“Revoked just now!” Users’ Behaviors toward Fitness-Data Sharing with Third-Party Applications

Noé Zufferey
University of Lausanne
Switzerland
noe.zufferey@unil.ch

Kavous Salehzadeh Niksirat
University of Lausanne
Switzerland
kavous.salehzadehniksirat@unil.ch

Mathias Humbert
University of Lausanne
Switzerland
mathias.humbert@unil.ch

Kévin Huguenin
University of Lausanne
Switzerland
kevin.huguenin@unil.ch

ABSTRACT

The number of users of wearable activity trackers (WATs) has rapidly increased over the last decade. Although these devices enable their users to monitor their activities and health, they also raise new security and privacy concerns, given the sensitive data (e.g., steps, heart rate) they collect and the information that can be inferred from this data (e.g., diseases). In addition to sharing with the service providers (e.g., Fitbit), WAT users can share their fitness data with third-party applications (TPAs) and individuals. Understanding how and with whom users share their fitness data and what kind of approaches they take to preserve their privacy are key to assessing the underlying privacy risks and to further designing appropriate privacy-enhancing techniques. In this work, we perform, through a large-scale survey of $N = 628$ WAT users, the first quantitative and qualitative analysis of users’ awareness, understanding, attitudes, and behaviors toward fitness-data sharing with TPAs and individuals. By asking these users to draw their thoughts, we explore, in particular, users’ practices and *actual* behaviors toward fitness-data sharing and their *mental models*. Our empirical results show that about half of WAT users underestimate the number of TPAs to which they have granted access to their data, and 63% share data with at least one TPA that they do not actively use (anymore). Furthermore, 29% of the users do not revoke TPA access to their data because they forget they gave access to it in the first place, and 8% were not even aware they could revoke access to their data. Finally, their mental models, as well as some of their answers, demonstrate substantial gaps in their understanding of the data-sharing process. Importantly, 67% of the respondents think that TPAs cannot access the fitness data that was collected before they granted access to it, whereas TPAs actually can do this

LINK

https://petsymposium.org/popets/2023/popets-2023-0004.php

REFERENCES

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Symp. on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 137–153. https://doi.org/10.1109/SP.2017.65

[2] Seyed Hossein Ahmadinejad and Philip W.L. Fong. 2013. On the Feasibility of Inference Attacks by Third-Party Extensions to Social Network Systems. In *Proc. of the ACM on Asia Conf. on Computer and Communications Security (AsiaCCS)*. ACM Press, Hangzhou, China, 161. https://doi.org/10.1145/2484313.2484333

[3] Seyed Hossein Ahmadinejad, Philip W.L. Fong, and Reihaneh Safavi-Naini. 2016. Privacy and Utility of Inference Control Mechanisms for Social Computing Applications. In *Proc. of the ACM on Asia Conf. on Computer and Communications Security (AsiaCCS)*. ACM, Xi'an China, 829–840. https://doi.org/10.1145/2897845.2897878

[4] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There Is Nothing That I Need to Keep Secret": Sharing Practices and Concerns of Wearable Fitness Data. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, USA, 421–434.

[5] Pauline Anthonysamy, Awais Rashid, James Walkerdine, Phil Greenwood, and Georgios Larkou. 2012. Collaborative Privacy Management for Third-Party Applications in Online Social Networks. In *Proc. of the Workshop on Privacy and Security in Online Social Media (PSOSM)*. ACM Press, Lyon, France, 1–4. https://doi.org/10.1145/2185354.2185359

[6] Apple. 2020. HealthKit | Apple Developer Documentation. https://developer.apple.com/documentation/healthkit.

[7] Apple. 2022. Legal - Data & Privacy - Apple. https://www.apple.com/legal/privacy/data/en/health-app/.

[8] Amid Ayobi, Paul Marshall, Anna L. Cox, and Yunan Chen. 2017. Quantifying the Body and Caring for the Mind: Self-Tracking in Multiple Sclerosis. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, New York, NY, USA, 6889–6901. https://doi.org/10.1145/3025453.3025869

[9] Igor Bilogrevic and Martin Ortlieb. 2016. "If You Put All The Pieces Together...": Attitudes Towards Data Combination and Sharing Across Services and Companies. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. ACM, San Jose California USA, 5215–5227. https://doi.org/10.1145/2858036.2858432

[10] Alex Bowden. 2018. Cyclist Who Had Five Bikes Stolen Says Thieves Are Looking for Quick Times on Strava to Try and Find High-End Bikes – Warns Other Users to Check Their Privacy Settings. https://road.cc/content/news/248798-cyclist-who-had-five-bikes-stolen-says-thieves-are-looking-quick-times-strava.

