



Controversies in Technoethics: Do the benefits of consumer wearable technology outweigh the privacy concerns?

Benjamin Saulnier [300121338]

Prof. Rocci Luppici

CMN 5115

April 14th, 2026

Introduction

The purpose of this study is to approach the growing privacy and security concerns of consumer wearable technology from a technoethical perspective. Wearable technology like smartwatches, meta glasses, and medical sensors have rapidly become adopted by the general public with worldwide shipments of these devices reaching 543 million units in 2024 alone (Doherty et al., 2025). As these technologies continue to infiltrate society, ethical issues have simultaneously arisen. What data is being collected, what is done with said data, and how informed consumers are have sparked important debates in the technoethical field. With limited legal regulations existing to govern this technology, this study will offer an in-depth analysis of the existing theories and debates around this subject. Through a systematic review of academic literature, this research paper should begin to reveal some answers to those questions and how we can best resolve these dilemmas. In the end, the goal is to explore whether the risks of adopting these technologies in everyday life is worth the perceived benefits consumers are receiving from them.

The following research questions will be used to guide by systematic review of the existing literature on technoethical debates surrounding consumer wearable technology:

- *Research Question 1: What user data is being collected by consumer wearable technology?*
- *Research Question 2: Is user data collected by producers of consumer wearable technology being handled in an ethical manner?*
- *Research Question 3: Is the data collection process of consumer wearable technology transparent enough for users to give informed consent?*

Review of Literature

The literature used in this case study covers a range of topics related to wearable technology. These devices have an extremely diverse range of applications and while this case study is focused on consumer wearable devices, some of the literature explores other fields. Leading authors such as Schaefer (2022), Weinberger (2025), and Dobson (2023) all cover wearable device applications in the field of healthcare. Meanwhile, other authors like Eckhaus (2022), Ameen (2021), and Pan (2024) focused their articles on consumer wearable devices. Both perspectives offer important insights into the technology and the related technoethical concerns. The literature on the theoretical perspectives below is essential to understanding and answering my research questions.

Surveillance Capitalism

My first research question seeks transparency in the data collection process by consumer wearable technology. This is important because of the age of “surveillance capitalism” that we are currently experiencing. This theory is described bluntly by some as “a parasitic or rogue mutation of the system that is facilitating an unprecedented, dramatic concentration of power, knowledge, and wealth into fewer and fewer hands...” with the objective to “...assert dominance over society” (Robson, p.186, 2023). This unprecedented threat is only being amplified by the unknown process of data collection presented by wearable technology.

Shoshana Zuboff is a leading author on surveillance capitalism. They provide a simpler definition when they describe it as a “new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control” (p.75, 2015). Throughout the article the author writes about social media platforms and search engines

collecting personal data to be used for nefarious purposes, however wearable technology is collecting even more personal data than these digital resources making it an even greater threat to society.

According to Mertzani & Pitt, surveillance capitalism is being normalized through social influence (2022). This normalization is partially due to the lack of transparency and complete understanding of the levels of surveillance that are occurring, and have significant consequences such as “the disruption of mental health, the diminution of self-esteem, the pursuit of spurious esteem, the exploitation of influencers, the increase of distraction, decrease of attention, and the neglect of critical thinking” (Mertzani & Pitt, p.58, 2022). The research conducted by these authors was focused on the youth and therefore these implications are how young people are being raised. If this topic is not addressed, there are fears that surveillance capitalism will become an unstoppable force in society.

Deontological Ethics

Deontology is an ethical theory focused on the actions of an individual. Rawling defines it as “an account of moral duty set out as a system of rules, as opposed to a theory that assesses the morality of our actions in accord with the impersonal value of their consequences” (p.1, 2023). In the context of my second research questions, this ethical theory is helpful in understanding whether it is morally correct to collect user data regardless of the advantages or disadvantages that it may bring.

