Seminar on Privacy in Ubiquitous Computing

Mehmed Mustafa
Institute of Computer Science
University of Göttingen
mehmed.mustafa@stud.uni-goettingen.de

Chris Warin
Institute of Computer Science
University of Göttingen
chris.warin@stud.uni-goettingen.de

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—privacy, bystander, privacy enhancing technology**

I. Introduction

Today's society is filled with technological devices that are capable of gathering data from people, such as smartphones, surveillance cameras, *Augmented Reality* (AR) devices or *Internet of Things* (IoT) devices [1]–[3]. Although these devices have been causing a number of concerns regarding the privacy of users, recent studies have shown that the privacy of bystanders (i.e. the individuals that are around users using these devices) is also often involved, as online-shared data often involves individuals other than the users sharing the data [4]. In other words, bystanders' personal information can be collected without their knowledge or consent [1].

A common real-life example could be a person taking a picture in a busy street, where the faces of bystanders are recognizable. The picture can later be posted on social media, and neither the posting or the taken picture have been made with the knowledge nor consent of the bystanders [2]. This example can easily be adapted with different mediums (i.e. pictures, videos, audio), and the collected data can be of different nature (i.e. face, voice, location). This high amount of devices capable of collecting data of different nature results in high pervasiveness in bystanders' privacy. This is a significantly harder problem to solve than regular user privacy, mainly because bystanders can be unaware that data involving them is shared in the first place [4].

In the past, several attempts with different approaches have been made in order to ensure the privacy of bystanders. Technological solutions exist: for protecting visual privacy, techniques such as Gaussian blur or pixelisation have been used in order to anonymize individuals—this is most commonly seen on TV [5]. However, with the framework they present in [5], Dufraux and Ebrahimi define Gaussian blur and pixelisation as naive methods to hide identity. Their results show high recognition rates (up to 56%) from the attacker (face recognition algorithms) on images that have been blurred or pixelised, even when privacy enhancing techniques are applied on the training set of images (recognition rate similar for Gaussian blur and up to 45% for pixelisation). On the online-sharing side, Olteanu, Huguenin, Dacosta and Hubaux [4] claim that few solutions exist for detecting and sharing interdependent data in a way that preserves privacy of interdependent users. They add that existing solutions are limited in efficiency, as they all assume that bystanders are aware of data including them being shared, and often disregard adversary models, such as the online service provider. On the legal side, simpler solutions have also been applied (e.g. forbidding the use of cameras, smartphones, or AR devices like Google Glass in certain places[2]). Still, all presented solutions have been proven either inefficient or insufficient [2], [4], [5].

Due to the inefficient past attempts to ensure bystanders' privacy, the issue remains to be solved. There can however not be a perfect solution, because of several critical aspects. First, individuals have different requirements in terms of privacy, and these requirements can change over their life [2]. According to Westin [6], they are categorized between privacy fundamentalists (i.e. distrustful regarding organizations requiring their data), pragmatics (i.e. deciding whether they want to obtain various services, opportunities, and more, in exchange of the potential pervasiveness caused by the organisation's information seeking), and unconcerned (i.e. trustful regarding organisations requiring their data). Although this categorization concerns the privacy requirements of individuals, the same can be applied when they become bystanders to the eye of others. In consequence, fundamentalists will seek solutions that will, for example, systematically anonymize them to ensure their privacy as bystanders. Pragmatists will decide whether they want to adopt a certain solution depending on certain aspects (e.g. the cost, how good the solution protects them, the usability of the solution) and with varying requirements in privacy (e.g. decide to not be anonymized to trusted users). Unconcerned will remain unaware of having their privacy compromised, or will not want to adopt a privacy enhancing solution because of the added complexity. This means that there cannot be one solution to fit everyone. Moreover, because bystanders can be unaware of being present in other individuals' data, most solutions require that they register themselves on the system to define their preferences. In other words, very few solutions can enhance the privacy of bystanders such that they don't need to care or take action about it.

