6-16-2017

Privacy Issues and Solutions for Consumer Wearables

Alfredo J. Perez

Sherali Zeadally

Privacy Issues and Solutions for Consumer Wearables

Alfredo J. Perez
Columbus State University
Sherali Zeadally
University of Kentucky

Consumer wearables have emerged as disrupting devices that benefit citizens in areas such as mobile health, fitness, security, and entertainment. The mass adoption of these devices not only generates high revenues but also exposes important privacy issues. The authors identify some of the major privacy issues associated with consumer wearables and explore possible solutions to address privacy concerns.

Keywords
IEEE Keywords:
Biomedical monitoring, Privacy, Wearable sensors, Data privacy, Accelerometers, Wearable computing
INSPEC:
Controlled Indexing data privacy, mobile computing, wearable computers
INSPEC:
Non-Controlled Indexing consumer wearables, mobile health, privacy issues, privacy concerns
Author Keywords:
privacy, Security, sensing, wearable devices, wearables, consumer wearables, privacy and wearables

Recent advances in the miniaturization of sensors, computing power, and mobile Internet have enabled the development of devices that focus on the collection of data generated by individuals on their daily activities. One type of device that has been commercially exploited in the past several years is the wearable, which aims to improve users' quality of life while providing easy access to a range of services.

Wearables include jewelry, glasses, clothing, and other devices that are either worn on the body or kept around the body (for example, hanging on a purse or a backpack). In 2015, the global market value of wearable technology was $24.2 billion, of which nearly 75 percent came from consumer wearables such as smart watches and wristbands.[1] Current trends show a continuous rise for years to come, with a projected growth to $150 billion by 2026.[1]

Wearables can be classified into two categories: special-purpose and consumer wearables. Special-purpose wearables are developed to satisfy the requirements of applications in specific realms, such as security and mobile Health (mHealth). The acquisition process for these wearables is costly and often requires access to dedicated companies. Examples include body-worn cameras and physiological sensor devices used by law enforcement and the military.

In contrast, consumer wearables are acquired through retailers and their prices vary from a few dollars to thousands of dollars, depending on the individual's purchasing power (for example, a smartwatch could be bought with a gold encasement, thereby increasing its price); however, these devices are readily available and cost less than $1,000 on average. Market research has found that wrist-worn fitness-oriented bands have remained the top choice among US consumers (almost 50 percent were likely to purchase a fitness band in the next 12 months).[2]

Popularity aside, consumer wearables expose various privacy issues that must be addressed. In this article, we explore these emerging issues, along with possible solutions to protect the privacy of wearable users and others in their vicinity.

CONSUMER WEARABLES

A consumer wearable is a computer with embedded sensors and actuators/output devices developed as a garment, accessory, or device that is worn (or carried) by a

person and easily purchased through retailers. Although wearable technology is not a novel concept,[3] the use and appeal of wearable devices have increased significantly in the past five years with the advent of the mobile Internet and emergence of low-cost, high-performance mobile devices.

Typical wearables consist of the following.

- *A set of sensors*. Examples of sensors found on wearables include accelerometers, gyro- scopes, GPS, and cameras. In addition to these sensors, some wearables include touch- based and audio-based input.
- *A microprocessor/microcontroller*. This component performs basic calculations, filters data, and can extract features or recognize human activities from sensor data.
- *An embedded storage media*. Many consumer wearables have a flash-type storage media with the purpose of storing sensor data for later analysis.
- *A communication interface*. This is a way for the device to communicate with other wearables through a personal area network (PAN) or with a more powerful device such as a cellular phone, or to directly forward data to the cloud. Examples include near-field communication (NFC), Bluetooth, 802.15.6, Wi-Fi, and cellular network interfaces.
- *Output devices*. Some of these output devices provide vibrations, sound, and visual cues (such as lights, screens, or heads-up displays) to notify the user about the device's status. Some wearables provide information on a smartphone's screen.

In addition, many consumer wearables are sold with subscriptions to cloud-based services that provide storage for the collected sensor data or perform some type of analysis and issue feedback to users. Figure 1 presents the flow of data in consumer wearable systems. Data is collected through the wearable, which performs an initial analysis or data filtering/smoothing process. Depending on its programming, the wearable can forward data to a more powerful device (such as a mobile phone), store data on the device, or send the data to a cloud-based service. Many consumer wearables use an application on a mobile phone that aggregates data along with

location information.

