Privacy Implications of Accelerometer Data: A Review of Possible Inferences

Jacob Leon Kröger
Technische Universität Berlin
Hardenbergstraße 32
10623 Berlin
+49 30 7001 41037
kroeger@tu-berlin.de

Philip Raschke
Technische Universität Berlin
Ernst-Reuter-Platz 7
10587 Berlin
+49 30 8353 58353
philip.raschke@tu-berlin.de

Towhidur Rahman Bhuiyan
Technische Universität Berlin
Hardenbergstraße 32
10623 Berlin
+49 30 7001 41001
t.bhuiyan@campus.tu-berlin.de

ABSTRACT
Accelerometers are sensors for measuring acceleration forces. They can be found embedded in many types of mobile devices, including tablet PCs, smartphones, and smartwatches. Some common uses of built-in accelerometers are automatic image stabilization, device orientation detection, and shake detection. In contrast to sensors like microphones and cameras, accelerometers are widely regarded as not privacy-intrusive. This sentiment is reflected in protection policies of current mobile operating systems, where third-party apps can access accelerometer data without requiring security permission. It has been shown in experiments, however, that seemingly innocuous sensors can be used as a side channel to infer highly sensitive information about people in their vicinity. Drawing from existing literature, we found that accelerometer data alone may be sufficient to obtain information about a device holder's location, activities, health condition, body features, gender, age, personality traits, and emotional state. Acceleration signals can even be used to uniquely identify a person based on biometric movement patterns and to reconstruct sequences of text entered into a device, including passwords. In the light of these possible inferences, we suggest that accelerometers should urgently be re-evaluated in terms of their privacy implications, along with corresponding adjustments to sensor protection mechanisms.

CCS Concepts
• **Security and privacy**

Keywords
Accelerometer, Sensor, Privacy, Side channel, Inference attack

ICCSP 2019, January 19–21, 2019, Kuala Lumpur, Malaysia.

ACM ISBN 978-1-4503-6618-2/19/01…$15.00
DOI: https://doi.org/10.1145/3309074.3309076

1. INTRODUCTION
An accelerometer is an instrument for measuring acceleration forces caused by the movements and vibrations of an object, or by gravity. Today, all sorts of mobile devices, including smartphones, tablet PCs, smartwatches, digital cameras, wearable fitness trackers, game controllers, and virtual reality headsets, are equipped with built-in microelectromechanical accelerometers [1]. Studies even suggest that accelerometers are the most widely used sensor in wearable devices [2] and also the sensor that is most frequently accessed by mobile apps [3].

Among other common applications, acceleration signals are used for image stabilization in cameras, for measuring the orientation of a device relative to Earth's gravitational pull (e.g. to enable automatic display rotation between landscape and portrait mode), and for detecting user actions, such as moving or shaking a device.

While some sensors, such as microphones, cameras and GPS, are widely perceived as privacy-sensitive [4, 5] and require explicit user permission to be activated in current mobile operating systems [3], accelerometers are less well-understood in terms of their privacy implications, and also much less protected [6, 7]. Even scholarly literature has largely ignored potential issues in this field, with researchers describing accelerometer data as "not particularly sensitive" [8] or even "privacy preserving" [9].

Experimental studies have shown, however, that sensitive personal data can be inferred from accelerometer readings. This paper presents a non-exhaustive overview of possible inferences, drawing from multiple academic disciplines, including information science, psychology, health science, and computer science. According to our findings, accelerometers in mobile devices may reveal information about a user's activities (section 2.1), location (sect. 2.2), identity (sect. 2.3), device inputs (sect. 2.4), health condition and body features (sect. 2.5), age and gender (sect. 2.6), moods and emotions (sect. 2.7), and personality traits (sect. 2.8).

2. POSSIBLE INFERENCES
In this chapter, we present experimental studies from the scholarly literature in which sensitive information was successfully derived from accelerometer data. A visual overview is provided in Fig. 3, at the end of the chapter.

2.1 Activity and Behavior Tracking
A wide range of physical activity variables and behavior-related information can be derived from raw accelerometer data. Accelerometer-based pedometers ("step counters"), for instance, register the impacts produced by steps during motion and can estimate energy expenditure and distance walked [10]. In medical studies, wearable devices with embedded accelerometers are

widely used to assess the amount of sedentary time and physical activity among patients [11, 12].

Body-worn accelerometers have also been shown to enable real-time body posture and activity classification. High recognition accuracy has been achieved for basic physical activities, including running, walking, cycling, lying, climbing stairs, falling, sitting and standing [13–16], as well as for more complex activities, such as writing, reading, typing, painting, sorting paperwork or searching the internet [17].

Not only the type but also the duration of activities and temporal behavior patterns can be derived from acceleration signals [18, 19]. When worn during the night, mobile devices with built-in accelerometers may enable sleep-wake cycle monitoring, through variables such as sleep onset and offset, total sleep time and sleep intervals [20, 21], as well as the monitoring of sleep-related behaviors [11].

Accelerometers in handheld and wrist-worn devices can further be used to detect specific hand gestures [22], eating and drinking moments [23, 24], and smoking [25, 26]. Gait features of subjects, extracted from accelerometer data, can even reveal their level of intoxication. Researchers were able to distinguish “sober walk” from “intoxicated walk” [27] and to estimate blood alcohol content [28] as well as the number of drinks consumed [29] via accelerometry alone.

