A Survey of Privacy Concerns in Wearable Devices

Prerit Datta
Department of Computer Science
Texas Tech University
Email: prerit.datta@ttu.edu

Akbar Siami Namin
Department of Computer Science
Texas Tech University
Email: akbar.namin@ttu.edu

Moitrayee Chatterjee
Department of Computer Science
Texas Tech University
Email: moitrayee.chatterjee@ttu.edu

***Abstract*—With the continued improvement and innovation, technology has become an integral part of our daily lives. The rapid adoption of technology and its affordability has given rise to the Internet-of-Things (IoT). IoT is an interconnected network of devices that are able to communicate and share information seamlessly. IoT encompasses a gamut of heterogeneous devices ranging from a small sensor to large industrial machines. One such domain of IoT that has seen a significant growth in the recent few years is that of the wearable devices. While the privacy issues for medical devices has been well-researched and documented in the literature, the threats to privacy arising from the use of consumer wearable devices have received very little attention from the research community. This paper presents a survey of the literature to understand the various privacy challenges, mitigation strategies, and future research directions as a result of the widespread adoption of wearable devices.**

***Index Terms*—privacy, wearable devices, IoT**

I. Introduction

IoT is an umbrella term that encompasses a wide array of application domains such as smart cities, agriculture, transportation, medical, industrial and manufacturing. Each of these domains has their own challenges and design issues. One such area that has seen a significant growth in recent years is that of the wearable devices. Wearable devices can be worn on different body-parts. The repository introduced by Vandrico [1] is one of the largest online databases of wearable devices. It includes a list of wearable devices categorized according to the body parts they are worn on (e.g., head). Among the list of these wearable devices, smartwatches and wristbands account for the largest percentage due to their ease of comfort, affordability and ease of integration and use with day-to-day activities. The market for wearable devices was estimated to be worth of 4 billion in 2017, with one in every six-person using a wearable device such as a Smartwatch [2] and continuous to grow significantly. Consumers use these wearable devices for a variety of daily activities including fitness tracking, calendar management, quickly responding to texts and emails and other routine activities.

These wearable devices are equipped with high-quality sensors that can enable an adversary to infer personal information about a user such as location, physiological and emotional behaviors [3], [4]. A concerning issue is that most of the consumers are not aware of the privacy risks posed by these wearable devices [5] or have severe misconceptions about privacy pertaining to these devices [6], [7].

Another area of privacy concern arising with the use of wearable devices is *life-logging*. Life-logging is a form of blogging wherein people called *life-loggers*, capture videos, photos or audio recordings as they go on about doing their daily chores and post it online. This can pose privacy concerns for both the innocent bystanders and the person wearing the device.

The term *privacy* has long been in use in politics and social sciences, with it being legally recognized as a fundamental human right in the early 1890's. Privacy is often defined as the "*right to be let alone*" [8] or to allow an individual "*freedom from intrusion*" [9]. Privacy and its definition has been viewed differently by researchers. Privacy concerns are often subjective and rely on the context to determine whether or not something is private and should be treated as a personal matter.

This paper presents a survey of the privacy challenges arising from the use of wearable devices in the existing literature. In addition, we discuss some of the existing solutions, open issues and future research directions. The paper is organized as follows: Section II provides an overview of the privacy literature of IoT and wearable devices. In Section III, we discuss privacy and other issues that need to be addressed in the wearable landscape. In addition, we examine some the possible mitigation strategies to overcome those challenges. Section IV concludes the paper.

II. State-of-the-Art

One of the earliest and widely used attempt to classify threats to privacy was introduced by Solove [10]. Solove defined four categories or stages of harmful activities from the perspective of data collection and how these activities can cause privacy breaches and thus, concerns for the users. The four main categories of the taxonomy are: 1) information collection, 2) information processing, 3) information dissemination, and 4) invasion. These are further sub-divided into activities that can lead to privacy invasion. For example, information collection is composed of *surveillance* - monitoring and collecting activities of an individual and *interrogation* - probing for more information. Since then, many researchers have analyzed threats to privacy in a variety of different contexts.

