Maria S. Cross and Andrea Cavallaro

# Privacy as a Feature for Body-Worn Cameras

Body-worn cameras (BWCs) are becoming increasingly prevalent within today's society. These devices are now commonly seen on supermarket assistants, shopping center security guards, and public transport staff. Schools are also trialling BWCs on teachers to monitor students' behavior [1]. The use of BWCs is believed to promote the transparency and accountability of behaviors as well as the security of the wearer [2], [3]. With an expected shipment of more than 5 million units in the next year [4] and a compounded annual growth rate of 16% in the next five years [5], BWCs will become a permanent feature within everyday life. Such an uptake of BWCs marks a transition from purposive to passive data collection.

In this article, we discuss the threat to privacy that this passive data collection creates, along with opportunities to mitigate this risk. Furthermore, we argue that the use case of BWCs at work will stimulate the development of solutions that prevent the collection of data that could infringe upon the privacy of the wearer. Finally, we discuss the desirable properties of privacy-enhancing technologies (PETs) for BWCs.

BWCs record large quantities of audio-visual and inertial data that, instead of collecting only select, primary information that is relevant to the intended use, also capture secondary information that is irrelevant for the intended purpose [6]. The recording of an interaction with an aggressive customer is an example of primary information, whereas the identity of other customers waiting to be served is an example of secondary information. Collecting secondary information, which may be personally identifiable information (i.e., information relating to an identified or identifiable natural person), goes against the principle of data minimization prescribed in data-protection regulations [7].

Primary and secondary information captured by BWCs can be used to comprehensively describe the behaviors of the wearer. Such a description may be employed to profile wearers through their physical characteristics [8], [9], their activities [10], the foods they eat [11], and how they interact with others [12]. Each additional day of BWC usage marks the collation of more information, also enabling the inference of insights that are not directly observable. Examples of such insights are how active the wearers are, what motivates them, and their psychological profiles. In detailing the condition of the wearer, these profiles are, in practice, also becoming health records, with potentially greater levels of detail than obtained through clinical interaction.

The exploitation of profiles derived from users' online behaviors has already led to public controversies [13], [14]. This is due, in part, to the asymmetric power relation between users and providers who shift the responsibility of privacy choices to users through lengthy and complex privacy notices. These notices are often written more to protect the provider than to inform users, whose consent should be a "freely given, specific, informed and unambiguous indication of the data subject's wishes" [7].

The situation changes when BWCs are used by employees (e.g., shop assistants or security staff) because the dependence of the wearer upon the organizations collating their data (i.e., their employer) invalidates any consent processes, as the consent cannot be assumed to be "freely given" [7]. It is, therefore, the responsibility of the employer to protect the privacy of employees wearing BWCs and to safeguard BWC data (and any information therein) through a duty of confidentiality.

Maintaining confidentiality becomes more challenging when the data are accessed by an external company. As each individual wearer generates large volumes of data, employers (i.e., data controllers [7]) must seek ways to store and manage the BWC data produced. These solutions and their operation are often beyond the capabilities of the organizations adopting the technology, encouraging the outsourcing of the handling and curation of BWC data. This new landscape creates an urgent need for BWC solutions that offer privacy as a feature and enable employers to govern access to their employees' private, secondary information.

PETs aim to minimize access to data representing personal, secondary

*(continued on page 145)*

*Digital Object Identifier 10.1109/MSP.2020.2989686*
*Date of current version: 26 June 2020*

 *(continued from page 148)*

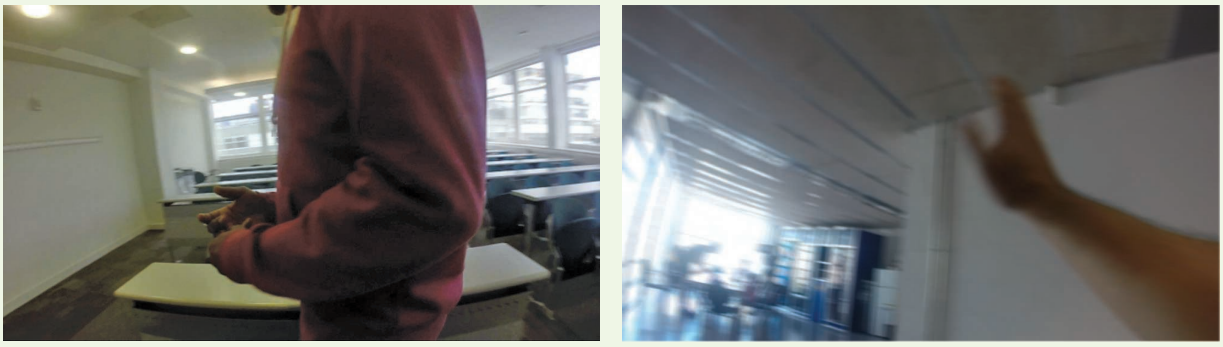



**FIGURE 1.** The challenges of BWC video data include (a) poor framing and (b) low visual quality due, for example, to motion blur or overexposure. (Used with permission from [24] and [25].)

information without compromising subsequent services that use the data. PETs may be applied once the data are transferred to a content management system or may be integrated within BWCs and transform the data in the device itself, prior to their transfer.

