GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Institute of Computer Science

MEHMED MUSTAFA, CHRIS WARIN

The Protection of Bystanders‘ Privacy

Seminar on Privacy in Ubiquitous Computing

Summary

- Introduction
- The pervasiveness in bystanders' privacy
- Past attempts at solutions
- Technologies for ensuring bystanders' privacy
- Limitations and Challenges
- Conclusion

Bystanders' privacy motivation

- People appearing in content recorded by someone or something else
  - E.g. an individual taking a photo in a busy street
  - Surveillance cameras in streets
  - Etc.

- Privacy of bystanders is an important topic
  - Millions of cameras, sensors, ubiquitous devices
  - A lot of content is shared without consent or even knowledge
  - Big ethical issues, e.g. revenge pornography [2]

Sources: https://www.pxfuel.com/en/free-photo-xsvjj
https://www.pxfuel.com/en/free-photo-jriym

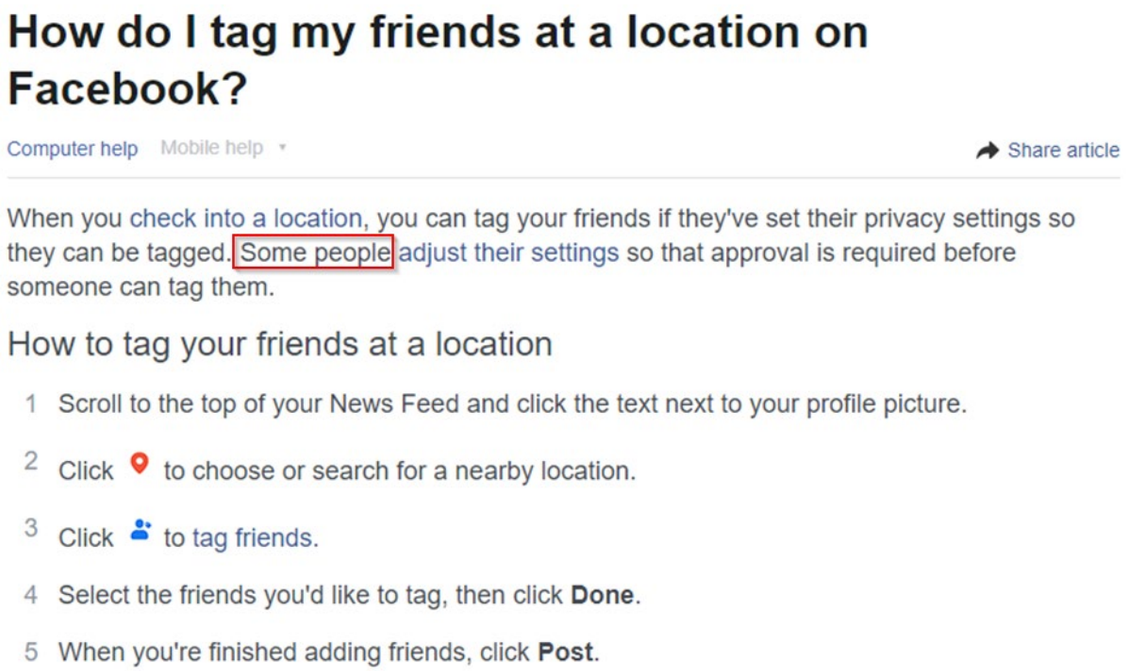
The pervasiveness in bystanders' privacy

- Visual privacy
  - Smartphones [1]
  - Surveillance cameras
    - Street [3]
    - IoT smart-homes [5]
  - Drones [4]
  - AR devices [8]

Sources: https://pxhere.com/en/photo/955462
https://commons.wikimedia.org/wiki/File:Wikimania_2014_attendee_with_google_glass_6733.jpg
https://pixy.org/373228/
https://ergoaudio.com/residential/2928/Surveillance

The pervasiveness in bystanders' privacy (2)

- Audio privacy
  - IoT voice assistants (e.g. Alexa) [6]
  - Healthcare devices [7]
- Location privacy
  - Online sharing of co-locations [2]



How do I tag my friends at a location on Facebook?

