Paper Details

Author details:

Anupam Das Email: Phone: (Institute for Software Research Affiliation: Carnegie Mellon University	Martin Degeling Email: Phone: (Institute for Software Research Affiliation: Carnegie Mellon University	Xiaoyou Wang Email: x Phone: Institute for Software Research Affiliation: Carnegie Mellon University
Junjue Wang Email: j Phone: Affiliation: Carnegie Mellon University	Norman Sadeh Email: Phone: Institute for Software Research Affiliation: Carnegie Mellon University	Mahadev Satyanarayanan Email: s Phone: Affiliation: Carnegie Mellon University

Title: Assisting Users in a World Full of Cameras: A Privacy-aware Infrastructure for Computer Vision Applications

Abstract: Computer vision based technologies have seen widespread adoption over the recent years. This trend is not limited to the rapid adoption of facial recognition technology [1] but extends to facial expression recognition, scene recognition and more. These technologies pose an increasing threat to privacy. Facial recognition can be used to not only identify individuals and track their whereabouts, but can also be used to infer information about their social activities such as with whom and where they hang out. Facial expression recognition can be used to infer their psychological state such as whether they look depressed, tired or sick. When combined with auxiliary data (e.g., lifestyle and behavioral data), these technologies can help infer a great deal of information about many facets of people's lives. Privacy advocates criticize the silent nature of facial recognition technology due to its lack of transparency of how video streams captured by cameras, at times concealed, are used. One of the fundamental principles associated with information privacy is the right to 'Notice' and 'Choice'. However, current applications of facial recognition technology lack effective mechanisms for informing users of not only the presence of cameras but also the collection, usage, share and retention of sensitive data. In addition, a number of real-world practices would ideally be required to provide choice options to users under certain regulatory bodies. However, things only get worse as existing regulations on using facial recognition technology often fall short on recognizing the threats it poses. For example, in the U.S., no federal privacy law explicitly regulates *commercial* uses of facial recognition technology, and existing laws (the only exceptions being the privacy laws of Illinois and Texas state) do not fully address the key privacy concerns that stakeholders have raised [2].

Several stakeholders including government agencies, industry trade organizations, and privacy advocacy organizations have proposed guidelines or best practices in using facial recognition technology commercially. Almost all of these guidelines include the practice of explicitly notifying individuals when facial recognition is being used and obtaining affirmative consent before using facial recognition to identify an individual. However, no

such tools exist that inform users about what data is collected and what choices they have with respect to how the data is used.

With this gap in mind we propose a novel privacy-aware infrastructure that not only notifies users of the existence of cameras nearby but also potentially enables them to opt in or out of facial recognition systems. Our approach focuses on those use cases where the use of facial recognition is optional, providing benefits to those deploying it as well as those being monitored. For such scenarios we improve the transparency of the systems and offer ways for users to control what data is collected about them (e.g., enabling users to obfuscate their faces on live video feed). We have developed a mobile application which in combination with a web registry notifies users of the existence of facial recognition based services nearby. The application displays summary information relevant to data collection, comparable to what is disclosed in privacy policies including description of purpose as well as information about retention time and data sharing practice. We hope this will lead to better transparency and higher acceptance of facial recognition based technologies. Our proposed infrastructure is applicable to a wide range of Internet-of-Things (IoT) scenarios that involve notifying users of nearby IoT sensors. As part of a research project we are currently working on automating many aspects of the infrastructure to make it more user friendly.

References:

[1] Facial recognition market expected to reach $9.6B by 2022, 2016.
https://www.digitalsignagetoday.com/news/facialrecognitionmarketexpectedtoreach96bby2022/.
[2] U.S. Government Accountability Office. Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law, 2015. http://www.gao.gov/assets/680/671764.pdf

Publication details:

A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan. Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications. In Proceedings of the 30th IEEE Computer Vision and Pattern Recognition Workshops (CVPRW), pages 1387–1396, 2017
(http://ieeexplore.ieee.org/document/8014915/)