BWCs capture time-varying information in audio, inertial measurements and video data, all of which are difficult to protect using standard privacy-preserving approaches, such as differentially private protocols [15]. PETs designed for BWCs should be protective, reliable, and operative (these properties are a selected subset from those listed in [16] and have been adapted to be specific to BWCs). A PET is protective if it safeguards private, secondary information that is not necessary for the service, reliable if it does not affect the service and maintains performance, and operative if it integrates easily with existing work practices and its functions are explainable.

The design of PETs also requires the identification of who or what the private information should be protected from: individuals observing the data or algorithms extracting sensitive information. Although protection from individuals can be implemented using standard access control procedures, the protection from algorithms is a recent and growing challenge.

Algorithmic inferences on audio data can reveal a wide range of potentially private information, such as one's height and weight [17], emotional state [18], [19], and health conditions [19]. Motion sensor data collected by inertial measurement units can also reveal information about an individual's physical characteristics, such as height and weight [20], level of activity [21], and changes in behavioral patterns [22]. These data may be protected with PETs developed for other types of devices and that use transformations of the data [23]. Protecting BWC video data is, however, more challenging.

To preserve the privacy of bystanders captured in BWC videos, PETs designed for traditional stationary cameras could be adopted, but additional steps are required to ensure that the privacy-preserving methods remain effective. In fact, the unique challenges associated with BWC videos [24], such as motion blur and poorly framed content (Figure 1), hinder the direct application of PETs designed for stationary cameras. Also, to preserve the privacy of the wearer, new solutions are needed for video data. This is a distinct challenge in BWCs, as they capture a unique first-person viewpoint [25], which may include the wearer handling medications or close-ups of smartphone screens (Figure 2). Furthermore, BWCs indirectly disclose the activities of the wearer, which are captured through the motion of the camera itself [26]. Such motion information is difficult to disentangle from the primary visual information needed for the intended use of the video data, making the design of obfuscation or data-minimization techniques that prevent the collection of this secondary information an important research opportunity.

In conclusion, the increasing adoption of BWCs presents the research community with several new challenges associated with the development of PETs that are specific to the unique type of first-person data collected by BWCs. These PETs should not only operate on each modality (vision, sound, and inertial) independently, but also across modalities, as cross-modal correlations heighten the threat to privacy [27].

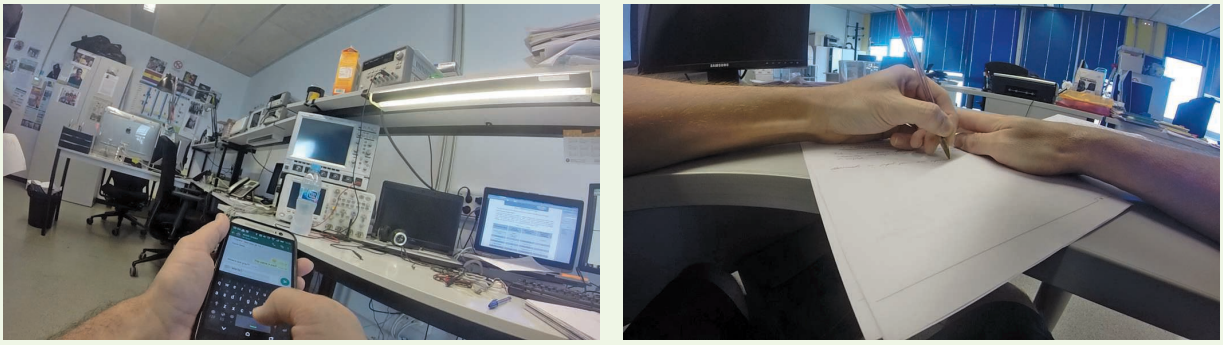
## Acknowledgments

We wish to thank the Alan Turing Institute (EP/N510129/1), which is funded by the U.K. Engineering and Physical Sciences Research Council, for its support throughout the project Privacy-Preserving Multimodal Learning for Activity Recognition (PRIMULA).