[11] Business Wire. 2020. Shipments of Wearable Devices Leap to 125 Million Units, Up 35.1% in the Third Quarter, According to IDC. https://www.businesswire.com/news/home/20201202005304/en/Shipments-of-Wearable-Devices-Leap-to-125-Million-Units-Up-35.1-in-the-Third-Quarter-According-to-IDC.

[12] Angela Chen. 2018. What Happens When Life Insurance Companies Track Fitness Data? https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health.

[13] Yuan Cheng, Jaehong Park, and Ravi Sandhu. 2013. Preserving User Privacy from Third-Party Applications in Online Social Networks. In *Proc. of the International Conference on World Wide Web - WWW '13 Companion*. ACM Press, Rio de Janeiro, Brazil, 723–728. https://doi.org/10.1145/2487788.2488032

[14] Eun Kyoung Choe, Nicole B Lee, Bongshin Lee, Wanda Pratt, and Julie A Kientz. 2014. Understanding Quantified-Selfers' Practices in Collecting and Exploring Personal Data. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, Toronto Ontario Canada, 1143–1152. https://doi.org/10.1145/2556288.2557372

[15] Blaine Cook and Chris Messina. 2012. OAuth 2.0 — OAuth. https://oauth.net/2/.

[16] Kenan Degirmenci. 2020. Mobile Users' Information Privacy Concerns and the Role of App Permission Requests. *International Journal of Information Management* 50 (Feb. 2020), 261–272. https://doi.org/10.1016/j.ijinfomgt.2019.05.010

[17] Jaime Delgado, Eva Rodríguez, and Silvia Llorente. 2010. User's Privacy in Applications Provided through Social Networks. In *Proc. of the ACM SIGMM Workshop on Social Media (WSM)*. ACM Press, Firenze, Italy, 39. https://doi.org/10.1145/1878151.1878163

[18] Simon Eberz, Giulio Lovisotto, Andrea Patane, Marta Kwiatkowska, Vincent Lenders, and Ivan Martinovic. 2018. When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts. In *S&P*. IEEE, San Francisco, CA, 889–905. https://doi.org/10.1109/SP.2018.00053

[19] Simon Eberz, Nicola Paoletti, Marc Roeschlin, Andrea Patani, Marta Kwiatkowska, and Ivan Martinovic. 2017. Broken Hearted: How To Attack ECG Biometrics. In *Proc. of the Network and Distributed System Security Symp. (NDSS)*. Internet Society, San Diego, CA. https://doi.org/10.14722/ndss.2017.23408

[20] Haroon Elahi, Guojun Wang, and Dongqing Xie. 2017. Assessing Privacy Behaviors of Smartphone Users in the Context of Data Over-Collection Problem: An Exploratory Study. In *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, San Francisco, CA, 1–8. https://doi.org/10.1109/UIC-ATC.2017.8397613

[21] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2014. TaintDroid: An Information Flow Tracking System for Real-Time Privacy Monitoring on Smartphones. *Commun. ACM* 57, 3 (March 2014), 99–106. https://doi.org/10.1145/2494522

[22] Daniel A. Epstein, Alan Borning, and James Fogarty. 2013. Fine-Grained Sharing of Sensed Physical Activity: A Value Sensitive Approach. In *Proc. of the ACM Int'l Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp)*. Association for Computing Machinery, New York, NY, USA, 489–498. https://doi.org/10.1145/2493432.2493433

[23] Shehroze Farooqi and Zubair Shafiq. 2019. Measurement and Early Detection of Third-Party Application Abuse on Twitter. In *The World Wide Web Conference on - WWW '19*. ACM Press, San Francisco, CA, USA, 448–458. https://doi.org/10.1145/3308558.3313515

[24] Christina Farr. 2019. Fitbit Has a New Health Tracker, but You Can Only Get It through Your Employer or Insurer. https://www.cnbc.com/2019/02/08/fitbit-releases-insprire-for-employers.html.

[25] Fitbit. 2020. Fitbit SDK. https://dev.fitbit.com/.