In [17], signals from a single body-worn accelerometer were used to detect if a subject is carrying a load. Accelerometer-based gait dynamics have also been used to estimate the weight of carried objects with robustness to variations in walking speeds, body types and walking conditions [30].

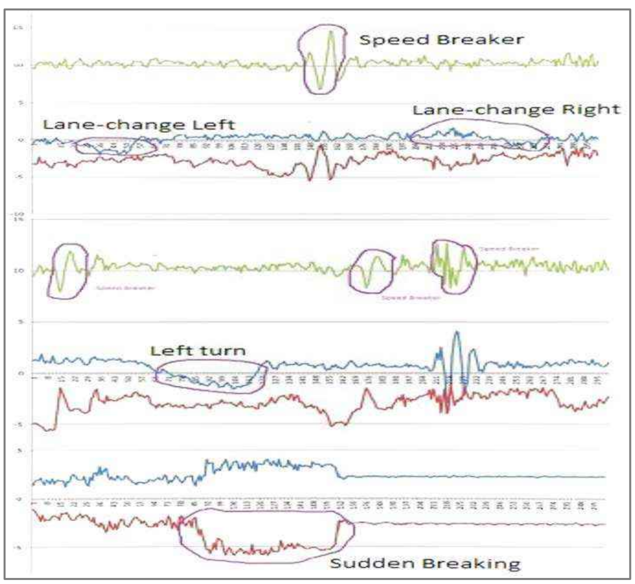

Figure 1: Classification of driving patterns based on streams of accelerometer data, from [31].

When located inside a car, motion sensors can be used to measure an operator’s driving behavior. In [31], Singh, Juneja and Kapoor identified events such as sudden breaking, sudden acceleration, right and left turns and lane changes from patterns in accelerometer data, as is illustrated in Fig. 1. From such information, researchers were able to detect aggressive or unsafe driving styles [32] and drunk driving patterns [33].

Based on indicative body movements and sound vibrations, both measured using accelerometers, researchers were able to derive speech activity and social interactions of subjects [9, 34]. Even ways of reconstructing speech solely from recorded vibrations have been explored. AccelWord, developed in [35], can detect hotwords spoken by a user, utilizing accelerometer data from commercially available mobile devices. Patents have already been filed for a “method of detecting a user's voice activity using an accelerometer” [36] and a “system that uses an accelerometer in a mobile device to detect hotwords” [37].

2.2 Location Tracking

It has been shown that accelerometers in mobile devices can be exploited for user localization and reconstruction of travel trajectories, even when other localization systems, such as GPS, are disabled. In [38], Han et al. were able to geographically track a person who is driving a car based solely on accelerometer readings from the subject’s smartphone. In their approach, they first calculate the vehicle’s approximate motion trajectory using three-axis acceleration measurements from an iPhone located inside the vehicle, and then map the derived trajectory to the shape of existing routes on a map. An example application of the algorithm is displayed in Fig. 2. Han et al. describe their results as “comparable to the typical accuracy for handheld global positioning systems.”

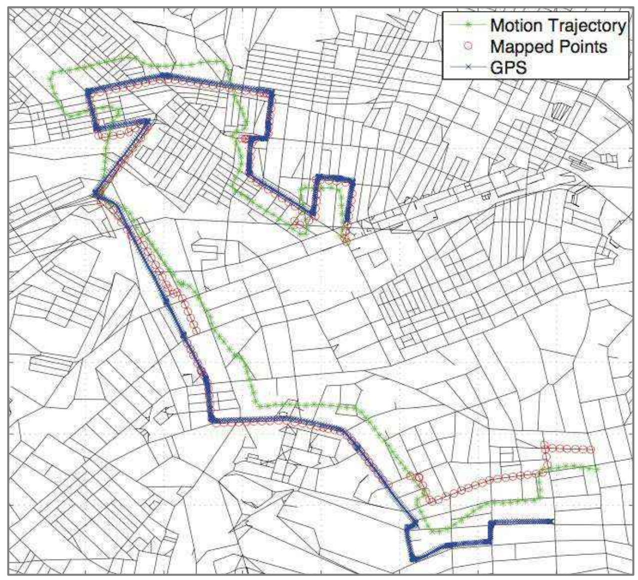

Figure 2: Map matching algorithm used in [38]. The green trail indicates the motion trajectory obtained from accelerometer data. The red trail indicates the inferred route. The blue trail indicates the actual route traveled (GPS data).

Hua, Shen and Zhong found that accelerometers in smartphones can also reveal the device’s location while the holder is using a metropolitan train system [39]. To achieve this, the researchers compare and match acceleration patterns with labeled training data to recognize specific station intervals through which the user travels. Results from experiments on a real metro line show that the accuracy of their approach could reach up to 89% and 92% if the metro ride is longer than 3 or 5 stations, respectively [39].

2.3 User Identification

Body movement patterns recorded by accelerometers in mobile devices have been demonstrated to be discriminative enough to differentiate between, or even uniquely identify, users. Various accelerometer-only approaches have been proposed to confirm the identity of a user based on biometric gait features [40, 41], hand gestures [42], or head movements [43]. Using accelerometer readings from smartphones, Kwapisz, Weiss and Moore were able to recognize individuals from a pool of 36 test subjects with 100% accuracy [44].