When evaluating the ethical implications of AI technologies in surveillance capitalism, Daga et al., found that this technology disrupted the autonomy, agency, and accountability of the individual (2025). By removing these pillars of the deontological framework, humans are at risk

of their sovereignty. In the case of AI, this includes sovereignty over personal data and informed choices. There are critical parallels to draw between AI technology and wearable technology in this case, as both are presenting significant privacy risks, leading to the demise of the autonomy that deontological ethics should provide us.

While literature related to this theory regarding consumer wearable technology was scarce, one important article published by Tambone et al., called for change in the healthcare field when using emerging technologies such as wearable devices. The change that they are suggesting is “no clinical act, however technologically advanced, can be justified if carried out without informed consent, under epistemic opacity, or in contradiction with the personalist principle that underpins all authentic care” (p.8, 2025). This proposition in theory would require people providing care to get informed consent, understand the situation, and respect the patient as a self-determining entity. This would drastically change the way that wearable technology may be deployed in the medical field. If we were to approach this from a consumer perspective, a similar policy change would require all producers of wearable technology to view consumers as more than a means to a financial end, and be more transparent in regarding the collection, storage, and use of personal data.

Informed Consent

The third research question reflects upon the concept of informed consent when collecting personal data from users. This theory has been adopted as an essential perspective in the medical field, and is now being challenged with the growing presence of electronic data. Venkatachalam et al., see informed consent as a solution to privacy issues when they say the companies making these devices “should offer comprehensive and simple informed consent forms that can be read by the majority of people, especially when it comes to the risks and

uncertainties associated with wearable technology” and “we should increase the awareness of honoring and preserving the users’ right to informed consent and privacy protection among medical institutions and their medical personnel” (2023). Going forward, informed consent will be essential to ensuring users are protected from unnecessary or unwanted surveillance.

In another article published by Rehak & Kuhne, they argue there is a problem when it comes to differentiating voluntariness and consent (2022). In some circumstances, data collecting technology such as corona apps are being deployed on a compulsory basis, making consent impossible since it is mandated. By making these technologies mandatory, or using intentionally vague language, companies are “shifting from facilitating informed consent to subtly coercing user decisions, ultimately reducing transparency and weakening users’ control over their personal data” (Wang et al., 2025).

Finally, an alternative approach to informed consent is presented by Schmidt et al., as they propose that “[m]aking information accessible and understandable is not enough to give the user control over their data if they cannot set their preferences and customise their consent according to their own wishes” (p.71979, 2025). This perspective adds an additional layer to the idea of informed consent, by requiring companies to not only inform but provide control and autonomy over their own personal data.

Procedures

The method used for this research project is a case study on the technoethics of consumer wearable technology guided by a systematic literature review (SLR). To ensure rigor in the methodology, I will follow the procedure laid out by O’Brien & Mc Guckin in their 2016 paper titled *The Systematic Literature Review Method: Trials and Tribulations of Electronic Database Searching at Doctoral Level*. The type of SLR that I will be conducting is qualitative as I search

for themes within the literature found in the databases. Some of the data will be transformed into quantitative statistics for presentation of the results. While following the procedure of O'Brien & McGuckin, this SLR will be guided by the systematic review conducted by Luppicini & So (2016), *A technoethical review of commercial drone use in the context of governance, ethics, and privacy*, when building the tables and presenting the findings.

This paper examines 21 peer reviewed articles on the topic of consumer wearable devices and the ethical dilemmas that come with this emerging technology. The 21 articles were found by using the academic databases made available through the University of Ottawa. Of the 6 databases searched, articles were selected from 4 (Scopus, Web of Science, PubMed, and ProQuest). To remain consistent in the search for relevant articles, each search looked for the terms “wearable technology” or “wearable devices”, “privacy” or “security”, and “ethics” or “technoethics”. This search found a total of 104 articles across the databases, from which 21 were deemed relevant for the subject of this review. Additional search criteria limited the search to articles in English, published after 2021, limited to the Arts and Humanities field, and limited to human-focused studies.

As a part of the systematic review, peer reviewed articles on these various theoretical perspectives were also searched in the databases. The topic of surveillance capitalism was searched with only two terms “surveillance capitalism” and “tech*”. This was also limited to English, peer-reviewed articles published after 2021 and related to the field of Arts and Humanities in the databases that allowed these filters. This yielded 18 results, of which 4 were deemed relevant to the topic chosen.