Computer help Mobile help Share article

When you check into a location, you can tag your friends if they've set their privacy settings so they can be tagged. Some people adjust their settings so that approval is required before someone can tag them.

How to tag your friends at a location

1. Scroll to the top of your News Feed and click the text next to your profile picture.
2. Click to choose or search for a nearby location.
3. Click to tag friends.
4. Select the friends you'd like to tag, then click **Done**.
5. When you're finished adding friends, click **Post**.

Sources: https://www.pikist.com/free-photo-sicea
https://www.facebook.com/help/201009576609790/

Past attempts at solutions

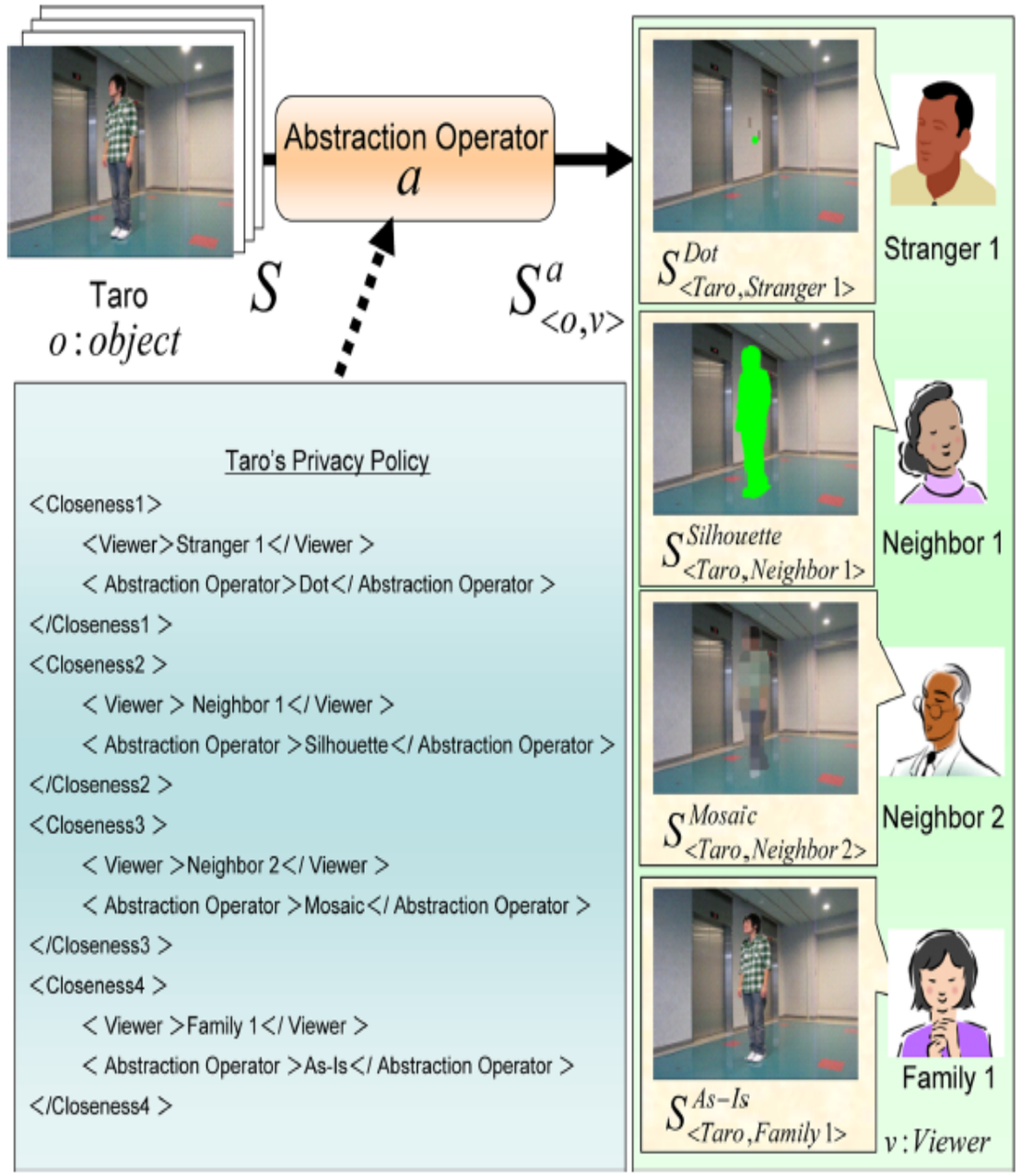
- Protection upon data collection
  - Mainly visual privacy
  - Obfuscation of bystanders depending on who watches [3]
  - Obfuscation of bystanders that wear detectable features
    - Colourful hats, QR codes [1]
- Protection upon sharing of interdependent data [2]
  - Few solutions, limited, e.g. assumption that bystanders are aware
- Legal domain
  - Prohibition of devices in certain places, e.g. Google Glass [1]

