Framework for Privacy in Photos and Videos When using Social Media

Srinivas Madhisetty and Mary-Anne Williams
Magic Lab, University of Technology Sydney, Ultimo, Sydney, Australia

Keywords: Privacy in Photos and Videos, Tacit Information.

Abstract: Privacy is a social construct. Having said that, how can it be contextualised and studied scientifically? This research contributes by investigating how to manage privacy better in the context of sharing and storing photos and videos using social media. Social media such as Facebook, Twitter, WhatsApp and many more applications are becoming popular. The instant sharing of tacit information via photos and videos makes the problem of privacy even more critical.The main problem was, nobody could define the actual meaning of privacy. Though there are definitions about privacy and Acts to protect it, there is no clear consensus as to what it actually means. I asked myself a question, how do I manage something when I don't know what it means exactly? I then decided to do this research by asking questions about privacy in particular categories of photos so that I could arrive at a general consensus. The data has been processed using the principles of Grounded Theory (GT) to develop a framework which assists in the effective management of privacy in photos and videos.

1 INTRODUCTION

This research contributes by investigating how to manage privacy better in the context of sharing and storing photos and videos using social media. There are many definitions of privacy, however the Oxford dictionary defines privacy as "A state in which one is not observed or disturbed by other people".

In layman term's, loss of privacy is when sharing of information takes place. This is irrespective of whether the information is sensitive or not. There is a loss of privacy when any information is shared. When we share a document or reveal certain information our exchange of information is grounded through a specific context. Proper grounding of the context is not afforded when photos and videos are shared. This is because a photo or a video can contain rich semantic and syntactic information coded as tacit knowledge. As the information is tacit, it becomes difficult to morph any abstractions that could be made from the photo or a video. This makes it more difficult to manage content as information freely passes through without any checks or balances that are afforded in other means of communication.

Social media such as Facebook, Twitter, WhatsApp and many more applications are becoming popular. The instant sharing of information via photos and videos makes the problem of privacy even more critical. There are severe unintended consequences when sharing of personal and other sensitive information is done without proper checks and balances.

This research is about how to store and retrieve photos by identifying key sensitive information embedded in photos and videos. By regulating the flow of information in photos and videos, privacy is managed effectively. (Bennett and Raab 2002) envision a privacy "regime" that integrates privacy policy instruments – including data protection legislation, voluntary fair information codes and privacy-protective information practices - in a global economy which is characterized by regulatory interdependence. Social networks provide unprecedented opportunity for individuals and organisations to share information. At the same time they present significant challenges to privacy (Chen and Williams 2009).

Identifying sensitive information in a photo or a video is a major problem. For example, what is sensitive to one person may not be sensitive to others. Therefore, rather than making assertions

Madhisetty, S. and Williams, M-A.
Framework for Privacy in Photos and Videos When using Social Media.
DOI: 10.5220/0006073803310336
In *Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017) - Volume 3*, pages 331-336
ISBN: 978-989-758-249-3
Copyright © 2017 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

about what is sensitive in a photo or a video, I have asked my participants why they share content and what are their concerns. This enabled me to deduce what was sensitive according to them. This enabled me to develop a conceptual framework which assists in the effective management of privacy particularly in photos and videos when shared through social media.

The main problem is that, after initial publication of the content using social media, its subsequent persistence makes the content not ephemeral. Technology enables the content to be available, such loss of privacy can be attributed to the lack of control about the content published using this relatively new technology. It will have a significant impact on individual privacy. The ephemeral nature of information is important to be able to have desirable levels of privacy. For example, when people move on from and into relationships and other major life events, an individual should be able to exercise the right to be left alone. With others able to republish photos and videos using social media the individual's privacy is breached significantly. "People should have the freedom to share whatever information they want, in any medium and any format", the freedom to access all of the information made available to them by others" and "the freedom to build trust and reputation through their identity and connections" (Facebook 2011).

2 THE PRIVACY PROBLEM

Privacy is not well defined; contextualising privacy is very difficult as the term privacy is subjective. Privacy means different things to different people. The concept of how well privacy is managed is often debatable. Managing privacy becomes more difficult when it comes to photos because photos contain tacit information which is very difficult to contextualise.