[26] Marco Furini, Silvia Mirri, Manuela Montangero, and Catia Prandi. 2020. Can IoT Wearable Devices Feed Frugal Innovation?. In *Proc. of the Workshop on Experiences with the Design and Implementation of Frugal Smart Objects (FRUGAL THINGS)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3410670.3410861

[27] Sandra Gabriele and Sonia Chiasson. 2020. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, Honolulu HI USA, 1–12. https://doi.org/10.1145/3313831.3376651

[28] Sandra Gabriele and Sonia Chiasson. 2020. Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376651

[29] Garmin. 2020. Overview | Garmin Connect Developer Program | Garmin Developers. https://developer.garmin.com/gc-developer-program/overview/.

[30] Jennifer Golbeck and Matthew Mauriello. 2016. User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns. *Future Internet* 8, 4 (March 2016), 9. https://doi.org/10.3390/fi8020009

[31] Nanna Gorm and Irina Shklovski. 2016. Sharing Steps in the Workplace: Changing Privacy Concerns Over Time. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, San Jose, California, USA, 4315–4319. https://doi.org/10.1145/2858036.2858352

[32] Gabriel Guo, Hanbin Zhang, Liuyi Yao, Huining Li, Chenhan Xu, Zhengxiong Li, and Wenyao Xu. 2022. MSLife: Digital Behavioral Phenotyping of Multiple Sclerosis Symptoms in the Wild Using Wearables and Graph-Based Statistical Analysis. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (Dec. 2022), 158:1–158:35. https://doi.org/10.1145/3494970

[33] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-See: An Interactive Tool for Visualizing Privacy Policies. In *Proc. of the Workshop on Privacy in the Electronic Society (WPES)*. Association for Computing Machinery, New York, NY, USA, 57–71. https://doi.org/10.1145/3411497.3420221

[34] Mario A. Gutierrez, Michelle L. Fast, Anne H. Ngu, and Byron J. Gao. 2016. Real-Time Prediction of Blood Alcohol Content Using Smartwatch Sensor Data. In *Smart Health*, Xiaolong Zheng, Daniel Dajun Zeng, Hsinchun Chen, and Scott J. Leischow (Eds.). Springer International Publishing, 175–186.

[35] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. 2018. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. In *27th USENIX Security Symposium (USENIX Security 18)*. 531–548.

[36] James J Heckman. 1990. Selection bias and self-selection. In *Econometrics*. Springer, 201–224.

[37] Alex Hern. 2018. Fitness Tracking App Strava Gives Away Location of Secret US Army Bases. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[38] Robert P Hirten, Matteo Danieletto, Lewis Tomalin, Katie Hyewon Choi, Eddye Golden, Sparshdeep Kaur, Drew Helmus, Anthony Biello, Alexander Charney, Riccardo Miotto, Benjamin S Glicksberg, Ismail Nabeel, Judith Aberg, David Reich, Dennis Charney, Laurie Keefer, Mayte Suarez-Farinas, Girish N Nadkarni, and Zahi A Fayad. 2021. Physiological Data from a Wearable Device Identifies SARS-CoV-2 Infection and Symptoms and Predicts COVID-19 Diagnosis: Observational Study. *Journal of Medical Internet Research* (2021), 36.

[39] Milena Janic, Jan Pieter Wijbenga, and Thijs Veugen. 2013. Transparency Enhancing Tools (TETs): An Overview. In *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, New Orleans, LA, 18–25. https://doi.org/10.1109/STAST.2013.11

[40] David Jonassen and Young Hoan Cho. 2008. Externalizing Mental Models with Mindtools. In *Understanding Models for Learning and Instruction*, Dirk Ifenthaler,

Pablo Pirnay-Dummer, and J. Michael Spector (Eds.). Springer US, Boston, MA, 145–159. https://doi.org/10.1007/978-0-387-76898-4_7

[41] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. USENIX Association, Ottawa, Canada, 39–52.

[42] Jennifer King, Airi Lampinen, and Alex Smolen. 2011. Privacy: Is There an App for That?. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. ACM Press, Pittsburgh, Pennsylvania, 1. https://doi.org/10.1145/2078827.2078843

[43] Hanna Krasnova, Nicole Eling, Oleg Schneider, Helena Wenninger, Thomas Widjaja, and Peter Buxmann. 2013. Does This App Ask For Too Much Data? The Role Of Privacy Perceptions In User Behavior Towards Facebook Applications And Permission Dialogs. *ECIS* (2013), 14.