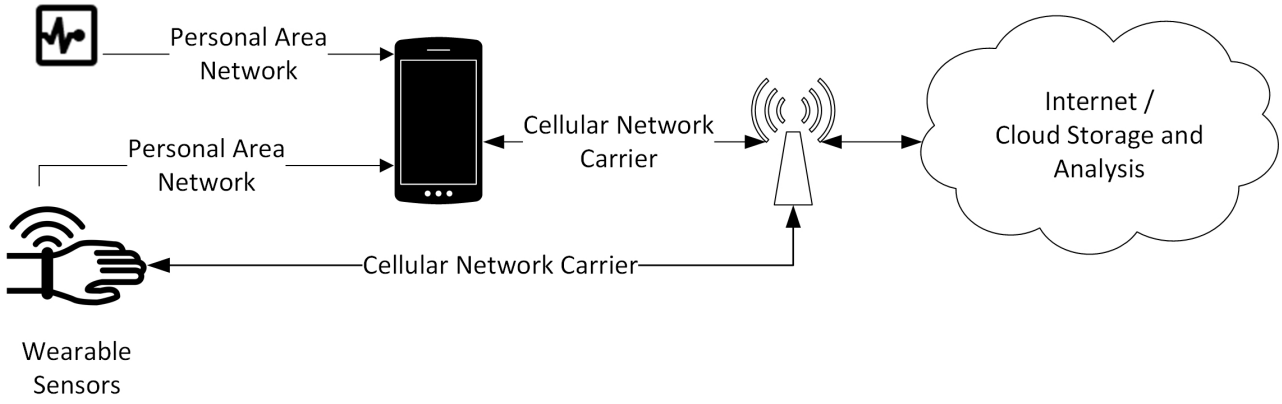

Figure 1. Consumer wearable systems.

The application on the mobile phone can perform data analysis locally and forward the data to a cloud-based service provided by the manufacturer (or to a third party). Data at the cloud service is analyzed and feedback is provided through the mobile device, a website, or the wearable itself. Depending on the cloud service provider, the collected data can be shared with other systems and users (such as social networking sites or third-party systems).

The current market for consumer wearables produces devices such as wristbands, smartwatches, smart jewelry, smart clothing, headsets, and others. There are more than 400 wearables on the market and more than 300 companies manufacturing these devices (http://vandrico.com/wearables/wearable-technology-database). Most of these devices are used in personal health management systems[2] such as fitness systems. Other uses include security, entertainment, and some specialized applications in healthcare.[4] Table 1 presents a sample list of wearable devices.

PRIVACY ISSUES FOR CONSUMER WEARABLES

Because the data collected from wearables can be related to the user, privacy is one of the major concerns in the utilization of these devices.[5] Market research by PWC[2] shows that most consumers in the US do not want to receive any type of human-centric data from friends and family, and that 43 percent of consumers surveyed do not feel

comfortable sharing any type of data about themselves. The human–computer interaction (HCI) community has also researched user privacy perceptions emerging from wearables, in particular the ownership of the space surrounding a wearable[6] and the attitudes about wearable usage.[7]

These works highlight that users have different concerns based on the type of data collected, the type of sensor used, and the purpose of the wearable.[7] Users' privacy concerns about consumer wearables are presented in Table 2. These concerns represent users' worries about possible privacy violations emerging from consumer wearable use. These concerns are associated with three categories (privacy issues) that represent major privacy aspects, including context privacy, by- stander privacy, and external data-sharing privacy.

Table 1. Examples of consumer wearable devices based on body location.

Body part	Wearable	Device type	Type of embedded sensors or actuators	Applications
Head	Glasses/head mounted displays	Microsoft HoloLens, Snap Spectacles, Oculus Rift	Accelerometers, gyro- scopes, micro- phone, cam- era, microphone/HUD, sound, vibration, intelligent digital assistants (HoloLens)	Leisure, games, virtual reality (VR), immersive reality
	Earphones/earrings	Bragi Dash, Ear-O-Smart, Samsung Gear IconX	Accelerometer, heart rate/vibration, sound	Entertainment, activity monitoring
	Headbands	BrainBit, Blue- fingers	EEG/sound	Entertainment, stress monitoring
	Necklaces	Bellabeat LEAF, ARC Pendant, Amber Alert GPS	Accelerometers, ECG, heart rate, GPS, micro- phone/vibration, lights	Activity tracker, physiological monitoring
Trunk	Chest straps	Zephyr Bioharness, Polar H7 Heart Rate Sensor	ECG, skin conductivity, heart rate, accelerometers,	Activity tracker, physiological monitoring,