Di Pietro and Mancini [11] discuss general security and privacy issues arising from the use of wearable wireless devices. The authors contend that because of the way wearable

978-1-5386-5035-6/18/$31.00 ©2018 IEEE

devices are designed to be always connected to the web (i.e., web presence), there could be potential information leakage based on interaction among devices even though they are logically unrelated. For example, a PDA interacting with the control system of a car may allow the PDA to track the car's location, or its license plate number even though its interaction with the car should have been limited to specific use such as opening the garage door. The authors propose two strategies to counteract the problem, that is, a *logical border* that makes use of *anonymous user-id (UID)* in order to limit the interaction with other devices (web presence) based on user-specified use limitations. The authors argue that although this approach seems lucrative, it burdens the user with specifying what can and cannot be shared. A better approach according to the authors is to create default "user-profiles" having inbuilt logical borders that limit interactions to the minimum.

Raij et al. [3] claim to be the first to highlight users concerns with the inferences (such as stress levels, dietary habits, etc.) that can be derived from their seemingly harmless physiological data. The authors conducted a study for a wearable sensor suite known as "Autosense" with 66 participants. The aim of their study was to assess the participants concern levels: 1) with the continuous data collection by wearable devices, 2) when certain restrictions and abstractions are applied to the data collected, and 3) when their data is shared among different parties. The authors found that the concern level is more significant when the users have a share in the data being collected. Also, the authors found that when temporal and spatial contexts were added to the data, the participants became more concerned about privacy due to the fact that their time and location could be inferred from such data. Finally, the authors conclude that the participants showed less concern in sharing their data with the researchers than with public even when they were guaranteed anonymity. Although this study brings forth some interesting results, it is, however, unclear if similar results could be obtained with just hand-held or smartwatches or fitness bands in comparison to a full-body suite of sensors as in the case of AutoSense.

Studies have shown that the users have severe misapprehensions about their privacy when it comes to wearable devices. For instance, in the study conducted by Lowens et al. [7] with 32 participants, the authors found that the users did not consider "daily activity" data to be sensitive (i.e., private) and many users believed that the lack of a physical keyboard on the device prevented them from entering and storing any sensitive information thereby leading to a false sense of privacy. Moreover, it was found that the users often had no idea about what type of data and how much data is being collected and stored by these wrist-worn devices. Many users had "don't care" and "nothing-to-hide" attitude when it came to privacy risks arising from the wearable devices.

Somewhat similar results were observed by the Udoh and Alkharashi [6] in a study conducted with 10 students about their behaviors, attitudes, and awareness of privacy threats emerging from the wearable devices. The authors discovered that the students had a false sense of privacy as they believed that the brand of wearable devices took appropriate measures to safeguard the users' privacy. With one of the participants even citing the case of Apple vs. the FBI, in which Apple refused to unlock an iPhone of an accused in a criminal proceeding to defend their viewpoint.

Moitti et al. [12] analyzed users' privacy concern pertaining to wearable devices. The authors analyzed the qualitative data from various sources such as e-commerce websites, forums and social media where the users expressed their concerns regarding the privacy of wearable devices. They categorized the users' privacy concerns into three categories based on whether the concern was related to 1) device or the application, 2) sensor specific, or 3) user's data. The authors found that the users were more concerned about the privacy challenges posed by wearable devices in comparison to the mobile devices due to location tracking and inconspicuously sharing it on social media.

Becker et al. [13] present a taxonomy for users' perceived privacy risk for wearable devices. The authors conducted a study on 71 participants asking them to rate the perceived risk on 9-point scale from a random sample of 35 devices chosen from wearable database [1]. The participants were then interviewed to explain the rationale behind their choices. The authors discovered that the users' perceived risk is based upon three major dimensions: perceived variety of data collected, perceived sensitivity of the data collected and how long the data is stored. The authors also discovered that the type of the device also plays a significant role in the perceived privacy risk by the users. For e.g., some participants found a fitness bracelet to be perceived as more riskier than an activity tracker embedded in a shoe even though both of these devices collect sensitive health data from the user. Perez et al. [14] discuss some of the privacy concerns and issues arising from use of wearable devices. They categorize privacy concerns based on data sharing, context and bystander.