It has also been shown that, through aerial vibrations, accelerometers can be sensitive enough to capture sound, including human speech, in sufficient quality to distinguish between different speakers with high accuracy [35].

The location trajectory of a mobile device, which can be inferred from accelerometer data under certain conditions (as explained in section 2.2), may reveal a user's work and home addresses [45], and – in conjunction with white pages, employment directories, tax records, or other auxiliary datasets – a user's real identity [46].

Following an approach commonly referred to as *device fingerprinting*, users can further be told apart based on unique characteristics and features of their personal devices. Calibration errors in accelerometers, which are caused by imperfections in the manufacturing process, have been found sufficient to uniquely identify their encapsulating device [6, 47]. Such a "fingerprint" can be used, for instance, to track users across repeated website visits, even when private browsing is activated and other tracking technologies, such as canvas fingerprinting or cookies, are blocked [48].

2.4 Keystroke Logging

The input that users type into to their devices through touchscreens and keyboards contains highly sensitive information such as text messages, personal notes, login credentials and transaction details.

Based on the observation that swipes, taps and keystrokes often correlate with distinctive hand movements of the user, it has been shown that inputs can be reconstructed using motion sensor data from handheld and wrist-worn devices [49–51]. Some researchers have exclusively used accelerometer data for such keystroke inference attacks. Aviv et al. demonstrated that accelerometers in smartphones can be exploited to infer tap- and gesture-based input, including PINs and graphical password patterns [52]. Based on the same type of data, Owusu et al. were able to obtain entire sequences of text entered through a phone's touchscreen [53].

Through examining the source code of other existing approaches, it has been found that even multi-sensor attacks solely use acceleration information for tap detection, leading to the conclusion that defense mechanisms against these kinds of side channel attacks should focus on accelerometers [54].

Not only does the above imply that accelerometer data could offer sensitive insights into a user's communication and transactions: Beltramelli and Risi even warn that a user's entire technological ecosystem could be compromised when passwords are leaked through embedded sensors in consumer electronics [55].

2.5 Inference of Health Parameters and Body Features

Body-worn accelerometers can be used to gain insight into a person's physical characteristics and health status. Using accelerometer data from smartphones, researchers were able to derive an approximation of the body weight and height of users [56, 57]. A strong correlation has been observed between accelerometer-determined physical activity and obesity [58].

Physical activity is generally recognized as a promoter and indicator of health [59]. A person's amount of physical activity can reveal sensitive information about latent chronic diseases and the person's degree of mobility [12] as well as about cognitive function and even risk of mortality [60]. As explained in section 2.1, a wide range of activity-related variables can be derived from accelerometer data, including energy expenditure, type of activity and temporal activity patterns. This association is increasingly put to use in health studies, where accelerometers are used to remotely assess the physical activity level of participants [61].

Another important factor in population health is the amount of sleep that people get. Sleep loss has been associated with developing serious illnesses, such as cardiovascular disease and diabetes, and even with increased all-cause mortality [62]. Numerous studies have shown that accelerometers in wearable devices can be used for evaluating sleep patterns [20], sleep fragmentation [63] and sleep efficiency [64]. Actigraphy, an accelerometer-based assessment method, has been described as an "essential tool in sleep research and sleep medicine" [20]. Experimental results from Pesonen and Kuula suggest that accelerometers in consumer-targeted wearables can be as effective for sleep monitoring as research-targeted devices [21].

Specialized accelerometers have been used to measure various other health parameters, including voice health [65], postural stability [12] and physiological sound [66].

2.6 Inference of Demographics

Estimates of demographic variables such as age and gender can be made based on data from body-worn accelerometers. It has long been demonstrated that adults and children differ in their smoothness of walking, which is reflected in accelerometer readings [67]. Menz, Lord and Fitzpatrick compared gait features between young and elder subjects using acceleration signals and discovered that younger subjects showed greater step length, higher velocity and smaller step timing variability [68]. Using data from accelerometers in smartphones, Davarci et al. were able to predict the age interval of test subjects with a success rate of 92.5% [69]. Their work is based on the observation that children and adults differ in the way they hold and touch smartphones.

Experimental results by Cho, Park and Kwon indicate that there are also gender-specific movement patterns [70]. In accordance, research has shown that it is possible to estimate the sex of individuals based on hip movements [56], gait features [71] and physical activity patterns [72], all derived from accelerometer data. An experiment also revealed that female gait patterns are significantly influenced by the heel height of their shoes [73]. Weiss and Lockhart emphasize that accelerometer-based gender recognition can work independently of a subject's weight and height [56]. Even acoustic vibrations caused by a person's voice and captured through a smartphone accelerometer can be used to classify speakers into male and female with high accuracy [35].

2.7 Mood and Emotion Recognition

The level of physical activity, which can be measured using body-worn accelerometers (see section 2.1), has been identified as a potential predictor of human emotions [74] and depressive moods [75]. Zhang et al. were able to recognize emotional states of test subjects (happy, neutral, and angry) with fair accuracy, relying only on accelerometer data from smart wristbands [76]. Accelerometers in smartphones have been used to detect stress levels [77] and arousal [78] in users. Also, Matic et al. found a positive association between accelerometer-derived speech activity and mood changes [9].