The next search would focus on the deontological perspective, otherwise known as duty-based ethics. This search string was short as well, containing only the terms “deontolog*” and

“tech*”. The same filters as the previous searches were applied to this one as well. This search returned only 1 relevant result of the 5 that were seen across the 6 databases.

Finally, the third theoretical perspective that is used in this systematic literature review is informed consent. To complete my search for this theory I used the terms “informed consent” and “tech*”. Once again, the same filters were applied when available in each database. I was able to obtain 6 relevant articles of the 102 that appeared from my search results.

Once the articles are selected, they were systematically analysed and coded for themes such as the type of wearable device mentioned, the problem mentioned, and possible solutions offered. The coding for each theme is to be marked as present or not present, needing only 1 mention of the theme to be considered present. To define the themes in a simple manner, it will be based off the usage of exact language (ie. using the word “smartwatch”), or a clear suggestion of the theme (ie. mentions of policy improvement would be considered government intervention since they are responsible for passing laws). The theoretical perspectives used to analyse the texts and interpret their meanings will be surveillance capitalism, deontological ethics, and informed consent.

General Findings

Looking at *Figure 1: Theme coding table*, we can observe the themes presented by the systematic literature review and their frequency.

Figure 1: Theme coding table

Theme	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	Total
Wearable Technology Mentioned																						
Hearable						X		X							X							3
Smartwatch		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		17
Glasses		X													X							2
Other	X	X		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	19
Ethical Problem Mentioned																						
Data privacy	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	20
Health deterioration				X		X		X	X			X		X	X	X	X	X	X	X	X	13
Policy transparency	X	X	X			X	X				X	X							X			8
Other	X			X		X	X		X	X	X	X	X	X					X		X	13
Age Group Mentioned																						
Senior/ Elderly	X					X	X			X			X	X	X			X	X	X		10
Adult	X	X				X	X	X		X			X	X			X				X	10
Youth/Child		X				X						X	X	X		X					X	7
Not specified			X	X	X				X		X											5
Solution offered																						
Government intervention	X						X	X		X	X	X	X		X	X	X		X	X		12
User responsibility			X	X	X	X		X				X			X	X						8
Data collector responsibility			X			X		X		X		X	X		X	X			X	X		10
No solution offered		X						X						X				X				4
Other							X				X											2

Wearable Technology Mentioned

The first key finding that I identified is that there were more articles that mentioned healthcare-related wearable devices than consumer-related wearables. In the article by Radanliev (2025), he says that without regulation to data management “[t]his can lead to invasive targeted advertising, increased insurance premiums based on health data, or even surveillance by governments or companies.” These concerns are echoed throughout the 21 articles, as 62% of the chosen texts contained references to wearable technology focused on health deterioration. Schaefer & Ballantyne (2022) expressed how “[c]ontact tracing is a form of public health surveillance and as such raises valid concerns about privacy, liberty and proportionality.” This complicates the debate as the technology may save lives by tracing contact between infected citizens in a scenario such as COVID-19, but there is a slippery slope between the use of this technology in the public interest and for private gain. There were also concerns about the involvement of third parties in the data collection process in the healthcare field. By involving wearable devices manufactured by third party companies, there are additional risks of data breaches. “Data collected from participants’ wearables no longer involves solely the researcher, as collected data are sent to the company as part of the data collection/analysis process” (Sui et al., 2023). This focus on ethics in the healthcare sector involving wearable technology is not surprising as one researcher points out that “digital health technologies, including smartphone applications and wearables, collectively termed Consumer Health Technologies (CHTs), are now commonly integrated in citizens' daily leisure and work lives” (Weinberger et al., 2025). This demonstrates that consumer wearable devices are still in early adoption phase despite being around for close to a decade. There is also the important fact that “healthcare data records are worth up to \$250 per record, compared to \$5.40 for a payment card, due to the comprehensive

personal information they contain” (Doherty et al., p.1, 2025). With personal health data being so valuable, it proves how important this issue is to resolve. The existing literature on the technology is heavily focused on the healthcare field but there is a growing discussion about the average consumer.