III. Privacy Challenges and Open Issues in Wearable Devices

In addition, to the various privacy challenges described in Section II, there remains several privacy challenges and other issues that need to be addressed by the research community and manufacturers:

A. Bystanders Privacy

Wearable devices that have a built-in camera such as head-mounted devices [14] or Google glass can record bystanders and their activities without their consent, which can lead to embarrassment or harm to their reputation when their images or voice/video recordings are posted online. In addition, recordings from these seemingly innocuous devices can reveal location and other sensitive information such as an image of ATM machine while a bystander is doing some transactions.

Researchers have proposed several solutions to mitigate this issue. These include explicitly obtaining consent to record people in public [15], [16], wearing special tags on clothes [17] or using gestures [18] which can be recognized by the

device and thus, automatically stops recording/removes the recording for those bystanders. Although, these approach may work in theory but may be quite hard to implement in practice. More promising approaches make use of deep-learning and image processing algorithms to remove the sensitive content. E. Zarepour et al. [19] propose a methodology that uses deep convolution neural networks (CNN) to remove sensitive images of people, objects and even locations (such as bedroom, bathroom etc.) from the data collected with over 70% accuracy. Other deep learning approaches propose visual blurring of images [20] or distorting them or replacing sensitive images with clip art that can be applied to both photos and video streams [21].

B. Re-identification and Linkage

Researchers have shown that behavioral inferences about the user's activity can be made even when the activity data is in the aggregated form [4]. In addition, since certain behavior attributes are often unique to an individual such as their walking speed, movement patterns, and step length, it can be used to recognize an individual's identity from a data of daily activities [22]. Although, various anonymization techniques such as k-anonymity [23], l-diversity [24], t-closeness [25] and differential privacy [26], have been proposed by the privacy researchers, they either suffer from similarity or homogeneity attacks that can reveal individual's identify even in aggregated form or may be unsuitable for the wearable domain.

To mitigate some of these challenges, researchers have proposed the use of anonymous user ID that do not reveal any information about the actual user [11] or having identities that work in a specific context [27] (such as having a different user ID for sharing between peers and another different user ID for information exchange between user and other devices). Having anonymous ID does not mean that the user may never be identified, rather the users real identity may be known to specific application acting on the behalf of the user and unknown to the rest of the world. Thus, more research is needed for strong anonymization algorithms suitable for the wearable devices to protect users identity in real-time and possible re-identification in aggregated data.

C. Workplace adaptation and Ethical issues

Despite of several health benefits of the fitness trackers and other wearable devices, there has been a resistance by several organizations for using the wearable devices at the workplace [28], [29]. Some of the main reasons against the adaptation of wearable devices at workplace are: 1) fear of employees to be tracked by their employers, 2) safety of the device in critical environments such as oil and gas industries, 3) interference or distraction caused by the device and 4) the device itself may record sensitive information at the workplace. In addition to establishing or changing the policies that governs the appropriate use and ethics of wearable devices in the workplace, data anonymization and anonymous ID described above may mitigate some of these challenges such as that of user tracking by the employer.

D. Issues Pertaining to Human Behavior

Equipped with powerful sensors for fitness, activity and sleep tracking, wearable devices give users the power to take control of monitoring their health continuously. However, studies have shown that self-tracking can also become an obsession and thus, can do more harm than good. Users have reported various symptoms such as a sense of helplessness and stress when they forget their wearable device at home or when they forget to start their activity monitoring manually while exercising [30], [31]. More studies are required to determine what factors contribute to this behavior and how people can maintain a healthy balance between self-tracking and exercising. Additionally, the manufacturers of the wearable devices need to break the taboo surrounding the fitness culture for the people with disabilities by means of appropriate advertising and presenting case studies [32].

E. Design Issues

A major problem with some of the wearable devices is that they lack certain physical cues that makes them hard to distinguish from similar devices. For e.g., Google glass or other similar looking wearable devices may record bystanders in public without the people even noticing that they are being recorded [15], [17]. Researchers suggest that these devices include certain audio/visual cues, such as a red-blinking light indicating that the device is capable of recording or to simply distinguish it from a regular artifact [33], [34].

Additionally, researchers and manufacturers need to explore ways of enabling real-time processing of the sensitive images and video on the device itself without having to require additional software to do the processing. This would mitigate privacy threat to both the user and the bystanders. A. Mathur et al. [35] propose a novel wearable device known as *DeepEye*, capable of processing sensitive images using deep learning (CNN) in real-time. Such devices, may revolutionize the lifelogging activity and also, mitigate some of the privacy challenges associated with it.