2.8 Inference of Personality Traits

Methods have been proposed for inferring preferences and other personality traits solely from body gestures and motion patterns. Englebienne and Hung used wearable accelerometers to estimate the motivations, interests and group affiliations of study participants in scenarios of social interaction, based on their movements, body postures and expansiveness of gesturing [34].

A person's level of physical activity, which can also be measured using body-worn accelerometers (see section 2.1), has been shown to correlate with certain personality traits such as conscientiousness, neuroticism, openness, and extraversion [79]. Artese et al. evaluated the body movements of test subjects for seven days using accelerometer-based monitoring devices and found that agreeableness, conscientiousness and extraversion were positively and neuroticism negatively associated to more steps per day and other physical activity variables [80]. Examining correlates between the personality and physical activity of female college students, Wilson et al. discovered that neuroticism and the functioning of the behavioral inhibition system were both related to physical activity measures derived from accelerometer readings [81].

3. DISCUSSION AND IMPLICATIONS

As shown in the previous section, accelerometers in mobile devices can allow serious invasions of user privacy. Even when other sensors, such as cameras, microphones and GPS are turned off, accelerometer data can be sufficient to obtain information about a device holder's location, health condition, body features, age, gender, emotions and personality traits. Acceleration signals may even be used to uniquely identify a person based on biometric movement patterns and to reconstruct sequences of text entered into a device.

It has to be acknowledged that most experimental studies cited in this paper have substantial limitations. First, many approaches were only tested in controlled laboratory settings [14, 17, 24, 26, 32, 33, 35, 40, 41, 43, 53, 57]. For methods applied under real-life conditions, considerable reductions in accuracy have been observed [9, 82]. Second, several of the presented methods require prior knowledge about the user or the user's context in order to function [39–44, 52]. Third, subjects in some of the experiments wore accelerometers attached to certain body parts, such as chest [9, 15], hip [40], waist [14], or even multiple body parts [24, 25, 64], whereas in reality, mobile devices are mostly worn around the wrist [23] or interchangeably in hands, bags, and pockets [83]. In light of these limitations, the real-world applicability of the presented methods can be questioned.

On the other hand, it may reasonably be assumed that at least some of the parties who regularly access accelerometer data from consumer devices (e.g. device manufacturers, service providers, app developers) possess larger sets of training data, more technical expertise and more financial resources than the researchers cited in this paper. Furthermore, data from other sensors and auxiliary data may be available to potential adversaries, improving their capability to draw sensitive inferences, while the methods considered in this paper solely rely on accelerometer data. Thus, our work represents only an initial and non-exhaustive exploration of the topic.

It would be enough if even one of the identified threats is realized, however, for user privacy to be seriously impacted. Also, it seems probable that the risk will continue to grow with further improvements of sensor technologies in terms of cost, size and accuracy, further advances in machine learning methods, and further proliferation of accelerometer-equipped mobile devices.

Given the widespread perception of accelerometers as non-intrusive, we call for an urgent reconsideration of their privacy implications, along with corresponding adjustments to technical