The two main artefacts that were diagnosed from conducting this research were that there was inadequate information about privacy and its consequences after users publishing their content such as a photo or a video. A mismatch of expectations of what was the intent to publish the photo versus how may be perceived and viewed over a period of time. There is a dire need for understanding of the subject in the photo and the context of the photo about what it represents needs to be established. It is an almost an impossible task to contextualise all photos, unless one has access to petabytes of data like most social media applications. Therefore a deductive method for analysing photos for privacy was not chosen. To understand how sensitive information in a photo or video is shared and stored in a particular manner does not affect the privacy of the photo, is the objective of this research. This research was conducted by asking people why they like to or has shared their photos or videos using social media. By understanding their expectations for publishing content, this research could arrive at a clearer picture about the subjective opinion on why participants consider their privacy has been breached. Questions about the metadata of the photo or video, were asked to understand the tacit properties of the photo or a video. This may not give the exact contextual properties, but have given a clear indication under which circumstances the photo or video was taken. The information captured was about the shutter speed, ISO, aperture, type of lens being used, etc. Through this tacit information tagged in a photo it is easy to make inferences about the circumstances the photo was taken at that time. Big Data could be used to process this metadata in post that it could build a significant profile about the individual, which could be a direct breach of privacy.

2.1 Research Question

How can sensitive information be stored, retrieved and managed in a photo or a video? To answer that question, first it is essential to determine what sensitive information people believe exists in a photo in a particular category, i.e. Family photo, holiday photo, profile pictures, etc. Second, it is important to associate these findings to assist in developing a framework which will assist the general public to manage their privacy effectively.

It is also equally important to understand the underlying motivations in sharing the photo and to be able to understand its context. The critical features which will allow information in a photo to pass through without affecting its privacy need to be understood and investigated. This understanding of expectations versus their consequences will give rise to the determinants of privacy. These determinants will manage how the information in a photo will be stored and retrieved.

For example, in the United States' the Internal Revenue Service searches Facebook and MySpace for evidence of tax evaders' income and whereabouts, and the Citizenship and Immigration Services have been known to scrutinise photos and posts to confirm family relationships or weed out sham marriages. Employers sometimes decide

whether to hire people based on their online profiles, with one study indicating that 70 percent of recruiters and human resource professionals in the United States have rejected candidates based on data found online. A company called Spokeo gathers online data for employers, the public and anyone else who wants it (Andrews 2012).

2.2 Motivation & Limitations

Using social media where anyone can publish photos and videos of any other individual, mostly well-intended at the time, could result in a huge concern later. So the consent to publish the photo or a video temprois at that moment. Once the photo or video is published, it is available for people to see until it is removed by the publisher. During my interactions with social media, I have encountered several issues in relation to privacy. The instant availability of information is one such example. Social media is a channel which distributes information instantly.

2.2.1 Significance of this Research

Though people have asked similar questions, they have not yielded a concrete answer. I intend to ask questions on a category basis, i.e(family photos, holiday photos etc) in order to obtain an objective meaning about privacy for that category. I understand that my research will yield answers which will be an indicator and not heuristics, because in my opinion privacy is a social construct. This construct of privacy has to be revisited several times to obtain paradigm after paradigm to be able to construct a total view about privacy. This is my attempt to construct this paradigm.

2.2.2 Research Methodology

We are able to categorise information in the news to reduce harm, as the newsreader announces that what they are about to show may cause distress to the viewer. Similarly, categorising photos could be done. The only problem is that they are so many of them, so how can we identify the PI (personal information) stored in a photo or a video as sensitive information? As privacy is a social construct, we can only manage privacy. There is no one solution to fix it. I characterise photos based on the settings of the photo (portrait, landscape, sports, etc, as well as various types of activities people tend mostly to share such as birthday photos, holiday photos, etc. With low-level categories which were not able to be included as a core category, an aggregation was made to be able to assimilate the data collected into the core categories.

At an epistemological level, the relationship between the researcher and what is being researched is observed in a contextualised subjective environment to derive certain objectivity. This research does not make any generalisations or quantify issues using numbers, but presents contextual findings grounded in the data, staying close to the construction of the world as participants originally experience (Maykut and Morehouse 1995); (Creswell 2003). Direct quotes of de-identified people were used to generate themes. According to (Stratus and Corbin 1998) avoiding preconceptions help the researcher to be more faithful to the data and more open about what the data is saying.