Finally, manufacturers of wearable devices should pay more attention to making wearable devices more accessible for people with disabilities and the elderly so that they can also reap the benefits of the various features that these devices have to offer.

F. Data Jurisdiction and Privacy Policies

Data Jurisdiction plays an important role in governing the freedom or level of access control given to the citizens of that country regarding their data. Some countries have very stringent surveillance laws while other have no data privacy laws at all [36].

Besides data jurisdiction, some device manufactures make *vague* or *ambiguous privacy policies* so that they have the maximum control or ownership of the users' data. Paul and Irvine [37] analyzed privacy policy of four popular fitness tracking organizations (Fitbit, Nike+, Jawbone, and BASIS). They found that almost all of the services claimed to have an ownership of the user's health data with only Nike+ allowing

TABLE I
SOME OF THE SOLUTIONS TO PRIVACY CHALLENGES FOR WEARABLE DEVICES IN THE LITERATURE.

Methodology	Description
Audio/Visual cues [16]	E.g. such as beep noise or flashing red light [34] on the wearable device to indicate that the device is capable of recording.
Opt-out Markers [17]	Physical tags on the clothing that can be detecting by the recording device to indicate a person does not wish to be recorded in public.
Gesture-based [18]	The recording device is pre-configured to recognize certain gestures to stop recording an individual.
GPS-based Blocking [33]	Prohibiting the recording based on GPS location of the lifelogger.
Anonymous ID [11], contextual identity [27]	To mask the identity of the user during data exchange.
k-anonymity [14], l-diversity [24], differential privacy [26]	Data anonymization algorithm to avoid user re-identification in aggregated data
Deep learning approaches [19] [21] [20]	Uses deep learning and image processing algorithms to automatically morph or remove sensitive images in lifelog data or processes them in real time [35].

users to delete their data completely at the time their work was published. The authors also found that surprisingly none of these organizations notified the users of any change to their privacy policy explicitly. The users are recommended at the best to "keep visiting the website for changes." One possible solution to mitigate the issues with privacy policies and data jurisdiction would be to make use of the Block chain technology. Block chain technology that has been gaining momentum due to its resilience against attacks. A. Banerje et. al [38] present a framework known as *LinkShare* to automatically enforce compliance with privacy policies to protect user's personal information by making use of block-chain technology. The framework uses natural language processing (NLP) to ensure compliance with the privacy policies and only the transactions that obey those policies are allowed to be stored on the block-chain where they cannot be tampered with.

IV. DISCUSSION AND CONCLUSIONS

This paper highlighted some of the major privacy challenges and open issues that persevere the wearable landscape. Table I summarizes some of the solutions discussed in the literature to mitigate privacy concerns from the use of wearable devices. It is evident that no single solution can solve all the privacy challenges in the wearable domain. What is rather needed, is a holistic approach jointly lead by government, manufacturers and the research community to develop common principles and practices for privacy protection and anonymization of the user data. More importantly, user education and awareness remains an important issue when it comes to privacy threats arising from the wearable devices. In addition, there is a dire need to simplify the privacy policies such as P3P policy [39] and Model Privacy Form [40], to make it easier for end-users to comprehend them easily and make an informed choice before giving their consent. Moving forward, block-chain and deep learning approaches discussed in the paper show a promising solution to many of the challenges. We believe that the issues outlined in this paper would be a useful for the research community to further explore the wearable landscape and to mitigate the challenges that remain.

ACKNOWLEDGMENT

This work is supported in part from National Science Foundation (NSF) under the grants 1821560 and 1723765.

REFERENCES

[1] Vandrico Inc, "Wearable Technology Database." [Online]. Available: https://vandrico.com/wearables/wearable-technology-database

[2] B. Marr, "15 noteworthy facts about Wearables in 2016," 2016. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2016/03/18/15-mind-boggling-facts-about-wearables-in-2016/

[3] A. Raij, A. Ghosh, S. Kumar, and M. Srivastava, "Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: ACM, 2011, pp. 11–20. [Online]. Available: http://doi.acm.org/10.1145/1978942.1978945

[4] T. Yan, Y. Lu, and N. Zhang, "Privacy disclosure from wearable devices," in *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing*, ser. PAMCO '15. New York, NY, USA: ACM, 2015, pp. 13–18. [Online]. Available: http://doi.acm.org/10.1145/2757302.2757306

[5] L. Hagen, "Overcoming the privacy challenges of wearable devices: A study on the role of digital literacy," in *Proceedings of the 18th Annual International Conference on Digital Government Research*, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 598–599. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085254

[6] E. S. Udoh and A. Alkharashi, "Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students," *FTC 2016 - Proceedings of Future Technologies Conference*, no. December, pp. 926–931, 2017.