[44] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *Proc. of the IEEE Symp. on Security and Privacy (S&P)*. IEEE, San Francisco, CA, USA, 1138–1155. https://doi.org/10.1109/SP.2019.00060

[45] Preeti Kumari, Lini Mathew, and Poonam Syal. 2017. Increasing Trend of Wearables and Multimodal Interface for Human Activity Monitoring: A Review. *Biosensors and Bioelectronics* 90 (April 2017), 298–307. https://doi.org/10.1016/j.bios.2016.12.001

[46] He Li, Jing Wu, Yiwen Gao, and Yao Shi. 2016. Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective. *International Journal of Medical Informatics* 88 (April 2016), 8–17. https://doi.org/10.1016/j.ijmedinf.2015.12.010

[47] Wanpeng Li and Chris J. Mitchell. 2014. Security Issues in OAuth 2.0 SSO Implementations. In *Information Security (Lecture Notes in Computer Science)*, Sherman S. M. Chow, Jan Camenisch, Lucas C. K. Hui, and Siu Ming Yiu (Eds.). Springer International Publishing, Cham, 529–541. https://doi.org/10.1007/978-3-319-13257-0_34

[48] X. Li, J. Xu, Z. Zhang, X. Lan, and Y. Wang. 2020. Modular Security Analysis of OAuth 2.0 in the Three-Party Setting. In *Euro S&P*. 276–293. https://doi.org/10.1109/EuroSP48549.2020.00025

[49] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li. 2018. Deep Learning Based Inference of Private Information Using Embedded Sensors in Smart Devices. *IEEE Network* 32, 4 (July 2018), 8–14. https://doi.org/10.1109/MNET.2018.1700349

[50] Yuting Liao. 2019. Sharing Personal Health Information on Social Media: Balancing Self-presentation and Privacy. In *Proc. of the Int'l Conf. on Social Media and Society (SMSociety)*. Association for Computing Machinery, New York, NY, USA, 194–204. https://doi.org/10.1145/3328529.3328560

[51] Andrés Lucero. 2015. Using affinity diagrams to evaluate interactive prototypes. In *IFIP conference on human-computer interaction*. Springer, 231–248.

[52] Deborah Lupton. 2021. "Sharing Is Caring:" Australian Self-Trackers' Concepts and Practices of Personal Data Sharing and Privacy. *Frontiers in Digital Health* 3 (2021). https://doi.org/10.3389/fdgth.2021.649275

[53] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. 2020. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. USENIX Association, USA, 341–358.

[54] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. 2016. Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms. In *Proc. of the ACM on Asia Conf. on Computer and Communications Security (AsiaCCS)*. ACM, Xi'an, China, 795–806. https://doi.org/10.1145/2897845.2897905

[55] Anindya Maiti, Murtuza Jadliwala, Jibo He, and Igor Bilogrevic. 2015. (Smart)Watch Your Taps: Side-channel Keystroke Inference Attacks Using Smartwatches. In *Proc. of the ACM Int. Symp. on Wearable Computers (ISWC)*. ACM, Osaka, Japan, 27–30. https://doi.org/10.1145/2802083.2808397

[56] Anindya Maiti, Murtuza Jadliwala, J. He, and I. Bilogrevic. 2018. Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches. *IEEE Transactions on Mobile Computing* 17, 9 (Sept. 2018), 2180–2194. https://doi.org/10.1109/TMC.2018.2794984

[57] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355. https://doi.org/10.1287/isre.1040.0032

[58] Anna Maria Mandalari, Daniel J. Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. 2021. Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (Oct. 2021), 369–388. https://doi.org/10.2478/popets-2021-0075

[59] K. I. Manktelow and Man Cheung Chung (Eds.). 2004. *Psychology of Reasoning: Theoretical and Historical Perspectives* (first ed.). Psychology Press, Hove ; New York.

[60] Stefania Marassi and Philippa Collins. 2021. Is That Lawful? Data Privacy and Fitness Trackers in the Workplace. *International Journal of Comparative Labour Law and Industrial Relations* 37, 1 (Feb. 2021).