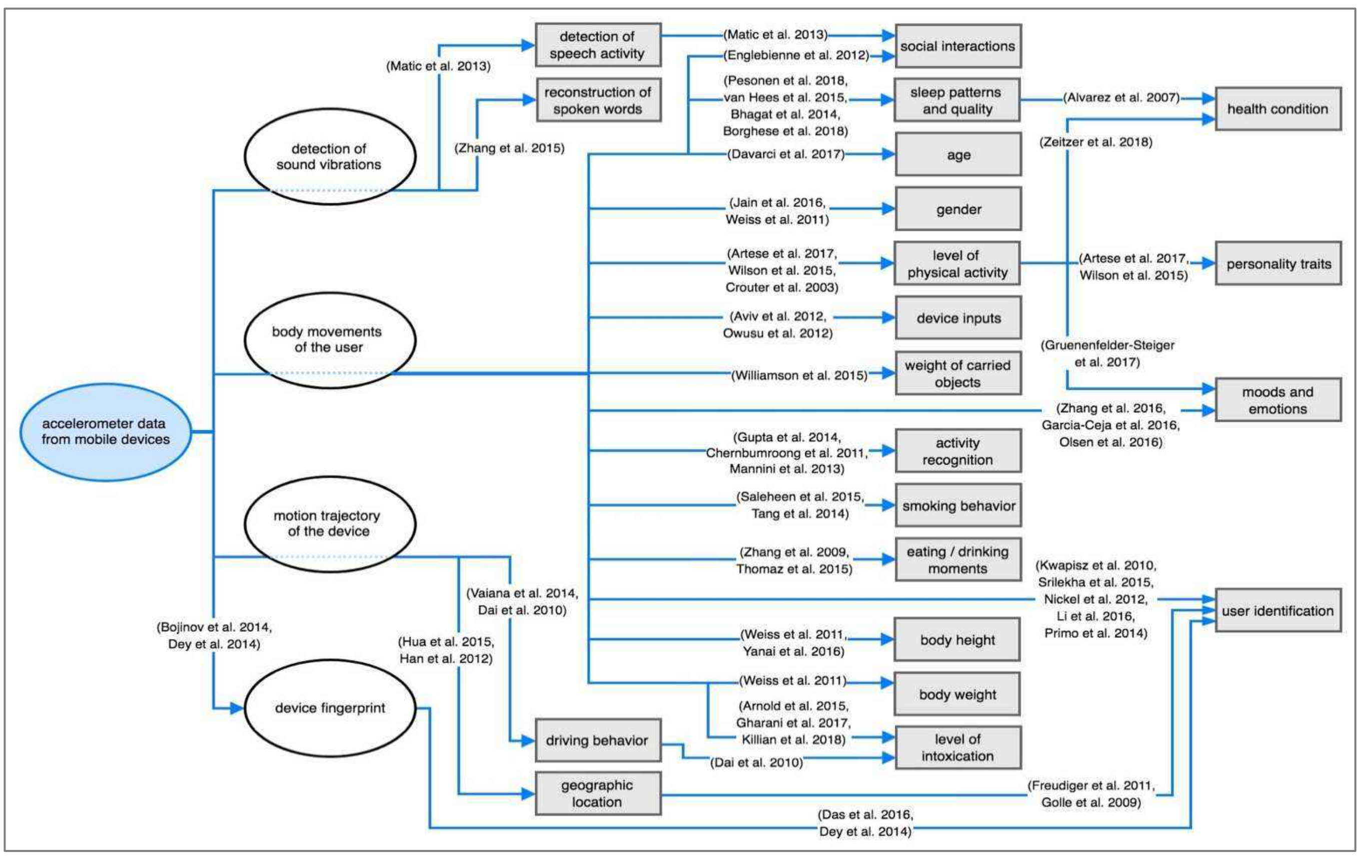

Figure 3: Overview of sensitive inferences that can be drawn from accelerometer data (according to the referenced studies).

and legal protection measures. In our opinion, the sensitivity of sensor data should generally be assessed in consideration of all inferences that could plausibly be drawn from it, and not based on the sensor's official purpose. Further research into the privacy-intrusion potential of accelerometers and other seemingly benign sensors is needed, taking into account state-of-the-art data mining techniques. As it is extremely difficult, however, to meaningfully determine the limits of continuously advancing inference methods, most sensors in mobile devices should be regarded and treated as highly sensitive by default.

4. CONCLUSION

Accelerometers are among the most widely used sensors in mobile devices, where they have a large variety of possible applications. They are commonly regarded as not privacy-intrusive and therefore often less access-restricted than other sensors, such as cameras and microphones. However, based on existing literature, we found that accelerometer data can enable serious privacy intrusions by allowing inferences about a device holder's location, identity, demographics, personality, health status, emotions, activities and body features.

Any trait or behavior of a user that results in characteristic movement patterns can potentially be detected through acceleration signals. Accelerometers are cheap, low in power consumption and often invisibly embedded into consumer devices. Thus, they represent a perfect surveillance tool as long as their data streams are not properly monitored and protected from potentially untrusted parties such as device manufacturers, service providers and app developers. In current mobile operating systems, third-party apps can access accelerometer data without requiring any permission or conscious participation from the user.

Although this paper conveys only a first impression of the privacy violations that could be enabled through accelerometers, the findings already are significant enough to express a warning to consumers who could be affected, as well as a call for action to the public and private actors who are entrusted with protecting user privacy in mobile devices.

5. REFERENCES

[1] Wearable Devices That Have an Accelerometer: 2018. *https://vandrico.com/wearables/device-categories/components/accelerometer*. Accessed: 2018-06-06.

[2] Richardson, S. and Mackinnon, D. 2017. *Left to their own Devices? Privacy Implications of Wearable Technology in Canadian Workplaces*. Surveillance Studies Centre.

[3] Bai, X. et al. 2017. Sensor Guardian: prevent privacy inference on Android sensors. *EURASIP Journal on Information Security*. 2017, 1 (Dec. 2017). DOI:https://doi.org/10.1186/s13635-017-0061-8.

[4] Hnat, T.W. et al. 2012. Doorjamb: unobtrusive room-level tracking of people in homes using doorway sensors. *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems* (2012), 309–322.

[5] Klasnja, P. et al. 2009. Exploring privacy concerns about personal sensing. *International Conference on Pervasive Computing* (2009), 176–183.

[6] Bojinov, H. et al. 2014. Mobile device identification via sensor fingerprinting. *arXiv:1408.1416*. (2014).

[7] Xu, Z. and Zhu, S. 2015. SemaDroid: A Privacy-Aware Sensor Management Framework for Smartphones. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (2015), 61–72.

[8] Weiss, G.M. et al. 2016. Actitracker: A Smartphone-Based Activity Recognition System for Improving Health and Well-Being. *IEEE International Conference on Data Science and Advanced Analytics (DSAA)* (Oct. 2016), 682–688.

[9] Matic, A. et al. 2013. Automatic Sensing of Speech Activity and Correlation with Mood Changes. *Pervasive and Mobile Sensing and Computing for Healthcare*. Springer Berlin Heidelberg. 195–205.

[10] Crouter, S. et al. 2003. Validity of 10 Electronic Pedometers for Measuring Steps, Distance, and Energy Cost. *Med. Sci. Sport Exer.* 35, (2003), 1455–60.

[11] Migueles, J. et al. 2017. Accelerometer Data Collection and Processing Criteria to Assess Physical Activity and Other Outcomes: A Systematic Review and Practical Considerations. *Sports Medicine*. 47, (2017).