[7] B. Lowens, V. Motti, and K. Caine, "Wearable privacy: Skeletons in the data closet," *Proceedings of the 2017 International Conference on Healthcare Informatics*, 2017.

[8] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890. [Online]. Available: http://www.jstor.org/stable/1321160

[9] Merriam-Webster, "Privacy — Definition of Privacy by Merriam-Webster." [Online]. Available: https://www.merriam-webster.com/dictionary/privacy

[10] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, no. 5, pp. 477–558, 2006. [Online]. Available: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf

[11] R. Di Pietro and L. V. Mancini, "Security and privacy issues of handheld and wearable wireless devices," *Communications of the ACM*, vol. 46, no. 9, pp. 74–79, sep 2003. [Online]. Available: http://portal.acm.org/citation.cfm?doid=903893.903897

[12] V. G. Motti and K. Caine, "Users' privacy concerns about wearables," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 231–244.

[13] M. Becker, C. Matt, T. Widjaja, and T. Hess, "Understanding privacy risk perceptions of consumer health wearables - an empirical taxonomy," in *Proceedings of the International Conference on Information Systems - Transforming Society with Digital Innovation, ICIS 2017, Seoul, South Korea, December 10-13, 2017*, 2017. [Online]. Available: http://aisel.aisnet.org/icis2017/IT-and-Healthcare/Presentations/12

[14] A. Perez and S. Zeadally, "Privacy Issues and Solutions for Consumer Wearables," *IT Professional*, pp. 1–13, 2017.

[15] S. Singhal, C. Neustaedter, T. Schiphorst, A. Tang, A. Patra, and R. Pan, "You are being watched: Bystanders' perspective on the use of camera devices in public spaces," in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '16. New York, NY, USA: ACM, 2016, pp. 3197–3203. [Online]. Available: http://doi.acm.org/10.1145/2851581.2892522

[16] M. S. Ferdous, S. Chowdhury, and J. M. Jose, "Analysing privacy in visual lifelogging," *Pervasive and Mobile Computing*, vol. 40, pp. 430 – 449, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119216301894

[17] T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies," in *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2377–2386. [Online]. Available: http://doi.acm.org/10.1145/2556288.2557352

[18] M. Koelle, S. Ananthanarayan, S. Czupalla, W. Heuten, and S. Boll, "Your smart glasses' camera bothers me!: Exploring opt-in and opt-out gestures for privacy mediation," in *Proceedings of the 10th Nordic Conference on Human-Computer Interaction*, ser. NordiCHI '18. New York, NY, USA: ACM, 2018, pp. 473–481. [Online]. Available: http://doi.acm.org/10.1145/3240167.3240174

[19] E. Zarepour, M. Hosseini, S. S. Kanhere, and A. Sowmya, "A context-based privacy preserving framework for wearable visual lifeloggers," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, March 2016, pp. 1–4.

[20] S. Wang, S. S. Cheung, and Y. Luo, "Wearable privacy protection with visual bubble," in *2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW)*, July 2016, pp. 1–6.

[21] E. T. Hassan, R. Hasan, P. Shaffer, D. Crandall, and A. Kapadia, "Cartooning for enhanced privacy in lifelogging and streaming videos," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, July 2017, pp. 1333–1342.

[22] S. A. Elkader, M. Barlow, and E. Lakshika, "Wearable sensors for recognizing individuals undertaking daily activities," in *Proceedings of the 2018 ACM International Symposium on Wearable Computers*, ser. ISWC '18. New York, NY, USA: ACM, 2018, pp. 64–67. [Online]. Available: http://doi.acm.org/10.1145/3267242.3267245

[23] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002. [Online]. Available: http://dx.doi.org/10.1142/S0218488502001648

[24] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "L-diversity: privacy beyond k-anonymity," in *22nd International Conference on Data Engineering (ICDE'06)*, April 2006, pp. 24–24.