[61] Maximilian Marsch, Jens Grossklags, and Sameer Patil. 2021. Won't You Think of Others?: Interdependent Privacy in Smartphone App Permissions. *Proc. of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 437:1–437:35. https://doi.org/10.1145/3479581

[62] Tenga Matsuura, Ayako A. Hasegawa, Mitsuaki Akiyama, and Tatsuya Mori. 2021. Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods. In *European Symposium on Usable Security 2021*. ACM, Karlsruhe Germany, 36–47. https://doi.org/10.1145/3481357.3481515

[63] Patrick Murmann, Matthias Beckerle, Simone Fischer-Hübner, and Delphine Reinhardt. 2021. Reconciling the What, When and How of Privacy Notifications in Fitness Tracking Scenarios. *Pervasive and Mobile Computing* 77 (Oct. 2021), 101480. https://doi.org/10.1016/j.pmcj.2021.101480

[64] K. Niazmand, K. Tonn, Y. Zhao, U. M. Fietzek, F. Schroeteler, K. Ziegler, A. O. Ceballos-Baumann, and T. C. Lueth. 2011. Freezing of Gait Detection in Parkinson's Disease Using Accelerometer Based Smart Clothes. In *IEEE Biomedical Circuits and Systems Conf. (BioCAS)*. 201–204. https://doi.org/10.1109/BioCAS.2011.6107762

[65] Mehdi Nobakht, Yulei Sui, Aruna Seneviratne, and Wen Hu. 2020. PGFit: Static Permission Analysis of Health and Fitness Apps in IoT Programming Frameworks. *Journal of Network and Computer Applications* 152 (Feb. 2020), 102509. https://doi.org/10.1016/j.jnca.2019.102509

[66] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proc. on Privacy Enhancing Technologies (PoPETs)* 2018, 4 (Oct. 2018), 5–32. https://doi.org/10.1515/popets-2018-0029

[67] Stefan Palan and Christian Schitter. 2018. Prolific.Ac—A Subject Pool for Online Experiments. *Journal of Behavioral and Experimental Finance* 17 (March 2018), 22–27. https://doi.org/10.1016/j.jbef.2017.12.004

[68] Rajesh Pandey. 2020. Android 11 Will Automatically Revoke Permissions from Unused Apps. https://www.neowin.net/news/android-11-will-automatically-revoke-permissions-from-unused-apps/.

[69] Jamie Pinchot and Donna Cellante. 2021. Privacy Concerns and Data Sharing Habits of Personal Fitness Information Collected via Activity Trackers. *JISAR* 14, 2 (June 2021), 4.

[70] Rocket Fuel. 2014. *'Quantified Self' Digital Tools: A CPG Marketing Opportunity*. Technical Report. Rocket Fuel.

[71] Christopher Rowl. 2019. With Fitness Trackers in the Workplace, Bosses Can Monitor Your Every Step - and Possibly More. https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step–and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html.

[72] Mohd Sabra, Anindya Maiti, and Murtuza Jadliwala. 2018. Keystroke Inference Using Ambient Light Sensor on Wrist-Wearables: A Feasibility Study. In *Proc. of the ACM Workshop on Wearable Systems and Applications (WearSys)*. ACM, Munich, Germany, 21–26. https://doi.org/10.1145/3211960.3211973

[73] Johnny Saldana. 2021. *The Coding Manual for Qualitative Researchers* (4th ed ed.). SAGE Publishing, Thousand Oaks, California.

[74] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. 2019. Understanding the Impact of Information Representation on Willingness to Share Information. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/3290605.3300753

[75] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. 2019. Understanding the Impact of Information Representation on Willingness to Share Information. In *Proc. of the Conf. on Human Factors in Computing Systems (CHI)*. ACM, Glasgow, Scotland Uk, 1–6. https://doi.org/10.1145/3290605.3300753

[76] Mohamed Shehab, Said Marouf, and Christopher Hudel. 2011. ROAuth: Recommendation Based Open Authorization. In *Proc. of the USENIX Symp. on Usable Privacy and Security (SOUPS)*. ACM Press, Pittsburgh, Pennsylvania, 1. https://doi.org/10.1145/2078827.2078842

[77] Anita Valanju Shelgikar, Patricia F. Anderson, and Marc R. Stephens. 2016. Sleep Tracking, Wearable Technology, and Opportunities for Research and Clinical Care. *Chest* 150, 3 (Sept. 2016), 732–743. https://doi.org/10.1016/j.chest.2016.04.016

[78] Sheng Shen, He Wang, and Romit Roy Choudhury. 2016. I Am a Smartwatch and I Can Track My User's Arm. In *Proc. of the Annual Int. Conf. on Mobile Systems, Applications, and Services (MobiSys)*. ACM, Singapore, Singapore, 85–96. https://doi.org/10.1145/2906388.2906407