[12] Yang, C.-C. and Hsu, Y.-L. 2010. A Review of Accelerometry-Based Wearable Motion Detectors for Physical Activity Monitoring. *Sensors*. 10, 8 (Aug. 2010), 7772–7788. DOI:https://doi.org/10.3390/s100807772.

[13] Chernbumroong, S. et al. 2011. Activity classification using a single wrist-worn accelerometer. *2011 5th International Conference on Software, Knowledge Information, Industrial Management and Applications (SKIMA) Proceedings* (Sep. 2011), 1–6.

[14] Gupta, P. and Dallas, T. 2014. Feature Selection and Activity Recognition System Using a Single Triaxial Accelerometer. *IEEE Transactions on Biomedical Engineering*. 61, 6 (Jun. 2014), 1780–1786. DOI:https://doi.org/10.1109/TBME.2014.2307069.

[15] Khan, A.M. et al. 2010. A Triaxial Accelerometer-Based Physical-Activity Recognition via Augmented-Signal Features and a Hierarchical Recognizer. *IEEE Transactions on Information Technology in Biomedicine*. 14, 5 (Sep. 2010), 1166–1172. DOI:https://doi.org/10.1109/TITB.2010.2051955.

[16] Lee, J.-V. et al. 2013. Smart Elderly Home Monitoring System with an Android Phone. *International Journal of Smart Home*. 7, 3 (2013), 16.

[17] Mannini, A. et al. 2013. Activity recognition using a single accelerometer placed at the wrist or ankle. *Med. Sci. Sport Exer.* 45, 11 (Nov. 2013), 2193–2203. DOI:https://doi.org/10.1249/MSS.0b013e31829736d6.

[18] Tapia, E.M. 2008. *Using machine learning for real-time activity recognition and estimation of energy expenditure*. Massachusetts Institute of Technology.

[19] Taraldsen, K. et al. 2012. Physical activity monitoring by use of accelerometer-based body-worn sensors in older adults: A systematic literature review of current knowledge and applications. *Maturitas*. 71, 1 (Jan. 2012), 13–19. DOI:https://doi.org/10.1016/j.maturitas.2011.11.003.

[20] Bhagat, Y.A. et al. 2014. Clinical validation of a wrist actigraphy mobile health device for sleep efficiency analysis. *2014 IEEE Healthcare Innovation Conference (HIC)* (Oct. 2014), 56–59.

[21] Pesonen, A.-K. and Kuula, L. 2018. The Validity of a New Consumer-Targeted Wrist Device in Sleep Measurement: An Overnight Comparison Against Polysomnography in Children and Adolescents. *J. Clin. Sleep Med.* 14, 04 (Apr. 2018), 585–591. DOI:https://doi.org/10.5664/jcsm.7050.

[22] Liu, J. et al. 2009. uWave: Accelerometer-based Personalized Gesture Recognition and Its Applications.

Pervasive Mob. Comput. 5, 6 (Dec. 2009), 657–675. DOI:https://doi.org/10.1016/j.pmcj.2009.07.007.

[23] Thomaz, E. et al. 2015. A Practical Approach for Recognizing Eating Moments with Wrist-Mounted Inertial Sensing. *UBICOMP*. 2015, (Sep. 2015), 1029–1040. DOI:https://doi.org/10.1145/2750858.2807545.

[24] Zhang, S. et al. 2009. Detection of Activities by Wireless Sensors for Daily Life Surveillance: Eating and Drinking. *Sensors*. 9, 3 (Mar. 2009), 1499–1517. DOI:https://doi.org/10.3390/s90301499.

[25] Saleheen, N. et al. 2015. puffMarker: A Multi-Sensor Approach for Pinpointing the Timing of First Lapse in Smoking Cessation. *UBICOMP*. 2015, (Sep. 2015), 999–1010.

[26] Tang, Q. 2014. Automated Detection of Puffing and Smoking with Wrist Accelerometers. *8th International Conference on Pervasive Computing Technologies for Healthcare* (2014).

[27] Killian, J. 2018. *Smartphone-Based Intelligent System: Training AI to Track Sobriety Using Smartphone Motion Sensors*. The Ohio State University.

[28] Gharani, P. et al. 2017. An Artificial Neural Network for Gait Analysis to Estimate Blood Alcohol Content Level. *Computing Research Repository*. (2017).

[29] Arnold, Z. et al. 2015. Smartphone Inference of Alcohol Consumption Levels from Gait. *2015 International Conference on Healthcare Informatics* (Oct. 2015), 417–426.

[30] Williamson, J.R. et al. 2015. Estimating load carriage from a body-worn accelerometer. *BSN* (Jun. 2015), 1–6.

[31] Singh, P. et al. 2013. Using Mobile Phone Sensors to Detect Driving Behavior. *Proceedings of the 3rd ACM Symposium on Computing for Development* (2013), 53:1–53:2.

[32] Vaiana, R. et al. 2014. Driving Behavior and Traffic Safety: An Acceleration-Based Safety Evaluation Procedure for Smartphones. *Modern Applied Science*. 8, (2014), 88–96.

[33] Dai, J. et al. 2010. Mobile phone based drunk driving detection. *2010 4th International Conference on Pervasive Computing Technologies for Healthcare* (Mar. 2010), 1–8.