When I began this systematic analysis, I suspected that most of the research would be focused on smartwatches, smartglasses, and hearables, yet my findings revealed numerous other devices that are relevant to the technoethical debate. Many articles consider smartphones as a wearable technology due to the way that users carry them wherever they go. Rees et al. noted that smartphones provide GPS location data (p.1, 2023), while O’Leary et al. found that certain smartphones can leverage sensor data (p.2, 2024). Smart clothing was mentioned as having various usages as well such as aids with cognitive impairment (Canali et al., p.151, 2024) to designer fashion statements (Hokka, p.109, 2024). The discovery of these additional devices provides a better understanding of the scale that wearable technology has achieved in society.

Ethical Problem Mentioned

One of the most important findings in this case study is the lack of awareness of the technoethical debate regarding this technology by consumers. In the article by Doherty et al., the authors found that 76% of wearable technology manufacturers “high-risk” for transparency. This goes along with their finding that 97% of consumers agree to the terms and conditions set out by these manufacturers without reading them. Despite this alarming lack of awareness, there has been a growing interest in privacy as demonstrated by Weinberger et al., who found that “all respondents considered data privacy to be relevant”, however, “all but one admitted to either not reading or only briefly scanning the privacy information (20 out of 21 participants)” (2025). Interestingly, this qualitative study identified some of the main reasoning behind this behaviour

as respondents expressed that they trusted the companies who handled their data and most had a general lack of interest in how it was being handled if they did not sense any harm to themselves. Currently, the majority of consumers are purchasing these devices for “aesthetic design, utilitarianism and sensual stimulation” (Eckhaus & Sheaffer, 2021) and are essentially ignoring the risks associated with the acquisition. It is essential that consumers are made aware of this topic since “consumer security concerns are important determinants of cutting-edge technologies adoption. Also, security concerns influence strategies companies use to keep customers’ data secure” (Ameen et al., 2021). With consumer behaviour being such an important factor in data company behaviour, the popularization of this debate may be the greatest solution to protect consumers. All hope has not been lost on this battle as Pan et al., discovered that “when the perceived necessity is low, users show more engagement with the policies” (2024). They also found “a significant correlation between the presence of threat clues and user commitment to reviewing privacy policies” (Pan et al., 2024). This means that as users are made aware of the threats that they face by adopting this technology, the more likely they are to protect themselves by examining privacy policies laid out by the companies.

Age Group Mentioned

Seniors, older adults, or elderly people were brought up most often in the context of healthcare, as adoption rates of consumer wearable technology is fairly low (Schaefer & Ballantyne, p.612, 2022). The devices were generally seen as positive innovations for seniors, since their healthcare applications are welcomed by the community. Privacy was less of a concern with this age group as “[s]tudies have shown that most patients do not feel that their privacy is violated by the use of smart sensors and are willing to give up some of their privacy for increased autonomy” (Predel et al., p.7, 2022). Increased autonomy in exchange for privacy

does have its own ethical concerns, as autonomy should be permitted to older adults without sacrificing their privacy. This age group is unique in the deployment of this technology as it can be used for additional autonomy but also “the use of Fitbits for the older demographic will likely focus more on external monitoring and risk management rather than the current focus of self-improvement, as marketed to a younger demographic” (Banerjee et al., p.247, 2025). This theme revealed how the health and fitness focus of many existing consumer wearable technology has benefited the older population.

Adults were mentioned just as often as seniors, however, the range of subjects that focused on adults was far more diverse than seniors or children. Examples of the subjects could be tracking and treating anxiety in adults (Dobson et al, 2023), deployment in work organizations (Plester et al., 2022), and even healthcare supply chains (Chang et al., 2023). In most cases, adults appeared to be the baseline group, as they overlapped with other age groups in many articles of the articles. This group is popular for this research due to their high adoption rate of wearable technology.