Expectations of people about the qualities of a photo or a video versus how these qualities embedded as tacit knowledge. This is the reason why Grounded Theory was chosen to develop themes and develop a framework to manage privacy effectively. Barney Glaser and Anselm Strauss have written a powerful book “The Discovery of Grounded Theory”. This method of research is vastly different to the conventional method for doing scientific research. It is more of a top-down approach. Rather than looking for a hypothesis after the literature review, the researcher is encouraged to find the patterns in the data after collection. (Grey 2009) argued that deductive reasoning moves towards testing a hypothesis, based on empirical evidence. However inductive reasoning seeks to discover binding principles to construct generalisations, relationships, and theories after analysis of data. It does not negate existing theories but outlines and stabilises them by collecting data (Grey 2009).

2.2.3 Data Collection

Surveys and questions that include open-ended questions that resemble interviews were used to generate data (Warburton 2005). Interviews produced a considerable amount of data. (Charmaz 2006) states that the GT approach is a set of principles and practices. This research has chosen 21 interviews to reach theoretical saturation. Data collected satisfied the criteria for GT analysis. A semi-structured style of interview was chosen to collect sensitive and complex responses so it could be converted to data. A semi-structured interview facilitated to ask questions which were open-ended and allowed the participants to talk freely about the contextual nature of what he or she shares using the

social media platform. I was able to derive in-depth data sets about what was the contextual nature of the media which my participants shared.

2.2.4 Key Findings

Four main themes emerged in this framework, in which nine categories explored the relationship between several sub-categories bundled into one, to better describe the phenomena of privacy. The four themes were, had no particular privacy concerns. Moderate concerns about sharing of PI. Serious concerns will do anything to control the flow of information others share. Will not participate in social media at all.

2.2.5 Key Categories

The data collected was broken down into key categories and each higher level categories had further sub categories. The most critical of the themes where there was a lot of detail in terms of categories was with the first theme, had no particular privacy concerns: The nine main categories are, Trust vs control of information. What kind of photo is shared and its appropriateness. Unintended consequences. Perceptions of others and how they engage with their belief system. Effective ways to communicate. To be able to relate to a larger audience. Information overload, Effective ways to filter information. Targeting by third parties to use the information in ways it was not intended to be used. Themes were characterised by particular questions which were more relevant.

Overarching questions for all Themes were the two below to find out what privacy means from a subjective sense to develop a rational objective. Tell me what you think about privacy concerns you have in relation to photos and videos. What is your general motivation to share photos and videos, and does that benefit you in any way?

Theme 4.2.1: What types of photos would you share using social media? How do you manage risk of sharing photos and videos? Do you trust social media privacy settings?

Theme 4.2.2.1: This is characterised by the motivation for sharing content with others. i.e (Motivation to share personal information with others, to derive a rational why this sharing of information is necessary?) Questions which were most relevant for this theme were “Do you believe that the consent is implicit when a photo is taken that it could be published latter using social media?

Theme 4.2.2.2: This theme is to develop a comprehensive understanding of the relationship that is between implicit and explicit consent to mitigate circumstances in terms of delivery of the content during pre & post publishing phase. Questions which were relevant were what are your concerns in relation to sharing of photos and videos. How does sharing benefit you in any way?

Theme 4.2.2.3: A timeframe was a key to manage privacy. For content to be managed effectively a timeline, which has a timeframe for photos and videos is very important. Questions which were relevant were What is the timeframe or how long do you think a photo or a video should be made available for others to see after it gets published?

2.2.6 Categories Evolved from the Theme

Nine major categories were considered important after the interviews for effectively managing privacy and derived after analysing how many times a word repeated itself in the context of managing privacy. If more than 75 percent of the people repeated a particular term, then that term was considered important. A minority view had less than 25% repetition.

2.3 Conceptual Framework for an Effective Privacy Management

The interviewers identified trust and control of information is essential for effective management of privacy. However there was ambiguity in terms of what trust and control actually meant. Control is a simple choice of what information they intend to use to communicate with others, as discussed in (Altman 1977) view of privacy. Control meant several things - it was about the type of information or the nature of the information which was sensitive or perceived as sensitive, and also the way the flow of such information was managed through various elaborate privacy settings. There was certain amount of trust in the general public that they would view content that was published and would not misuse the photo or video in a way which would cause harm to the publisher in anyway. There was however a certain amount of variance because once the photo or video was uploaded then the publisher had limited ways to control what people would do with it. So there was some amount of forced trust as there was no alternative but to trust. Had they been given a choice to control the choices of what other people could do with their already published content, they would control it. So the implication of forced trust is the

lack of clarity around how the photos and videos would be stored and shared via social media applications. There are some short term software solutions which provide certain amount of control; however how far this was trusted by the user is not clear. For example, social media applications provide some control by offering various privacy settings.