Technologies for ensuring bystanders' privacy

- PriSurv System [3]
- Cardea Framework [1]
- ConsenShare Framework [2]

PriSurv System [3]

- Usage: Surveillance cameras
- Perfect for small public areas
- Users can define different privacy policy for different viewer groups
- Supports several visual information hiding methods
- Relies on RFID technology for visual detection



Cardea Framework [1]

- Usage: any smart device with a camera and internet connection
- Context awareness
- Supports 2 hand gestures for changing privacy dynamically
- Supports blurring as a hiding method
- Uses computer vision techniques

  for visual detection

ConsenShare Framework [2]

- Usage: Online Social Networks
- Separation between Content and Identity Management
- Users can approve/reject content before their identity is shared
- Background faces are blurred by default
- The framework could be extended for audio, video and co-location.

(a) Original photo (b) Background image (c) Face images (d) Final photo

Limitations and Challenges [1 – 3]

- Users have to give out and store their data (visual etc.) online
- Face detection could still produce wrong results
- Proposed solutions are centralized (P2P solution could help?)
- Privacy of non-registered individuals is not taken into consideration
- Usage of the proposed technologies is non-compulsory

Conclusion

- Challenges are still very present
  - Flexible solutions are needed…
  - … But that also requires user participation [8]
- PETs for bystanders are getting more popular [1, 2]
  - But still only in research
  - Bystanders' privacy is still not actively protected in everyday life
- Utility of these tools will remain limited unless made mandatory
  - Protection can only work if everybody uses the tools
  - This could be the case in a few years [2]

Thanks for your attention!

Do you have any questions?

References

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

[2] 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)*, 2018, pp. 1–16.

[3] N. Chinomi and B. Ito, 'PriSurv: Privacy Protected Video Surveillance System Using Adaptive Visual Abstraction', in *Advances in Multimedia Modeling*, 2008, pp. 144–154.

[4] Y. Yao, H. Xia, Y. Huang, and Y. Wang, 'Privacy mechanisms for drones: Perceptions of drone controllers and bystanders', in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 6777–6788.

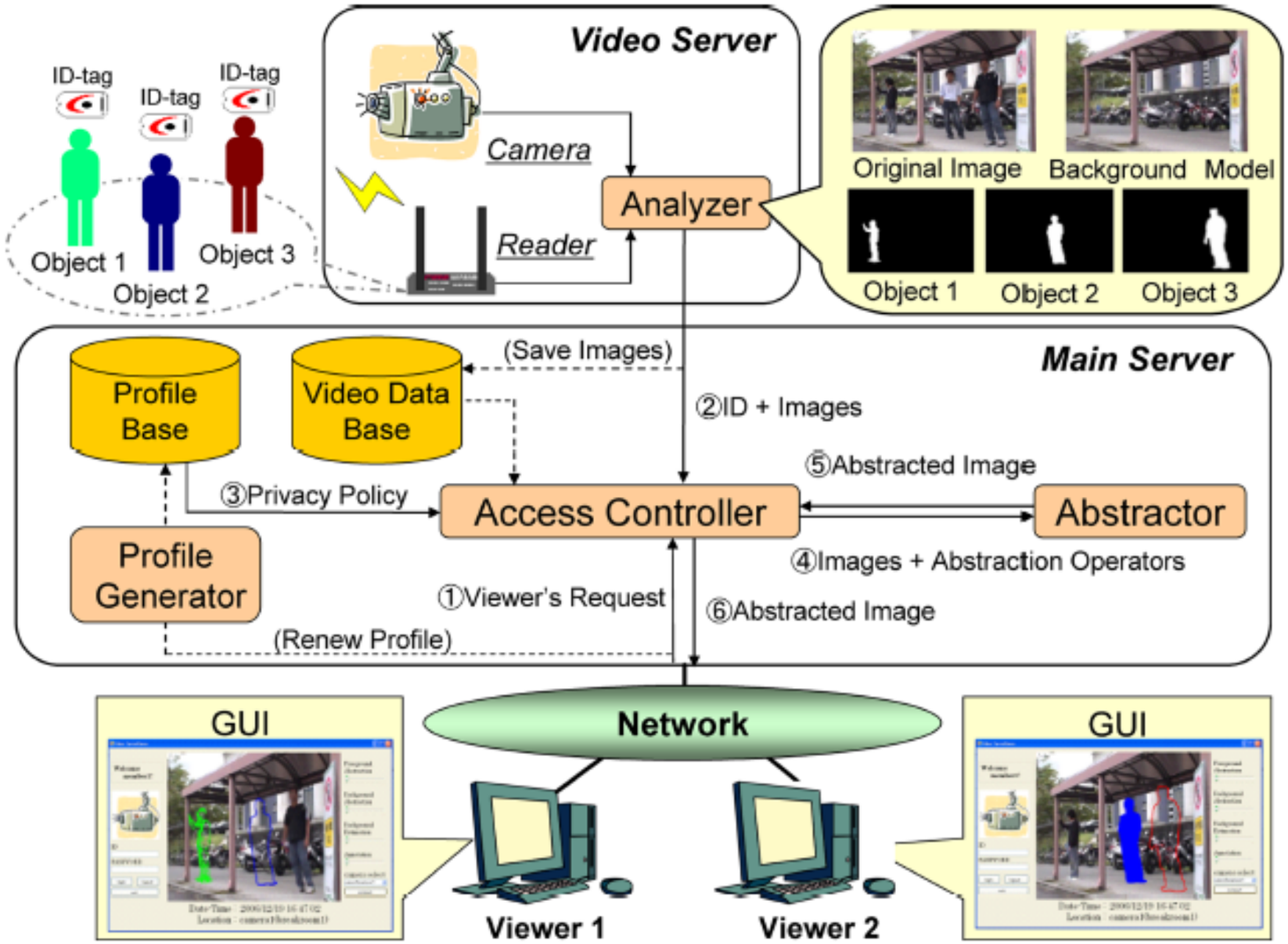
[5] J. Bernd, R. Abu-Salma, and A. Frik, 'Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance', 2020.

[6] Npr, 'Amazon Customer Receives 1,700 Audio Files Of A Stranger Who Used Alexa', 2018. https://www.npr.org/2018/12/20/678631013/amazon-customer-receives-1-700-audio-files-of-a-stranger-who-used-alexa (accessed Sep. 03, 2020).

[7] Larson, Eric C, TienJui Lee, Sean Liu, Margaret Rosenfeld, and Shwetak N Patel. 'Accurate and Privacy Preserving Cough Sensing Using a Low-Cost Microphone'. In *Proceedings of the 13th International Conference on Ubiquitous Computing*, 375–384, 2011.

[8] Denning, Tamara, Zakariya Dehlawi, and Tadayoshi 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*, 2377–2386, 2014.

Extra: PriSurv System Architecture



Extra: Cardea Framework Overview