	Belt wearable	Game Golf, Spire Health Tracker, Samsung WELT	breath rate, breath depth, position, body temperature	sports tracker (leisure)
Arm	Wristbands	Fitbit Alta, Jawbone Onyx	Heart rate, accelerometers, microphone, GPS, gyro- scope, skin conductivity/screen, vibration, lights, LCD, speaker	Activity tracker, physiological monitoring, mood monitoring, sports tracker, input devices, controllers
	Smart watches	Apple Watch 2, Fossil Q Asus Zenwatch 3, LG Watch Urbane, Casio Smart Outdoor Watch, Tag Heuer Connected	Intelligent digital assistants (Android Wear 2.0 devices include Google Assistant and Apple Watch 2 includes Siri in combination with mobile phone)	
	Armbands	Myo Gesture Control Armband		
Leg	Calf wearable	BSXinsight, NeuroMetrix Quell	Oxygen saturation/lights, electrodes	Muscle oxygenation tracking, neurological stimulation (pain relief management)
	Ankle wearable	Flyfit, Owlet Baby Monitor	Accelerometers, heart rate, oxygen saturation	Activity tracker, physiological monitoring
	Foot wearable	Wahoo Stride Sensor, Adidas miCoach Speed Cell, Nike+ Sensor	Accelerometers, steppers	Activity tracker
External	Clip-on clothing, backpack	TZOA, mobile phones	Air quality, UV radiation, light, humidity, temperature, accelerometers, gyroscopes, microphones	Environmental monitoring, activity/physiological monitoring, location-based services

Table 2. Users' privacy concerns while wearing a device that continuously registers their actions.[6]

Privacy concern	Description
Social implications	Unawareness of a network of friends regarding data being collected about them
Criminal abuse	Fear that wearable data will be used by criminals to harass a user
Facial recognition	Association and recognition of a by- stander to a place or situation where the bystander would not wish to be recognized by others
Access control	Fear of third-party service providers sharing data without consent
Social media sync	Immediate publishing or sharing by the wearable device without knowledge of the user
Discrete display and visual occlusion	Notifications/information to users that might be seen by bystanders who should not have access
Right to forget	The user's wish to delete collected data that he or she wants to forget
Surveillance and sousveillance	Continuous tracking of activities that might make the user feel that no matter what he or she does, everything is recorded
Speech disclosure	Capturing speech that a user or bystanders would not want to record or share
Surreptitious A/V recording	Recording of video without permission that might affect bystanders
Location disclosure	Fear of sharing a location inadvertently to third parties that should not have access

The association between privacy concerns and privacy issues is presented in Table 3.

Table 3. Privacy issues for consumer wearables.[6]

Privacy issue	Users' privacy concern
Context privacy	Access control Location disclosure Social implications Discrete display and visual occlusion Users' fears Speech disclosure Right to forget
Bystander privacy	Speech disclosure Social implications Facial recognition (identifiability) Surreptitious A/V recording Users' fears Location disclosure
External data-sharing privacy	Access control Location disclosure Social implications Users' fears Criminal abuse Social media sync Discrete display and visual occlusion Right to forget

Context Privacy

Many consumer wearables continuously collect data about the user. For example, some activity trackers collect data even when the user is sleeping to provide an accurate view of the user's health. Some wearables have voice-activated assistants that are included directly (such as Google Assistant in Android Wear 2.0 or Cortana in Microsoft HoloLens) or can connect to the wearable (for example, Apple's Siri). These assistants can perform accurate, continuous tracking of speech and non-speech sounds about the wearer and the device's surroundings.

Wearables can collect data about events that a user might not want to share with cloud service providers. As such, consumer wearables should provide mechanisms to handle context privacy in a way that the user can allow data collection and uploading only when he or she desires, to deny contexts where sensing should not take place, or both. In addition, many wearables are designed not to be a burden, so users can forget that they are wearing them.