Certain measures which generate trust in the long term could be implemented, such as who has viewed the content, thereby providing more information about how the content should be managed and what could happen that could compromise the content in the future after the initial publication. The general public's view is that a log of such activity when provided to the publisher of the content will generate certain negative privacy to the viewer because they lose anonymity, but positive privacy for the publisher of the content who is at more risk. There could be a provision which will allow the user to turn on or off who has seen the content. Privacy is very contextual and subjective. The lower level categories found are, trust in privacy settings provided by the software, how much of it was forced trust, what could be done if the application was agile to accommodate measures.

2.3.1 How to Identify Forced Trust and Manage Privacy Effectively?

The participants I interviewed had very diverse views about what is forced trust: the generalisation of forced trust meant it was subjective.

However an aggregation of the data concludes that inhibitions about why people share information have direct implications to privacy, such as their apprehension about how it will be managed post-processing. Forced trust is applied when the user has no option to not share his or her information. Participants were more afraid that their information may not only be misused but be downloaded and stored separately. The option for others to download information in photos and videos inhibited some of my participants from sharing their information. The interview data directly suggests that there should be a mechanism which will ask for consent from the publisher of the photo if someone wants to view or download that photo. The anonymity about who had seen the content was very worrying for many of my participants. There was also a suggestion that there should be certain discretion exercised in terms of allowing people to watch photos and videos. This option must be very clear.

The direct benefit many of my participants felt while sharing information on social media was that they believed it to be an effective way to communicate to a large group of people in real time; this was a major enabler for the popularity of social media. Trustworthiness is a complex mechanism to implement: when publishing information a certain amount of trust is necessary so that information can be shared with others. My participants believed that, although there were features on social media applications about who could view the content, many participants did not really trust the settings provided. They felt they were an untrustworthy way of implementing control over the flow of information. Trust and control are used to manage privacy. The control method is chiefly what IT applications use to control the flow of information. Trusting an application means that it has to generate certain confidence with the user that the information shared using the social media has no further consequences. As it has failed to do that, many of my participants do not trust the settings provided to manage privacy. Another thing my participants had a huge concern about was the real time availability of information in social media applications. Users don't have a chance to review their decisions about sharing information so the data will flow via photo or video freely, thereby having a direct impact on the privacy of the individual.

3 CONCLUSIONS

Managing privacy in photo and videos should not be an after thought after the sharing has occurred using social media. As privacy is a loosely defined it is very difficult to for see all the consequences before publishing content. However managing the content effectively will mitigate risks of privacy. Further research needs to be done to derive an over arching picture about privacy because as technology keeps moving forward, an equal emphasis needs to be given for privacy concerns of individuals. The conceptual framework discussed is a part of the proposed framework.

REFERENCES

Altman I 1977, 'Privacy regulation: culturally universal or culturally specific?', Journal of Social Issues 33 (3): 66–84.

Andrews, L. 2012, 'Facebook is using you', The New York Times, 4 February.

Bennett, C. and Raab, C. 2002, Governance of Privacy: Policy Instruments in Global Perspective, Barnes & Noble, London.

Creswell, J.W. 2003, Research Design: Qualitative, Quantitative and mixed methods approaches, Sage Publication, Thousand Oaks, California.

Charmaz, K. 2006, Constructing grounded theory. A practical guide through qualitative analysis, Sage Publication, London.

Chen, S. and Williams, M-A. 2009, ' Privacy in Social networks: A comparative study', PACIS, vol. 4, pp. 81.

Facebook 2011, Facebook principles, viewed 17 February 2014, <http://www.facebook.com/principles.php.>.

FC. K. 2010, 'The fundamental limits of privacy for social networks', MIT Technology Review Physics arXiv Blog, viewed 5 May 2010, <http://www.technologyreview.com/view/418819/the-fundamental-limits-of-privacy-for-social>.

Grey, D.E. 2009, 'Doing Research in the Real World', 2nd edn, Sage Publication, London.

Stratus, A. and Corbin, J. 1998, Basics of qualitative research, Sage Publication, Thousand Oaks, California.

Maykut, P. and Morehouse, R. 1994, Beginning Qualitative Research: A Philosophic and Practical Guide, The Farmer Press, London.

Warburton, W.I. 2005, 'What are grounded theories made of? 2005', LASS Faculty Post-Graduate Research conference University of Southhampton, UK, 6-7 June.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS