Understanding and Recognizing Bystanders in Images for Privacy Protection

Rakibul Hasan[1], David Crandall[1], Mario Fritz[2], and Apu Kapadia[1]

[1]Indiana University, Bloomington, IN, USA
{rakhasan,djcran,kapadia}@indiana.edu
[2]CISPA Helmholtz Center for Information Security, Saarland, Germany
fritz@cispa.saarland

Privacy violations of *bystanders* in photographs taken in public places is a long-studied problem. Proposed solutions rely on bystanders to be proactive and use tools and techniques to protect their privacy [1–9]. These tools require them to share sensitive information, such as location, facial features, and privacy preferences with other users and cloud servers, which are themselves violations of privacy. Here, we attempt to detect *bystanders* in images automatically using computer vision and machine learning. Upon detection, any privacy-preserving action could be taken (e.g., obfuscation), enforcing a privacy-by-default policy without placing the burden on the bystanders or sharing any sensitive information.

We begin by understanding what *rationales* and *concepts* humans use to distinguish between *subject* and *bystander* in images, since these concepts are nuanced and context-specific. In a study, we asked participants to label people in images as bystanders or subjects, provide justification for their labels, and rate each person for (presumably) relevant concepts, e.g., whether the person was posing for and comfortable being in the image, can be replaced by another random person and so on. Our correlation and regression analyses revealed significant association among these features and the most common reasons humans use to classify *subject/bystander*. Using factor analysis, we identified two underlying constructs humans use to identify bystanders: *visual-appearance* and *importance of the person for the image*. We experimented with several classification models for automatic detection. The best performing model (mean accuracy 85% for 10-fold cross-validation) is a two-step prediction pipeline based on our hypothesis on how humans do it. First, we predict the relevant concepts using features extracted from the images (such as body-pose [10], facial expression [11], and the location of a person) using regression models. These *predicted* values were then used to classify *subject/bystander*. Detailed study methodology and (additional) findings are presented in the poster.

References

1. Bo, C., Shen, G., Liu, J., Li, X.-Y., Zhang, Y., Zhao, F. (2014). Privacy.Tag: Privacy Concern Expressed and Respected. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems (pp. 163176). New York, NY, USA: ACM. https://doi.org/10.1145/2668332.2668339

2. Aditya, P., Sen, R., Druschel, P., Joon Oh, S., Benenson, R., Fritz, M., Wu, T. T. (2016). I-Pic: A Platform for Privacy-Compliant Image Capture. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (pp. 235248). New York, NY, USA: ACM. https://doi.org/10.1145/2906388.2906412
3. Shu, J., Zheng, R., Hui, P. (2016). Cardea: Context-aware visual privacy protection from pervasive cameras. ArXiv Preprint ArXiv:1610.00889.
4. Li, A., Darling, D., Li, Q. (2018). PhotoSafer: Content-Based and Context-Aware Private Photo Protection for Smartphones. In 2018 IEEE Symposium on Privacy-Aware Computing (PAC) (pp. 1018). https://doi.org/10.1109/PAC.2018.00008
5. Li, A., Li, Q., Gao, W. (2016). PrivacyCamera: Cooperative Privacy-Aware Photographing with Mobile Phones. In 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 19). https://doi.org/10.1109/SAHCN.2016.7733008
6. Zhang, L., Liu, K., Li, X.-Y., Liu, C., Ding, X., Liu, Y. (2016). Privacy-friendly Photo Capturing and Sharing System. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 524534). New York, NY, USA: ACM. https://doi.org/10.1145/2971648.2971662
7. Steil, J., Koelle, M., Heuten, W., Boll, S., Bulling, A. (2018). PrivacEye: Privacy-Preserving First-Person Vision Using Image Features and Eye Movement Analysis. ArXiv Preprint ArXiv:1801.04457.
8. Perez, A., Zeadally, S., Matos Garcia, L., Mouloud, J., Griffith, S. (2018). FacePET: Enhancing Bystanders Facial Privacy with Smart Wearables/Internet of Things. Electronics, 7(12), 379.
9. Henne, B., Szongott, C., Smith, M. (2013). SnapMe if You Can: Privacy Threats of Other Peoples Geo-tagged Media and What We Can Do About It. In Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks (pp. 95106). New York, NY, USA: ACM. https://doi.org/10.1145/2462096.2462113
10. Cao, Z., Hidalgo, G., Simon, T., Wei, S.-E., Sheikh, Y. (2018). OpenPose: real-time multi-person 2D pose estimation using Part Affinity Fields. ArXiv Preprint ArXiv:1812.08008.
11. Li, S., Deng, W., Du, J. (2017). Reliable Crowdsourcing and Deep Locality-Preserving Learning for Expression Recognition in the Wild. In 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 25842593).