Context privacy refers to the problem of inference about context and actions that could be obtained about the user from the sensor data shared with the cloud service provider. To resolve this issue, the user should impose conditions or rules on sensor data collection to handle the compart- mentalization of data (for example, on a need-to-know basis) with the cloud service provider, thereby diminishing or avoiding the inference. These rules can be defined at different granularities, from allowing or denying raw sensor data readings to the creation of rules for complex ac- tivities.[8] However, for most current wearables, the user can only allow or deny the collection of sensor data by turning the wearable off, removing the device from the body, or allowing sensor readings based on basic rules (such as sensor on or off).

> Bystander privacy is the problem of protecting the privacy of third parties who can be affected when a wearable device is used in their surroundings.

Bystander Privacy

Some wearables have sensors that not only capture data about the wearer but also allow the collection of data about the user's surroundings. Examples include head-mounted cameras and embedded micro- phones, which can capture data that can

identify people and actions that are not related to the wearable's user. Extensive media coverage about head-mounted wearables in addition to research have under- scored the importance of this issue.[7–9]

Bystander privacy is the problem of protecting the privacy of third parties who can be affected when a wearable device is used in their surroundings. Pidcock et al.[10] argued that this problem has been over- looked, as most research has focused on the wearer's privacy. Nevertheless, public perception about this issue dictates otherwise. HCI research found that consumers have serious concerns about wearables that explicitly show cameras (such as smart glasses) and microphones.[7] Consumers are anxious about speech disclosure, spying, surveillance, and identifiability that could result from photos, videos, or audio samples collected with these devices.

External Data-Sharing Privacy

As mentioned earlier, consumer wearable devices collect data about the individual, and such data is usually forwarded to a cloud service that aggregates, analyzes, and provides feedback to the user. Collected data generally corresponds to health-related data, but other types of data can also be collected and forwarded, depending on the capacity of the device (such as photos or location traces) and the goal of the system.

In the US, unless the wearable is utilized in systems developed to enhance a citizen's health and is part of a medical healthcare system (for example, mHealth), cloud service providers do not have to follow the guidelines specified in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).[11]

Under these laws, a user of an mHealth system has some key rights to manage the privacy of his or her health information, such as the right to request copies of medical records and health information, the right to make changes to information believed to be wrong, the right to know who accesses the user's health data, and the right for the user to manage with whom his or her health data is shared (with an exception for when the data affects the user's healthcare). In addition, these acts of law establish accountability measures for privacy breaches. Similar privacy laws for mHealth

systems exist in other countries.[11]

In the US, these rules do not apply to cloud service providers of consumer wearables unless the device is certified as medical grade and used in a medical healthcare system. Therefore, privacy policies are utilized as legal agreements between users and cloud service providers to communicate with users about how their privacy is handled. But these privacy policies seek to protect the interests of the businesses providing these services instead of the users.

A report by the US Federal Trade Commission (FTC) stated that privacy policies are not successful in informing users about data practices due to their length, complexity, and the lack of language uniformity.[12] Therefore, users have little control about how and when their data is shared—the only option is not to use the device or the service at all. Although many cloud ser- vices allow users to share their data explicitly through social networks, the concern here is about what the company could do with the data based on the user's acceptance of the privacy policy.

SOLUTIONS FOR PRIVACY ISSUES IN CONSUMER WEARABLES

Here we offer solutions for wearable privacy issues in three areas: context privacy, bystander privacy, and external data-sharing privacy.

Context Privacy

Solutions for context privacy can be classified into two groups: mechanisms for allowing data collection and mechanisms for denying data collection. In the first group, the goal is to create rules for the device to collect data only when the user wishes to do so. Even though it has been proposed for community-based sensing, the virtual trip line (VTL) approach allows data collection based on a geographical and temporal context.[13] In the VTL system, data collection is al- lowed only on the "virtual lines" defined by the geographical context. Similar approaches include the concept of bubble sensing,[14] where contexts are based on sensor data readings, and privacy bubbles,[15] upon which users define contexts to manage content. Because these approaches (with the exception of privacy bubbles) were proposed for community-based sensing, they relied on the idea that there is a campaign organizer who defined these contexts. As such,

there is no involvement of the actual user on the establishment of the contexts, which might not represent the user's choices.

