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 [1], surveillance cameras [2], *Augmented Reality* (AR) devices [3] or *Internet of Things* (IoT) devices [1]. Although these devices been causing a number of concerns regarding the privacy of users, another topic—that is less publicly discussed, but as important—is the privacy of bystanders, i.e. the people that are around users using these devices, and of which personal information can be collected without their knowledge or consent. 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 is taken without their knowledge nor consent, and can later be posted on social media. The data that are collected from bystanders can come from different mediums (i.e. pictures, videos, audio), and can be of different nature (i.e. face, voice, location). This results in pervasiveness in bystanders' privacy and touches several domains, namely economical, social, legal, and technological. 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 StopCovid 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 Framework

Reference [4]

B. Sharing of Multi-Subject and Interdependent Data

Reference [5]

C. Cardea Framework

Reference [3]

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

References

Please number citations consecutively within brackets [3]. The sentence punctuation follows the bracket [6]. Refer simply to the reference number, as in [2]—do not use "Ref. [2]" or "reference [2]" except at the beginning of a sentence: "Reference [1] was the first ..."

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.

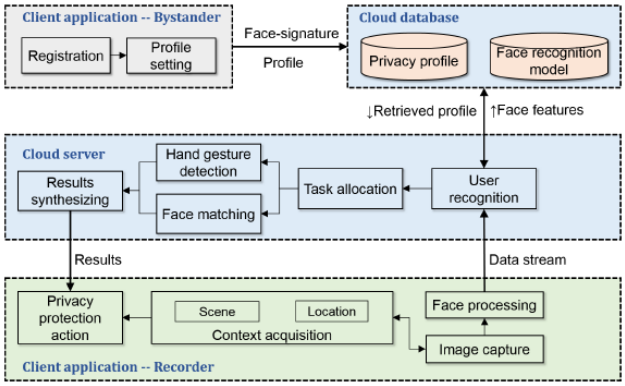

Figure 1. Cardea framework overview.

Number footnotes separately in superscripts.[4] Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [1]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.[7]

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [5].

ABBREVIATIONS AND ACRONYMS

IoT *Internet of Things*
AR *Augmented Reality*

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*, pp. 457–459, 2017.

[2] 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*, pp. 2377–2386, 2014.

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

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

[5] 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)*, pp. 1–16, Internet Society, 2018.

[6] 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*, pp. 66–71, IEEE, 2010.

[7] S. Aditya and O. Druschel, "I-pic: A platform for privacy-compliant image capture," 2016.