[25] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd International Conference on Data Engineering*, April 2007, pp. 106–115.

[26] C. Dwork, "Differential privacy," in *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ser. ICALP'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–12. [Online]. Available: http://dx.doi.org/10.1007/11787006_1

[27] R. Kravets, G. S. Tuncay, and H. Sundaram, "For your eyes only," in *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*, ser. MCS '15. New York, NY, USA: ACM, 2015, pp. 28–35. [Online]. Available: http://doi.acm.org/10.1145/2802130.2802137

[28] J. Mark C. Schall, R. F. Sesek, and L. A. Cavuoto, "Barriers to the adoption of wearable sensors in the workplace: A survey of occupational safety and health professionals," *Human Factors*, vol. 60, no. 3, pp. 351–362, 2018, pMID: 29320232. [Online]. Available: https://doi.org/10.1177/0018720817753907

[29] N. Gorm and I. Shklovski, "Sharing steps in the workplace: Changing privacy concerns over time," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 4315–4319. [Online]. Available: http://doi.acm.org/10.1145/2858036.2858352

[30] A. Barton, "Happier and healthier? Getting at the root of our self-tracking obsession," feb 2017. [Online]. Available: https://www.theglobeandmail.com/life/health-and-fitness/fitness/happier-and-healthier-getting-at-the-root-of-our-self-trackingobsession/article34120896/

[31] K. Penningroth, "The darker side of fitness wearables," nov 2016. [Online]. Available: http://www.statepress.com/article/2016/02/nothing-comes-without-drawbacks-not-even-your-fitbit

[32] J. P. Elman, ""find your fit": Wearable technology and the cultural politics of disability," *New Media & Society*, vol. 20, no. 10, pp. 3760–3777, 2018. [Online]. Available: https://doi.org/10.1177/1461444818760312

[33] R. Hoyle, R. Templeman, S. Armes, D. Anthony, D. Crandall, and A. Kapadia, "Privacy behaviors of lifeloggers using wearable cameras," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '14. New York, NY, USA: ACM, 2014, pp. 571–582. [Online]. Available: http://doi.acm.org/10.1145/2632048.2632079

[34] A. Ashok, V. Nguyen, M. Gruteser, N. Mandayam, W. Yuan, and K. Dana, "Do not share!: Invisible light beacons for signaling preferences to privacy-respecting cameras," in *Proceedings of the 1st ACM MobiCom Workshop on Visible Light Communication Systems*, ser. VLCS '14. New York, NY, USA: ACM, 2014, pp. 39–44. [Online]. Available: http://doi.acm.org/10.1145/2643164.2643168

[35] A. Mathur, N. D. Lane, S. Bhattacharya, A. Boran, C. Forlivesi, and F. Kawsar, "Deepeye: Resource efficient local execution of multiple deep vision models using wearable commodity hardware," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '17. New York, NY, USA: ACM, 2017, pp. 68–81. [Online]. Available: http://doi.acm.org/10.1145/3081333.3081359

[36] Chilala, "Which countries have the worst data retention laws? - Best VPNz," 2015. [Online]. Available: https://www.bestvpnz.com/which-countries-have-the-worst-data-retention-laws/

[37] G. Paul and J. Irvine, "Privacy implications of wearable health devices," in *Proceedings of the 7th International Conference on Security of Information and Networks*, ser. SIN '14. New York, NY, USA: ACM, 2014, pp. 117:117–117:121. [Online]. Available: http://doi.acm.org/10.1145/2659651.2659683

[38] A. Banerjee and K. P. Joshi, "Link before you share: Managing privacy policies through blockchain," in *2017 IEEE International Conference on Big Data (Big Data)*, Dec 2017, pp. 4438–4447.

[39] W3C, "P3P: The Platform for Privacy Preferences." [Online]. Available: https://www.w3.org/P3P/

[40] Gramm-Leach-Bliley, "Final Model Privacy Form Under the Gramm-Leach-Bliley Act A Small Entity Compliance Guide," Federal Trade Commission, Tech. Rep., 2009. [Online]. Available: http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_FR.pdf.