For mechanisms to deny data collection, the virtual walls approach allows users to define the contexts where data collection should not be performed.[16]

Independent of these two types of mechanisms, these approaches make use of contexts that are based on low-level rules to access raw sensor data. More research is needed to create these rules on activities that a user can better understand (such as "don't collect data when I eat"). Also, be- cause these approaches were developed primarily for community-based sensing, they are con- trolled by a campaign organizer rather than the user, which is not optimal for a wearable system because the privacy rules should be controlled directly by the user.

Bystander Privacy

Notification systems have been proposed to handle bystander privacy.[10] These systems alert by- standers when someone collects identifiable data (such as photos) in his or her surroundings to take appropriate measures (for example, leaving the area or expressing their concern about data collection).

Blurring has also been utilized to protect bystander privacy. Examples include algorithms for blurring faces and bodies in panoramic photos[17] and a combination of machine learning and privacy profiles to blur bystanders based on their privacy choices.[18]

External Data-Sharing Privacy

Technical solutions for external data sharing exist as methods for anonymization in databases. These methods fall under two major categories: anonymization for the release of microdata (un- aggregated data) and anonymization for the release of summarized (aggregated) data.

For privacy in a microdata release, the goal is to guarantee that if a record is released in the microdata, an attacker could not associate confidential attributes of a record in the microdata with an identifier from the record (such as a name, social security number, or face). Examples of methods for anonymizing microdata include *k*-

anonymity (where each record in a microdata re- lease is indistinguishable from at least $k - 1$ other records with respect to identifying attributes), *l*-diversity (the microdata table contains at least *l* well-represented values with respect to a sensitive or confidential attribute), and *t*-closeness (the distance between the distribution of a sensitive attribute in an anonymized group should not be different from the global distribution by more than a threshold value *t*).[19]

For aggregated data, the goal is to guarantee whether the release of a statistic (an average) can reveal information about a particular record in the database or an identifier that was used to create the statistic. Differential privacy has been proposed as an approach to handle privacy in the release of aggregated data.[18] In this approach, the goal is to compute the desired statistical data and perturb it with some noise such that perturbed statistical data cannot reveal whether a particular record was utilized to generate the statistical data. Differential privacy provides a definition to generate the noise in such a way that the perturbed statistical data can represent the data but cannot reveal information about a particular record.

FUTURE PRIVACY CHALLENGES WITH CONSUMER WEARABLES

Here we discuss future privacy challenges and open issues.

Access Control

Current models for data management and processing in consumer wearables require the user to upload data to cloud service providers. The issue of a service provider sharing data with third parties without user consent could be addressed by the development of novel privacy frame- works that ask explicitly for permission when a service provider attempts to process or share data externally. Mechanisms for fine-grained access control (electronic consent for data-sensor readings) are needed for users to better handle their privacy.

One aspect that remains an open issue in consumer wearables is about ownership or licensing of wearable sensor data. How different is wearable sensor data from other types of digital data—such as images, music, or movies—from the copyright point of view?

The Privacy by Design (PbD) framework is an approach that incorporates

privacy throughout the engineering process of a product.

Privacy by Design

The Privacy by Design (PbD) framework is an approach that incorporates privacy throughout the engineering process of a product. This framework incorporates seven principles that should guide the design, development, utilization, and disposal of a device or software system for privacy protection.[12] In particular, the framework seeks to protect health and financial data. As many wearable devices are currently used for personal health management systems, PbD is directly related to the development of these devices.

The PbD framework was recommended by the FTC to help to protect the privacy of users.[12] In order for this framework to become an operational reality in the information communication technology area, various stakeholders—namely industry, academia, and consumers— should adopt the framework. In industry, PbD calls for the framework to become guiding principles of any IT product. In academia, privacy should become a pillar to educate IT professionals. For consumers, the implications and consequences of privacy should be a deciding factor when purchasing a wearable.

ACKNOWLEDGMENTS

We thank the anonymous reviewers and the editor for their valuable comments that helped us improve the quality and presentation of this article. Alfredo Perez's effort was supported by the US National Science Foundation under award 1560214, and Sherali Zeadally's effort was supported by a University Research Professorship Award from the University of Kentucky in 2016.

REFERENCES

1. J. Hayward, *Wearable Technology 2018-2028*, IDTechEx, May 2018; www.idtechex.com/research/reports/wearable-technology-2016-2026-000483.asp.
2. *Health Wearables: Early Days*, report, PWC Health Research Institute, May 2016; www.pwc.com/us/en/health-industries/health-research-institute/publications/health- wearables-early-days.html.

