Consumer consent, privacy and ethics of wearables

Consumer consent, privacy and ethics of wearables

Reading time 11 mins

Key Points

- A booming tech market is leading to increased concerns regarding the privacy and ethics of wearables
- Most users don’t understand the security risks
- 75% of people distrust the way their data is shared
- Identity theft drastically increased during the pandemic

- Detailed health data can be shared with insurance companies
- Data aggregation can predict future user behaviour

Ready to start developing your new product?
Call us for a quote!

Get in touch

Ben Mazur

Managing Director

Last updated Jun 12, 2023

I hope you enjoy reading this post.
If you would like us to develop your next product for you, click here

The last few years have seen massive growth in the wearable technology industry, especially with products such as smartwatches and fitness trackers. The value of the Internet of Things (IoT) market – from wearables to electronics and home appliances – is expected to reach over $153 billion by 2028 [1]. However, with interest growing in how personal data is used, consumer consent, privacy and ethics of wearables remain a leading concern.

Wearables like Garmin smartwatches, Apple Watch and Fitbit Sense are becoming more common; there's also an ethical dilemma of wearable technology that must be considered before use [2]. The security risks associated with these devices are often not well understood by users, who can find themselves inadvertently sharing sensitive information.

What are the security risks of wearable technology?

Security is an important concern for wearable technology users. In a recent smart device survey by Consumers International and the Internet Society, 75% of people distrust the way data is shared, but only 50% of respondents know how to disable data collection [3].

Wearables can be hacked and used to track your location, movements, health, financial information and more. While it's convenient to have this information on hand at all times, it also means that your personal data is vulnerable to cybercriminals who can use it to steal your identity or even blackmail you.

Some of the most common vulnerabilities in wearables include:

- Unsecure Data Transmission: This is one of the most common ways for hackers to gain access to your data, especially if you have a fitness tracker or smartwatch that sends information via Bluetooth or Wi-Fi. Cybercriminals can intercept this data and access sensitive information such as credit card details or social security numbers
- Poor Data and Access Controls: Many IoT devices collect and store data in an unencrypted format, meaning that if hackers can gain access to it, there is no protection against using the stored information. The lack of access control in these devices makes them vulnerable to intrusion from any network node that can establish a connection with the device
- Weak passwords (especially 4-digit numeric ones)

If you're using a wearable device that has been compromised by hackers or malicious software, they could potentially access your personal information without your knowledge.

Privacy and ethics of wearables issues to consider

If you've ever worn a smart device, you might have noticed that when it's paired with an app on your phone, it can silently collect information about where you go and how active you are. After putting one on for the first time, it's usually not long before it congratulates you on how far you have walked that day or even suggests that you do more exercise. This is done using GPS tracking or over WiFi if it's synced to an app on your phone.

There are a number of concerns here:

- Privacy: Wearable devices are often connected to social media accounts, so users can easily share their location with others. This could be a security concern for some people if they're worried about how their location will be used by others or if they have an issue with sharing certain information (e.g. a medical condition) about themselves online
- Data Protection: There have been reports of smart watches sending sensitive data back to manufacturers without users' consent, which could result in sensitive information being exposed to third parties without anyone knowing [4]
- Security: With biometric scanners now being used as part of payment systems and other mobile apps, there's a higher risk of cyber fraud and identity theft (which increased by 45% during the pandemic) if these systems aren't properly secured against hackers [5]

Health data is sensitive to privacy invasions

Your health data is valuable to companies who are looking for ways to improve their products and services. For example, Apple recently partnered with Stanford University to collect data about heart health from Apple Watches. This is being used in research studies which could lead to new medical devices or treatments for heart disease [6]

However, this type of research also raises questions regarding the ethics of wearable devices. For example, should companies be collecting this kind of sensitive personal information without consumer consent? And how do we know that the people analysing this information won't misuse it?

This leads us to another concern: wearables can also be used to collect data that could have implications for an individual's medical coverage or insurance rates if they do not meet certain health standards set by their employer or government agency.

One example of this is Fitbit which collects information about its users' diet, exercise habits, sleep quality and activity levels. This can be shared with doctors for diagnosis purposes, but also with insurance companies who will use that information to calculate premiums based on how healthy someone appears to be according to their activity levels [7].