[34] Englebienne, G. and Hung, H. 2012. Mining for motivation: using a single wearable accelerometer to detect people's interests. *Proceedings of the 2nd ACM international workshop on Interactive multimedia on mobile and portable devices* (2012), 23.

[35] Zhang, L. et al. 2015. AccelWord: Energy Efficient Hotword Detection through Accelerometer. *MOBISYS* (2015), 301–315.

[36] Dusan, S.V. et al. 2016. System and method of detecting a user's voice activity using an accelerometer. US9438985B2. Sep. 6, 2016.

[37] Mohapatra, P. et al. 2017. Energy-efficient, accelerometer-based hotword detection to launch a voice-control system. US20170316779A1. Nov. 2, 2017.

[38] Han, J. et al. 2012. ACComplice: Location inference using accelerometers on smartphones. *Fourth International Conference on Communication Systems and Networks* (Jan. 2012), 1–9.

[39] Hua, J. et al. 2015. We Can Track You If You Take the Metro: Tracking Metro Riders Using Accelerometers on Smartphones. *arXiv:1505.05958*. (May 2015).

[40] Nickel, C. et al. 2012. Authentication of Smartphone Users Based on the Way They Walk Using k-NN Algorithm. *Proceedings of the 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (2012), 16–20.

[41] Primo, A. et al. 2014. Context-Aware Active Authentication Using Smartphone Accelerometer Measurements. *IEEE Conference on Computer Vision and Pattern Recognition Workshops* (Jun. 2014), 98–105.

[42] Srilekha, R. and Jayakumar, D. 2015. A Secure Screen Lock System for Android Smart Phones Using Accelerometer Sensor. *International Journal For Science Technology And Engineering*. 1, 10 (May 2015), 96–100.

[43] Li, S. et al. 2016. Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. *IEEE International Conference on Pervasive Computing and Communications* (Mar. 2016), 1–9.

[44] Kwapisz, J.R. et al. 2010. Cell phone-based biometric identification. *IEEE International Conference on Biometrics: Theory, Applications and Systems* (Sep. 2010), 1–7.

[45] Freudiger, J. et al. 2011. Evaluating the privacy risk of location-based services. *International conference on financial cryptography and data security* (2011), 31–46.

[46] Golle, P. and Partridge, K. 2009. On the anonymity of home/work location pairs. *International Conference on Pervasive Computing* (2009), 390–397.

[47] Dey, S. et al. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable. *Network and Distributed System Security Symposium* (2014).

[48] Das, A. et al. 2016. Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses. *Network and Distributed System Security Symposium* (2016).

[49] Cai, L. and Chen, H. 2011. TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion. *HotSec*. 11, (2011), 9–9.

[50] Wang, H. et al. 2015. MoLe: Motion Leaks Through Smartwatch Sensors. *MOBICOM* (2015), 155–166.

[51] Xu, Z. et al. 2012. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks* (2012), 113–124.

[52] Aviv, A.J. et al. 2012. Practicality of Accelerometer Side Channels on Smartphones. *Proceedings of the 28th Annual Computer Security Applications Conference* (2012), 41–50.

[53] Owusu, E. et al. 2012. ACCessory: Password Inference Using Accelerometers on Smartphones. *Proceedings of the Twelfth Workshop on Mobile Computing Systems* (2012), 9:1–9:6.

[54] Song, Y. et al. 2014. Two Novel Defenses against Motion-Based Keystroke Inference Attacks. *Computing Research Repository*. (2014).

[55] Beltramelli, T. and Risi, S. 2015. Deep-Spying: Spying using Smartwatch and Deep Learning. *arXiv:1512.05616*. (Dec. 2015).

[56] Weiss, G.M. and Lockhart, J.W. 2011. Identifying user traits by mining smart phone accelerometer data. *Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data* (2011).

[57] Yanai, H.-F. and Enjyoji, A. 2016. Estimating Carrier's Height by Accelerometer Signals of a Smartphone. *HCI International* (Cham, 2016), 542–546.

[58] Ferrari, G.L. de M. et al. 2017. Accelerometer-determined peak cadence and weight status in children from São Caetano do Sul, Brazil. *Ciência & Saúde Coletiva*. 22, (Nov. 2017), 3689–3698. DOI:https://doi.org/10.1590/1413-812320172211.21962015.

[59] Warburton, D.E.R. et al. 2006. Health benefits of physical activity: the evidence. *Can. Med. Assoc. J.* 174, 6 (Mar. 2006), 801–809. DOI:https://doi.org/10.1503/cmaj.051351.

[60] Zeitzer, J.M. et al. 2018. Daily Patterns of Accelerometer Activity Predict Changes in Sleep, Cognition, and Mortality in Older Men. *J. Gerontol.* 73, 5 (Apr. 2018), 682–687. DOI:https://doi.org/10.1093/gerona/glw250.

[61] Chan, C.B. et al. 2012. Cross-sectional Relationship of Pedometer-Determined Ambulatory Activity to Indicators of Health. *Obesity Research*. 11, 12 (2012), 1563–1570. DOI:https://doi.org/10.1038/oby.2003.208.

[62] Alvarez, G.G. and Ayas, N.T. 2007. The Impact of Daily Sleep Duration on Health: A Review of the Literature. *Progress in Cardiovascular Nursing*. 19, 2 (2007), 56–59. DOI:https://doi.org/10.1111/j.0889-7204.2004.02422.x.