## Authors

***Maria S. Cross*** (m.s.cross@se18.qmul.ac.uk) received her M.Sc. degree in artificial intelligence from Queen Mary University of London (QMUL), United Kingdom, and her Ph.D. degree in health informatics from the University College London, United Kingdom. She is currently a postdoctoral research assistant at the Centre for Intelligent Sensing, QMUL.

***Andrea Cavallaro*** (a.cavallaro@qmul.ac.uk) is a professor of multimedia signal processing at Queen Mary University of London (QMUL), United Kingdom, and a



(a) (b)

**FIGURE 2.** The unique first-person viewpoint captured by BWCs may include (a) smartphone screens and (b) personal documents. (Used with permission from [25].)

Turing fellow with the Alan Turing Institute, the U.K. National Institute for Data Science and Artificial Intelligence. He is a fellow of the International Association for Pattern Recognition; director of the QMUL Centre for Intelligent Sensing; editor-in-chief of *Signal Processing: Image Communication*; senior area editor for *IEEE Transactions on Image Processing*; chair of the IEEE Image, Video, and Multidimensional Signal Processing Technical Committee; and an IEEE Signal Processing Society Distinguished Lecturer.

## References


[1] R. Adams, "Schools trial body cameras to aid safety and monitor behaviour," *The Guardian*, Feb. 7, 2020. Accessed on: Apr. 2, 2020. [Online]. Available: www.theguardian.com/education/2020/feb/07/schools-trial-body-cameras-to-aid-safety-and-monitor-behaviour

[2] C. Lum, M. Stoltz, C. S. Koper, and J. A. Scherer, "Research on body-worn cameras: What we know, what we need to know," *Criminol. Public Policy*, vol. 18, no. 1, pp. 93–118, 2019. doi: 10.1111/1745-9133.12412.

[3] B. Ariel, M. Newton, L. McEwan, G. A. Ashbridge, C. Weinborn, and H. Sabo Brants, "Reducing assaults against staff using body-worn cameras (BWCs) in railway stations," *Crim. Justice Rev.*, vol. 44, no. 1, pp. 76–93, 2019. doi: 10.1177/0734016818814889.

[4] "Gartner says worldwide wearable device sales to grow 17 percent in 2017," Gartner, Stamford, CT, Aug. 24, 2017. Accessed on: Apr. 6, 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-08-24-gartner-says-worldwide-wearable-device-sales-to-grow-17-percent-in-2017

[5] "Wearable and body-worn cameras market: Growth, trends and forecast (2020–2025)," Mordor Intelligence, Hyderabad, India, 2019. Accessed on: Apr. 2, 2020. [Online]. Available: https://www.mordorintelligence.com/industry-reports/wearable-and-body-worn-cameras-market

[6] T. Nortcliffe, "Safeguarding body worn video data," Home Office, London, Rep. no. 011/18, Oct. 2018.

[7] Council of the European Union (EU), European Parliament. (2016, Apr. 27). 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ 2016 L 119/1, Article 4. Accessed on: May 3, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[8] J. Finocchiaro, A. U. Khan, and A. Borji, "Egocentric height estimation," in *Proc. IEEE Winter Conf. Applications of Computer Vision (WACV)*, Santa Rosa, CA, Mar. 2017, pp. 1142–1150. doi: 10.1109/WACV.2017.132.

[9] M. Nouredanesh, A.W. Li, A. Godfrey, J. Hoey, and J. Tung, "Chasing feet in the wild: A proposed egocentric motion-aware gait assessment tool," in *Proc. European Conf. Computer Vision (ECCV)*, Munich, Sept. 2018, pp. 176–192. doi: 10.1007/978-3-030-11024-6_12.

[10] H. Pirsiavash, and D. Ramanan, "Detecting activities of daily living in first-person camera views," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Providence, RI, June 2012, pp. 2847–2854. doi: 10.1109/CVPR.2012.6248010.

[11] D. Damen, H. Doughty, G. M. Farinella, S. Fidler, A. Furnari, E. Kazakos, D. Moltisanti, J. Munro et al., "Scaling egocentric vision: The epic-kitchens dataset," in *Proc. European Conf. Computer Vision (ECCV)*, Munich, Sept. 2018, pp. 720–736.

[12] A. Fathi, J. K. Hodgins, and J. M. Rehg, "Social interactions: A first-person perspective," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, Providence, RI, June 2012, pp. 1226–1233. doi: 10.1109/CVPR.2012.6247805.