Recent technologies for ensuring bystanders' privacy have had to adapt to these challenges. As a result, they are mostly based on user participation, meaning that users create a profile

on a server used by the technology, where they indicate their preferences in terms of privacy [2], [7]. This allows bystanders with any privacy requirements to be satisfied; the unconcerned bystanders are not required to register themselves. These technologies are centred about different aspects of privacy: the majority aim to provide visual privacy to bystanders (with again different approaches, e.g. privacy regarding drones, surveillance cameras, etc.), but some are centred on location privacy [8], or audio privacy [9].

The protection of bystanders' privacy is a concern that touches several domains, namely economical, social, legal, and technological [1]. We have defined our focus by first selecting a variety of papers that evoked, or treated the topic of bystanders' privacy. From this basis, we refined our selection based on technological solutions that enhance the privacy of bystanders, which led us to further literature. As a result, we present a number of technologies that ensure bystanders' privacy around one or more aspects (e.g. visual privacy, location privacy, etc.), along with their limitations.

This report focuses on the different technologies that address the pervasiveness in the privacy of bystanders. Section II lists different real-life examples of bystanders' privacy being compromised. Section III goes over different technologies that ensure different aspects of the privacy of bystanders. Section IV describes the current limitations and challenges that these technologies are facing, whether they are technological or not. Finally, section V concludes this report.

II. Bystanders' privacy pervasiveness

Give real-life examples and why they are problematic.

A. Videos and images

Surveillance cameras, smartphone photos/videos in the street capturing bystanders

B. Audio

Google Home / Amazon Alexa in a household: other members are also listened

C. Location

Pervasive location information in apps (e.g. French Stop-Covid app recenses more contacts' location information than announced)

D. Others

IoT, see example in 2.b

III. Technologies for ensuring the privacy of bystanders

A. PriSurv System

Video surveillance systems are necessary for a safe and secure community, which explains why they are widely deployed. However, high deployment rate of these systems in public places leads to privacy invasion of the objects being recorded. Solution of this problem is a challenging task because privacy and security should be balanced appropriately and when possible in real-time.

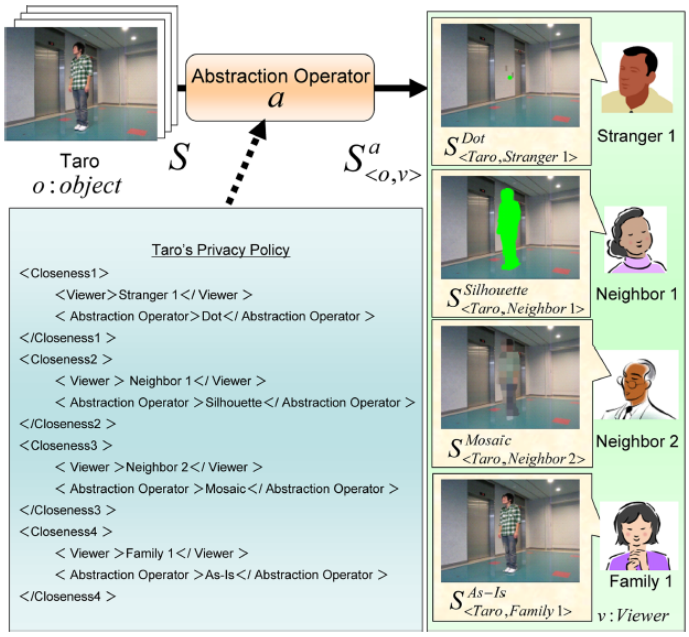

Figure 1. PriSurv simple run case [7].

There are several other studies on privacy based on video surveillance. Two studies proposed image processing methods in order to protect the privacy of objects [10],[11]. In other two studies the privacy protection of objects depends either on the authority of objects or observers [12],[13]. Privacy information can be embedded by using digital watermarking technology in such way that only predefined authorized viewers will have access to it [14]. However, these solutions are not flexible enough, because the sense of privacy of different objects is not considered. For example, object A may want their privacy to be protected from observer A, but not from observer B. Some objects may not want a privacy protection at all.