[63] Hees, V.T. van et al. 2015. A Novel, Open Access Method to Assess Sleep Duration Using a Wrist-Worn Accelerometer. *PLOS One*. 10, 11 (Nov. 2015). DOI:https://doi.org/10.1371/journal.pone.0142533.

[64] Borghese, M. et al. 2018. Estimating sleep efficiency in 10-to- 13-year-olds using a waist-worn accelerometer. *Sleep Health*. 4, 1 (Feb. 2018), 110–115. DOI:https://doi.org/10.1016/j.sleh.2017.09.006.

[65] Lei, Z. et al. 2017. Supervised learning in voice type discrimination using neck-skin vibration signals: Preliminary results on single vowels. *J. Acoust. Soc. Am.* 141, 5 (May 2017), 3916–3916. DOI:https://doi.org/10.1121/1.4988844.

[66] Liu, C. et al. 2015. A physiological sound sensing system using accelerometer based on flip-chip piezoelectric technology and asymmetrically gapped cantilever. *2015 IEEE 65th Electronic Components and Technology Conference (ECTC)* (May 2015), 1874–1877.

[67] Smidt, G. et al. 1972. Accelerographic analysis of several types of walking. *Amer. J. Physical Med.* 50, (1972), 285–300.

[68] Menz, H.B. et al. 2003. Age-related differences in walking stability. *Age and Ageing*. 32, 2 (Mar. 2003), 137–142. DOI:https://doi.org/10.1093/ageing/32.2.137.

[69] Davarci, E. et al. 2017. Age group detection using smartphone motion sensors. *2017 25th European Signal Processing Conference* (Aug. 2017), 2201–2205.

[70] Cho, S.H. et al. 2004. Gender differences in three dimensional gait analysis data from 98 healthy Korean adults. *Clin. Biomech.* 19, 2 (Feb. 2004), 145–152. DOI:https://doi.org/10.1016/j.clinbiomech.2003.10.003.

[71] Jain, A. and Kanhangad, V. 2016. Investigating gender recognition in smartphones using accelerometer and gyroscope sensor readings. *International Conference on Computational Techniques in Information and Communication Technologies* (Mar. 2016), 597–602.

[72] Jago, R. et al. 2005. Adolescent patterns of physical activity differences by gender, day, and time of day. *Amer. J. Physical Med.* 28, 5 (Jun. 2005), 447–452. DOI:https://doi.org/10.1016/j.amepre.2005.02.007.

[73] MERRIFIELD, H.H. 1971. Female Gait Patterns in Shoes with Different Heel Heights. *Ergonomics*. 14, 3 (May 1971), 411–417. DOI:https://doi.org/10.1080/00140137108931260.

[74] Kanning, M. and Schlicht, W. 2010. Be Active and Become Happy: An Ecological Momentary Assessment of Physical Activity and Mood. *Journal of Sport and Exercise Psychology*. 32, 2 (Apr. 2010), 253–261. DOI:https://doi.org/10.1123/jsep.32.2.253.

[75] Gruenenfelder-Steiger, A.E. et al. 2017. Physical Activity and Depressive Mood in the Daily Life of Older Adults. *The Journal of Gerontopsychology and Geriatric Psychiatry*. 30, 3 (Jan. 2017), 119–129. DOI:https://doi.org/10.1024/1662-9647/a000172.

[76] Zhang, Z. et al. 2016. Emotion recognition based on customized smart bracelet with built-in accelerometer. *PeerJ*. 4, (Jul. 2016). DOI:https://doi.org/10.7717/peerj.2258.

[77] Garcia-Ceja, E. et al. 2016. Automatic Stress Detection in Working Environments from Smartphones' Accelerometer Data: A First Step. *IEEE Journal of Biomedical and Health Informatics*. 20, 4 (Jul. 2016), 1053–1060. DOI:https://doi.org/10.1109/JBHI.2015.2446195.

[78] Olsen, A.F. and Torresen, J. 2016. Smartphone accelerometer data used for detecting human emotions. *2016 3rd International Conference on Systems and Informatics (ICSAI)* (Nov. 2016), 410–415.

[79] Wilson, K. and Dishman, R. 2014. Personality and Physical Activity: A Systematic Review and Meta-analysis. *Med. Sci. Sport Exer.* (May 2014), 473.

[80] Artese, A. et al. 2017. Personality and Actigraphy-Measured Physical Activity in Older Adults. *Psychology and Aging*. 32, 2 (Mar. 2017), 131–138. DOI:https://doi.org/10.1037/pag0000158.

[81] Wilson, K.E. et al. 2015. Personality Correlates of Physical Activity in College Women: *Medicine & Science in Sports & Exercise*. 47, 8 (Aug. 2015), 1691–1697. DOI:https://doi.org/10.1249/MSS.0000000000000570.

[82] Foerster, F. et al. 1999. Detection of posture and motion by accelerometry: a validation study in ambulatory monitoring. *Computers in Human Behavior*. 15, 5 (Sep. 1999), 571–583. DOI:https://doi.org/10.1016/S0747-5632(99)00037-0.

[83] Khan, A.M. et al. 2010. Accelerometer's position free human activity recognition using a hierarchical recognition model. *The 12th IEEE International Conference on e-Health Networking, Applications and Services* (Jul. 2010), 296–301.