[13] C. Cadwalladr, "The great British Brexit robbery: How our democracy was hijacked," *The Guardian*, May 7, 2017. Accessed on: Apr. 6, 2020. [Online]. Available: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked- democracy

[14] A. Kofman and A. Tobin, "Facebook ads can still discriminate against women and older workers, despite a civil rights settlement," ProPublica, New York, Dec. 13, 2019. Accessed on: Apr. 6, 2020. [Online]. Available: https://www.propublica.org/article/facebook-ads-can-still-discriminate-against-women-and-older-workers-despite-a-civil-rights-settlement

[15] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Annu. Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, St. Petersburg, Russia, May–June 2006, pp. 486–503. doi: 10.1007/11761679_29.

[16] M. Hansen, J. H. Hoepman, M. Jensen, and S. Schiffner. "Readiness analysis for the adoption and evolution of privacy enhancing technologies: Methodology, pilot assessment, and continuity plan," European Union Agency for Network and Information Security (ENISA), Heraklion, Greece, Mar. 2016. Accessed on: May 3, 2020. [Online]. Available: https://www.enisa.europa.eu/publications/pets

[17] R. M. Krauss, R. Freyberg, and E. Morsella, "Inferring speakers' physical attributes from their voices," *J. Experimental Soc. Psychol.*, vol. 38, no. 6, pp. 618–625, 2002. doi: 10.1016/S0022-1031(02)00510-3.

[18] G. Trigeorgis, F. Ringeval, R. Brueckner, E. Marchi, M. A. Nicolaou, B. Schuller, and S. Zafeiriou, "Adieu features? End-to-end speech emotion recognition using a deep convolutional recurrent network," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, Shanghai, China, Mar. 2016, pp. 5200–5204. doi: 10.1109/ICASSP.2016.7472669.

[19] B. Schuller, S. Steidl, A. Batliner, A. Vinciarelli, K. Scherer, F. Ringeval, M. Chetouani, F. Weninger et al., "The INTERSPEECH 2013 computational paralinguistics challenge: Social signals, conflict, emotion, autism," in *Proc. INTERSPEECH*, Lyon, France, Aug. 2013, pp. 148–152.

[20] A. Masuda and T. Maekawa, "Estimating physical characteristics with body-worn accelerometers based on activity similarities," *J. Inform. Process.*, vol. 24, no. 2, pp. 237–246, 2016. doi: 10.2197/ipsjjip.24.237.

[21] M. N. S. Zainudin, M. N. Sulaiman, N. Mustapha, and T. Perumal, "Monitoring daily fitness activity using accelerometer sensor fusion," in *Proc. IEEE Int. Symp. Consumer Electronics (ISCE)*, Kuala Lumpur, Malaysia, Nov. 2017, pp. 35–36. doi: 10.1109/ISCE.2017.8355540.

[22] A. Gruenerbl, V. Osmani, G. Bahle, J. C. Carrasco, S. Oehler, O. Mayora, C. Haring, and P. Lukowicz, "Using smartphone mobility traces for the diagnosis of depressive and manic episodes in bipolar patients," in *Proc. Augmented Human Int. Conf.*, Kobe, Japan, Mar. 2014, pp. 1–8. doi: 10.1145/2582051.2582089.

[23] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Privacy and utility preserving sensor-data transformations," *Pervasive Mobile Comput.*, vol. 63, pp. 1–13, Mar. 2020. doi: 10.1016/j.pmcj.2020.101132.

[24] A. Brutti and A. Cavallaro, "On-line cross-modal adaptation for audio-visual person identification with wearable cameras," *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 1, pp. 40–51, Feb. 2017. doi: 10.1109/THMS.2016.2620110.

[25] G. Abebe, A. Catala, and A. Cavallaro, "A first-person vision dataset of office activities," in *Proc. Int. Workshop Multimodal Pattern Recognition Social Signals Human Computer Interaction*, Beijing, Aug. 2018, pp. 27–37. doi: 10.1007/978-3-030-20984-1_3.

[26] G. Abebe, and A. Cavallaro, "A long short-term memory convolutional neural network for first-person vision activity recognition," in *Proc. IEEE Int. Conf. Computer Vision Workshops*, Venice, Italy, Oct. 2017, pp. 1339–1346. doi: 10.1109/ICCVW.2017.159.

[27] A. Cavallaro and A. Brutti, "Audio-visual learning for body-worn cameras," in *Multimodal Behaviour Analysis in the Wild*, X. Alameda-Pineda, E. Ricci, and N. Sebe, Eds. New York: Academic, 2019, pp. 103–119.


SP