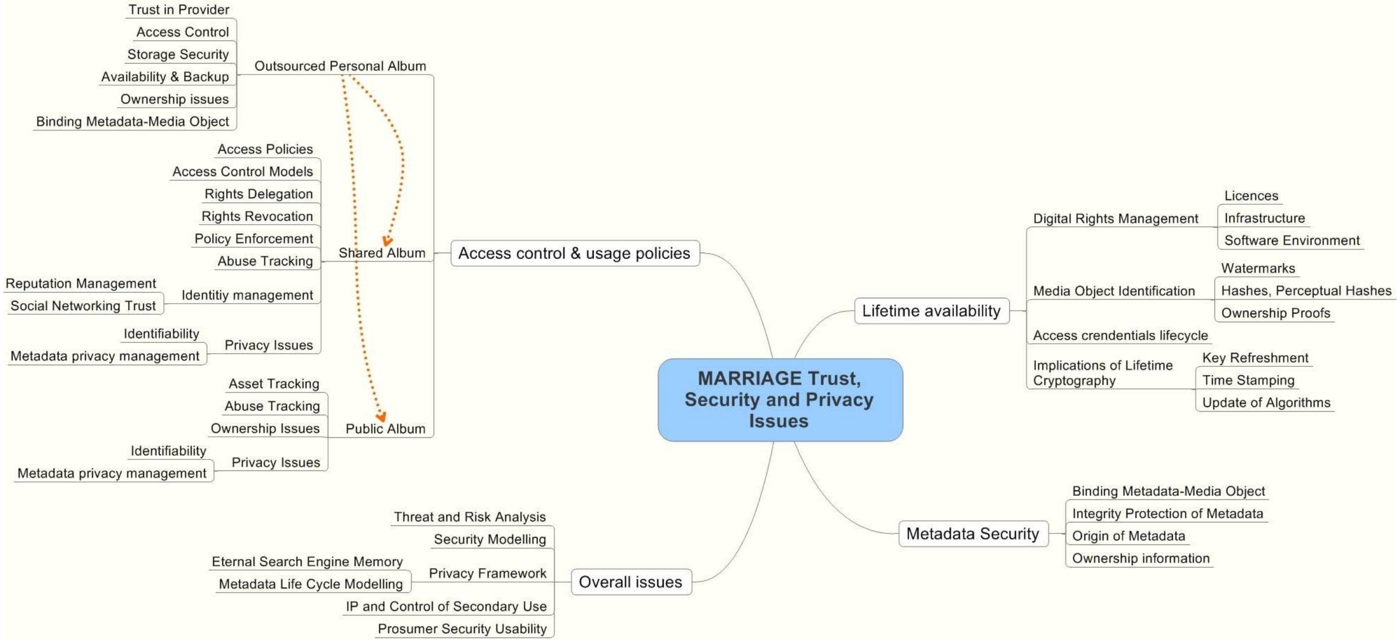

Figure 8: Research challenges in lifetime multimedia security

Many of these issues are not well researched under the lifetime and multi-generation perspective. The closest activities in this area are performed on the topics of long-term archival of signed documents, and on long-term archival of digital objects in a museum context, where uninhibited access and intellectual property management are the focus areas.

4 Conclusion

The lifetime handling of personal multimedia objects introduces a number of new trust, security and privacy challenges for the Web 2.0. These relate to long-term availability, to the flow of privacy-sensitive metadata, to object identifiability, access control, rights management and long-term availability of cryptography. With the movement of media albums over mobile devices, personal computers and on-line platforms, a overall framework for security in personal, lifetime multimedia is needed. This article summarizes the issues the framework must cover for increased trust in the Web 2.0 for a long period of time. A trustworthy, sustainable Web 2.0 platform for personal multimedia albums then might have the opportunity to keep its users and subscribers for a lifetime.

5 References

[1] T. O'Reilly, *What Is Web 2.0.* 2005.

[2] M. Madden and S. Fox, *Riding the Waves of "Web 2.0".* Washington DC, USA: 2006.

[3] J. Rothenberg, "Ensuring the Longevity of Digital Documents," *Scientific American. vol.* 272, pp. 24-29, 1 1995.

[4] A. Mathes, *Folksonomies - Cooperative Classification and Communication Through Shared Metadata.* Urbana-Champaign: 2006.

[5] M. Deng, L. Fritsch and K. Kursawe, "Personal Rights Management," *in Privacy Enhancing Technologies - Proceedings of the 6th workshop on privacy-enhancing technologies PET2006,* vol. 4258, G. Danezis and P. Golle, Ed. Berlin: Springer, 2006.

[6] B. Furht and D. Kirovski, *Multimedia Watermarking Techniques and Applications.* Boston, USA: Auerbach Publishers,2006.

[7] T. Morkel, J. Eloff and M. Olivier, *An Overview of Image Steganography,* 5th Information Security South Africa ISSA 2005, 2005, Sandton, South Africa.

[8] S. Wang and X. Zhang, "Recent development of perceptual image hashing," *Journal of Shanghai University. vol.* 11, pp. 323-331, 4 2007.

[9] Japan Electronics and Information Technology Industries Association, *Exchangeable image file format for digital still cameras: Exif Version 2.2.* 2002.

[10] M. Naaman, Harada Susumu; Wang QianYing and Wang QianYing, *Context Data in GeoReferenced Digital Photo Collections,* ACM Multimedia 2004, 2004, New York.

[11] T. Fretland, L. Fritsch and A. Groven, *State of the art of digital rights management.* Oslo, Norway: 2007.