3. S. Park, C. Kyunghee, and J. Sundaresan, “Wearables: Fundamentals, Advancements, and a Roadmap for the Future,” *Wearable Sensors: Fundamentals, Implementation and Applications*, E. Sazonov and M. Neuman, Elsevier, 2014.
4. O.J. Muensterer et al., “Google Glass in Pediatric Surgery: An Exploratory Study,”
5. *Int'l J. Surgery*, vol. 12, no. 4, 2014, pp. 281–289.
6. *Privacy in a Digital, Networked World — Technologies, Implications, and Solutions*,
7. S. Zeadally and M. Badra, Springer, 2015.
8. R. Mitchell, “Sensing Mine, Yours, Theirs, and Ours: Interpersonal Ubiquitous Interactions,” *Proc. 2015 ACM Int'l Symposium Wearable Computers* (ISWC), 2015,
9. pp. 933–938.
10. V.G. Motti et al., “Users' Privacy Concerns about Wearables: Impact of Form Factor, Sensors, and Type of Data Collected,” *Proc. 1st Workshop on Wearable Security and Privacy* (Wearable), 2015; doi.org/10.1007/978-3-662-48051-9_16.
11. D. Christin et al., “A Survey on Privacy in Mobile Participatory Sensing Applications,” *J. Systems and Software*, vol. 84, no. 11, 2011, pp. 1928–1946.
12. J. Häkkilä et al., “Design Probes Study on User Perceptions of a Smart Glasses Concept,” *Proc. 14th ACM Int'l Conf. Mobile and Ubiquitous Multimedia* (MUM), 2015, pp. 223–233.
13. S. Pidcock et al., “Notisense: An Urban Sensing Notification System to Improve Bystander Privacy,” *Proc. 2nd Int’l Workshop Sensing Applications Mobile Phones* (PhoneSense), 2011, pp. 1–5.
14. S. Avancha, A. Baxi, and D. Kotz, “Privacy in Mobile Technology for Personal Healthcare,” *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, 2012, pp. 1–54.
15. *Protecting Consumer Privacy in an Era of Rapid Change*, government report, Federal Trade Commission, March 2012.
16. B. Hoh et al., “Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring,” *Proc. 6th Int’l Conf. Mobile Systems, Applications, and Services* (MobiSys), 2008, pp. 15–28.

17. H. Lu et al., “Bubble-Sensing: A New Paradigm for Binding a Sensing Task to the Physical World Using Mobile Phones,” *Proc. Int’l Workshop Mobile Devices and Urban Sensing* (MODUS), 2008, pp. 1–8.
18. D. Christin et al., “Share with Strangers: Privacy Bubbles as User-Centered Privacy Control for Mobile Content Sharing Applications,” *Information Security Technical Report*, vol. 17, no. 3, 2013, pp. 105–116.
    A. Kapadia et al., “Virtual Walls: Protecting Digital Privacy in Pervasive Environments,” *Proc. Int’l Conf. Pervasive Computing*, 2007, pp. 162–179.
A. Devaux et al., “Face Blurring for Privacy in Street-Level Geoviewers Combining Face, Body and Skin Detectors,” *Proc. IAPR Conf. Machine Vision Applications* (MVA), 2009, pp. 86–89.
19. T. Ye et al., “Negative Face Blurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass,” *Proc. 23rd ACM Int’l Conf Information and Knowledge Management*, 2014, pp. 2036–2038.
20. S. De Capitani et al., “Data Privacy: Definitions and Techniques,” *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 20, no. 6, 2012, pp. 793–817.

ABOUT THE AUTHORS

Alfredo J. Perez is an assistant professor with the TSYS School of Computer Science at Columbus State University. His research interests include mobile computing and sensing, wireless sensor networks, and security and privacy in mobile sensor networks. Perez received a PhD in computer science and engineering from University of South Florida. He is a member of the National Academy of Inventors and the IEEE Communications Society. Contact him at perez_alfredo@columbusstate.edu.

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. His research interests include cybersecurity, privacy, Internet of Things, and energy-efficient networking. Zeadally received his doctoral degree in computer science from the University of Buckingham. He is a fellow of the British Computer Society and the Institution of Engineering Technology. Contact him at szeadally@uky.edu.