[79] Muhammad Shoaib, Ozlem Durmaz Incel, Hans Scholten, and Paul Havinga. 2018. SmokeSense: Online Activity Recognition Framework on Smartwatches. In *Mobile Computing, Applications, and Services*, Kazuya Murao, Ren Ohmura, Sozo Inoue, and Yusuke Gotoh (Eds.). Vol. 240. Springer International Publishing, Cham, 106–124. https://doi.org/10.1007/978-3-319-90740-6_7

[80] Stephanie L. Silveira, Jessica F. Baird, and Robert W. Motl. 2021. Rates, Patterns, and Correlates of Fitness Tracker Use among Older Adults with Multiple Sclerosis. *Disability and Health Journal* 14, 1 (Jan. 2021), 100966. https://doi.org/10.1016/j.dhjo.2020.100966

[81] Statista. 2022. Wearable Band Market Share in North America by Vendor 2018-2020. https://www.statista.com/statistics/1042044/north-america-quarterly-wearable-band-market-share-by-vendor/.

[82] Etye Steinberg. 2021. Run for Your Life: The Ethics of Behavioral Tracking in Insurance. *Journal of Business Ethics* (June 2021). https://doi.org/10.1007/s10551-021-04863-8

[83] Ilaria Torre, Frosina Koceva, Odnan Ref Sanchez, and Giovanni Adorni. 2016. Fitness Trackers and Wearable Devices: How to Prevent Inference Risks?. In *Proc. of the EAI Conf. on Body Area Networks (BODYNETS)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, 125–131.

[84] Ilaria Torre, Odnan Ref Sanchez, Frosina Koceva, and Giovanni Adorni. 2018. Supporting Users to Take Informed Decisions on Privacy Settings of Personal Devices. *Personal and Ubiquitous Computing* 22, 2 (April 2018), 345–364. https://doi.org/10.1007/s00779-017-1068-3

[85] J D Tygar and Marti Hearst. 2006. Why Phishing Works. (2006), 10.

[86] Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini. 2021. Are Those Steps Worth Your Privacy?: Fitness-Tracker Users' Perceptions of Privacy and Utility. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 4 (Dec. 2021), 1–41. https://doi.org/10.1145/3494960

[87] Na Wang. 2012. Third-Party Applications' Data Practices on Facebook. In *Proc. of the CHI Conf. on Human Factors in Computing Systems (CHI)*. ACM, Austin Texas USA, 1399–1404. https://doi.org/10.1145/2212776.2212462

[88] Na Wang, Heng Xu, and Jens Grossklags. 2011. Third-Party Apps on Facebook: Privacy and the Illusion of Control. In *Proc. of the ACM Symposium on Computer Human Interaction for Management of Information Technology (CHIMIT)*. ACM Press, Cambridge, Massachusetts, 1–10. https://doi.org/10.1145/2076444.2076448

[89] Rick Wash and Emilee Rader. 2011. Influencing Mental Models of Security: A Research Agenda. In *Proc. of the Conf. New Security Paradigms Workshop (NSPW)*. Association for Computing Machinery, Marin County, California, USA, 57–66. https://doi.org/10.1145/2073276.2073283

[90] Gary M. Weiss, Jessica L. Timko, Catherine M. Gallagher, Kenichi Yoneda, and Andrew J. Schreiber. 2016. Smartwatch-Based Activity Recognition: A Machine Learning Approach. In *IEEE-EMBS Int. Conf. on Biomedical and Health Informatics (BHI)*. IEEE, Las Vegas, NV, USA, 426–429. https://doi.org/10.1109/BHI.2016.7455925

[91] Pamela Wisniewski, Heng Xu, Heather Lipford, and Emmanuel Bello-Ogunu. 2015. Facebook Apps and Tagging: The Trade-off between Personal Privacy and Engaging with Friends: Facebook Apps and Tagging: The Trade-off Between Personal Privacy and Engaging with Friends. *Journal of the Association for Information Science and Technology* 66, 9 (Sept. 2015), 1883–1896. https://doi.org/10.1002/asi.23299

[92] Verena M. Wottrich, Eva A. van Reijmersdal, and Edith G. Smit. 2018. The Privacy Trade-off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns. *Decision Support Systems* 106 (Feb. 2018), 44–52. https://doi.org/10.1016/j.dss.2017.12.003