PriSurv system [7] can adaptively protect privacy of objects and disclose their visual information according to the privacy policies of the different objects. PriSurv is a video surveillance system, which is defined by visual abstraction and protects the privacy of objects appearing within a video depending who observes the video. Closeness between objects and observers determines the privacy policies to be used.

1) Simple run case: Figure 1 is an example run case of PriSurv, which shows how visual abstraction is used in order to protect the privacy of an object appearing within an image. Let o, a, v and S denote an object, an abstraction operator, a viewer and an original image, respectively. In the example, "Taro" is the object which appears within the original image and is monitored by "Stranger 1", "Neighbor 1", "Neighbor 2" and "Family 1" which are the different viewers. Since the closeness between the object and viewers is different, different abstraction operators are used for hiding the visual information of the object. In the example, these operators are "Dot", "Silhouette", "Mosaic" and "As-Is", which are 4 of the 12 possible operators. Each viewer then receives a privacy

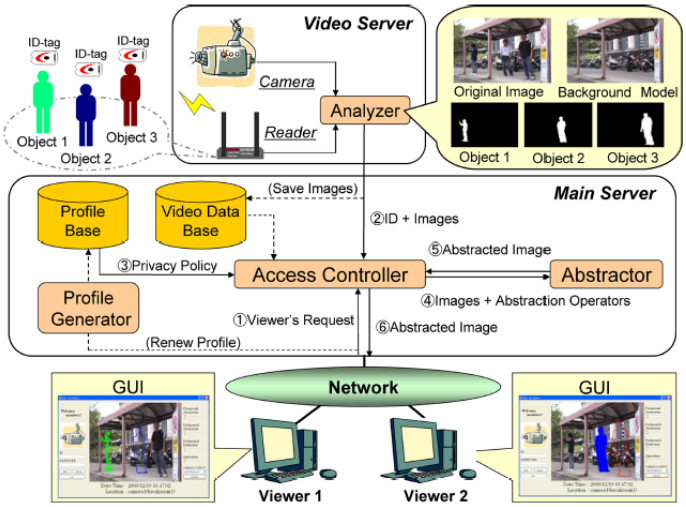

Figure 2. PriSurv system overview [7].

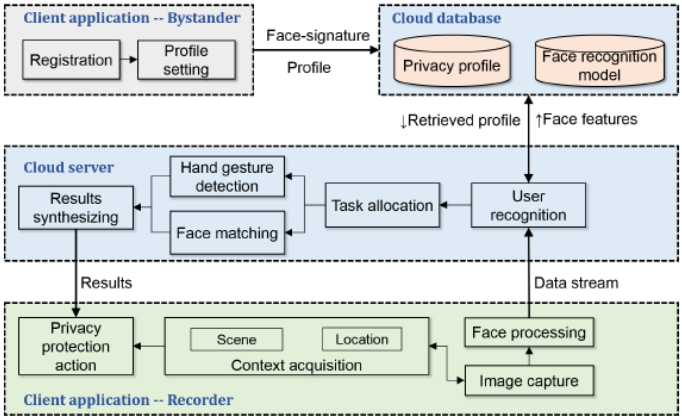

Figure 3. Cardea framework overview [2].

protected version of the original image which is denoted by $S^a_{<o,v>}$. A simplified version of Taro's privacy policy, which is a part of the abstraction operator, is also available to give a better understanding of how the closeness is defined.

2) System overview: Figure 2 shows the architecture of the PriSurv system. It consists of three main parts: Video Server, Main Server and Network. It also has six different components: Analyzer, Profile Generator, Profile Base, Access Controller, Abstractor and Video Data Base.

The Analyzer, which is a part of the video server, is responsible for identifying different objects. Each identifiable object must have its own *Radio-frequency identification* (RFID)-tag. The surveillance area is divided into smaller N x N areas and the location area of each RFID-tag is determined by an RFID-reader. Each object inside the original image is extracted and then identified separately by comparing the obtained visual data with the binary images of each object.

The Profile Generator is used for setting up privacy policies for different members of the system. Each member's personal information such as name, age, gender and address and privacy policy is stored securely inside the Profile Base. The Profile Generator is also responsible for converting data taken from the GUI to *Extensible Markup Language* (XML)-based syntax. The profile of each member can only be updated by them and other members have no access to this data.