Predictive analytics can compromise privacy

One type of data can be aggregated with another type to compromise privacy [8]. For example, a wearable device that monitors your heart rate could be combined with location data stored on the Internet or your browsing history. This information can then be used to determine patterns of behaviour, identify you, and reveal more than you want to share about yourself.

In some cases, it can also reveal things about yourself that you may not even know yet (e.g. whether you're pregnant). Data from wearables can be used in conjunction with other sources of personal information (e.g. social media) to predict future behaviour without any specific instruction from users themselves.

This is called "predictive analytics" and is becoming more common across many industries daily. This includes fitness trackers and mobile apps for health management purposes like diabetes monitoring software [9].

Be careful what data you share and

how it is used by companies

Considerable research is still being done in the field of wearable technology ethics [10]. They are a small part of the IoT, but with their growing popularity in recent years, it's important to consider how these devices fit into our world as consumers. If you want to purchase one, it's important to understand how companies collect and use your data.

- Read the Privacy Policy: We've become too used to ticking the "I have read the Privacy Policy" box without actually doing so (only 9% of Americans say they always read them) [11]. It's important for you to understand how your data is collected and used and how to stay protected when using a wearable device.
- Informed Consent: When you sign up for an app on your wearable device or online with a wearable company, make sure that they inform you whether they sell or share your data with other companies or third parties outside of their own organisation. You may also want to find out if there are any limits on how long they store your data or if there are any restrictions on who can access it.

Smart devices are becoming more and more common in our lives. We use them to track our health, pay bills, and manage tasks around our homes. While these devices can be convenient, they also come with some risks. What are your thoughts on privacy and ethics in the wearable industry? We would love to hear your thoughts in the comments.

References

1. Global Consumer IOT Market Size By Type, By Application, By Geographic Scope And Forecast (No. 31486). (2021, July). https://www.verifiedmarketresearch.com/product/consumer-iot-market/
2. Xue, Y. (2019). A review on intelligent wearables: Uses and risks. Human Behavior and Emerging Technologies, 1(4), 287–294. https://doi.org/10.1002/hbe2.173
3. Consumers International and the Internet Society. (2019, May). The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf
4. Landi, H. (2021, September 13). Fitbit, Apple user data exposed in breach impacting 61M fitness tracker records. Fierce Healthcare. Retrieved August 4, 2022, from https://www.fiercehealthcare.com/digital-health/fitbit-apple-user-data-exposed-breach-impacting-61m-fitness-tracker-records
5. Persen, L. (2022, May 16). Identity fraud: is a digital reshuffle needed as dangers increase? Biometric Update |. https://www.biometricupdate.com/202205/identity-fraud-is-a-digital-reshuffle-needed-as-dangers-increase
6. Muoio, D. (2021, March 25). Apple-backed Stanford study suggests iPhone, Apple Watch could. MobiHealthNews. https://www.mobihealthnews.com/news/apple-backed-stanford-study-suggests-iphone-apple-watch-could-remotely-monitor-heart-patients
7. Could Your Fitbit Data Be Used to Deny You Health Insurance? (2021, April 29). GovTech. https://www.govtech.com/health/could-your-fitbit-data-be-used-to-deny-you-health-insurance.html
8. McIntosh, V. (2019, October 25). Understanding aggregate, de-identified and anonymous data. Comparitech. https://www.comparitech.com/blog/information-security/aggregate-vs-anonymous-data/
9. OSP. (2019, August 26). AI-based Predictive Analytics To Automatically Identify Diabetes Type 2 Patients. Osplabs. https://www.osplabs.com/case-study/ai-based-predictive-analytics-to-automatically-identify-diabetes-type-2-patients/#:%7E:text=The%20AI%2Ddriven%20diabetes%20predictive,of%20de%2Didentified%20medical%20records.

10. Tu, J., & Gao, W. (2021). Ethical Considerations of Wearable Technologies in Human Research. Advanced Healthcare Materials, 10(17), 2100127. https://doi.org/10.1002/adhm.202100127
11. Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Up next

12 IoT in retail technologies that increase sales & improve customer engagement

Last updated Apr 18, 2024 | HACKS, INNOVATION, INSIGHTS, IoT, PRODUCT DESIGN, RETAIL

Top IoT in retail technologies to drive sales, engage customers, improve visibility, and lower costs.

Call us for a quote!

read more