The Access Controller determines the closeness relationship between a requesting viewer and an object to be monitored by reading the XML-based privacy policies of the object stored inside the Profile Base. Once the types of abstraction operators are extracted, Access Controller sends them to the Abstractor.

The Abstractor is a processor for images that performs visual abstraction by using abstraction operators.

The Video Data Base stores past video data and makes it available to viewers after appropriate visual abstractions are performed.

B. Sharing of Multi-Subject and Interdependent Data

Reference [4]

C. Cardea Framework

Reference [2]

D. Others - More specific Audio or Location based technologies should be found

IV. Limitations and Challenges of Privacy Ensuring Technologies

A. Cardea (user contribution)

Willingly putting your personal data on a cloud to avoid having your privacy invaded by others can be seen as counter productive

B. Example 2

C. Example 3

D. (optionally) Ideas that could fix these limitations

V. Conclusion

Table I
Table Type Styles

Table Head	Table Column Head		
	Table column subhead	*Subhead*	*Subhead*
copy	More table copy[a]		

[a]Sample of a Table footnote.

Abbreviations and Acronyms

IoT *Internet of Things*
AR *Augmented Reality*
RFID *Radio-frequency identification*
XML *Extensible Markup Language*

REFERENCES

[1] Y.-H. Lu, A. Cavallaro, C. Crump, G. Friedland, and K. Winstein, "Privacy protection in online multimedia," in *Proceedings of the 25th ACM international conference on Multimedia*, 2017, pp. 457–459.

[2] J. Shu, R. Zheng, and P. Hui, "Cardea: Context-aware visual privacy protection from pervasive cameras," *arXiv preprint arXiv:1610.00889*, 2016.

[3] T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 2377–2386.

[4] A.-M. Olteanu, K. Huguenin, I. Dacosta, and J.-P. Hubaux, "Consensual and privacy-preserving sharing of multi-subject and interdependent data," in *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2018, pp. 1–16.

[5] F. Dufaux and T. Ebrahimi, "A framework for the validation of privacy protection solutions in video surveillance," in *2010 IEEE International Conference on Multimedia and Expo*. IEEE, 2010, pp. 66–71.

[6] M. Langheinrich, "Privacy in ubiquitous computing," in *Ubiquitous Computing*. CRC Press Boca Raton, FL, 2009, pp. 95–160.

[7] N. Chinomi and B. Ito, "Prisurv: Privacy protected video surveillance system using adaptive visual abstraction," in *Advances in Multimedia Modeling*, 2008, pp. 144–154.

[8] S. Pidcock, R. Smits, U. Hengartner, and I. Goldberg, "Notisense: An urban sensing notification system to improve bystander privacy," in *Proc. 2nd Int'l Workshop Sensing Applications on Mobile Phones*, 2011, pp. 1–5.

[9] E. C. Larson, T. Lee, S. Liu, M. Rosenfeld, and S. N. Patel, "Accurate and privacy preserving cough sensing using a low-cost microphone," in *Proceedings of the 13th international conference on Ubiquitous computing*, 2011, pp. 375–384.

[10] A. Cavallaro, O. Steiger, and T. Ebrahimi, "Semantic video analysis for adaptive content delivery and automatic description," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 15, pp. 1200–1209, 11 2005.

[11] I. Kitahara, K. Kogure, and N. Hagita, "Stealth vision for protecting privacy," vol. 4, 09 2004, pp. 404–407 Vol.4.

[12] J. Wickramasuriya, M. Alhazzazi, M. Datt, S. Mehrotra, and N. Venkatasubramanian, *Privacy-protecting video surveillance*, 02 2005.

[13] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. Li, A. Ekin, J. Connell, C.-F. Shu, and M. Lu, "Enabling video privacy through computer vision," *Security & Privacy, IEEE*, vol. 3, pp. 50–57, 06 2005.

[14] W. Zhang, S.-c. Cheung, and M. Chen, "Hiding privacy information in video surveillance system," 01 2005, pp. 868–871.