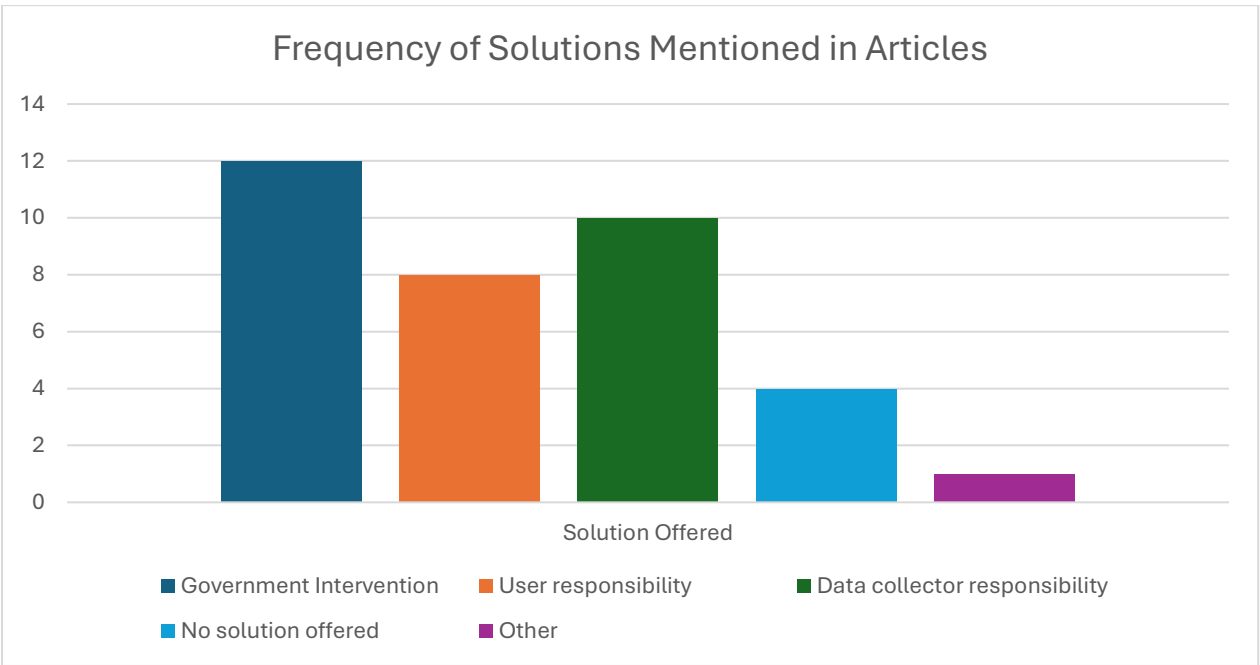
When children were mentioned, they were typically portrayed as victims of privacy violations and in need of protection. Doherty et al. provided the alarming example of “Germany’s ban on certain children’s smartwatches, which were found to function as covert listening tools, violating both child protection laws and parental trust” (p.5, 2025). The research on children and wearable usage may be limited by what Canali, et al. describe as a variable adoption date of the technology based on factors such as “whether they use other technologies (e.g., smartphones are normally gateways for wearables), where they live, and the socioeconomic status of their family” (p.9, 2022). This age group could be an area of future interest, however for the moment the limited data has prevented heavy research on these subjects.

Solutions Offered

Possibly the most concerning part of the findings is the lack of concrete solutions for the ethical issues introduced by the technology. As demonstrated by the solutions frequency chart (Figure 2), there was no clear consensus on a solution for the unique problems presented by the articles. There were three main groups with some overlap between them. The three groups being those who believe the consumers are responsible for their own protection, those who advocate for government policies to regulate, and those who believe it is the responsibility of the companies to protect their consumers. Radanliev proposes a “data-driven methodological framework that explicitly embeds transparency, accountability, and regulatory alignment” (2025) for governments to implement. To add to this argument, Schaefer & Ballantyne suggest that “with adequate governance protections and purpose limitations, mandates on contact tracing apps or wearables may be justified” (2022). These are some of the ways the articles found that governments were meant to intervene in the situation. Meanwhile, Pan et al., says that they “advocate for users to exercise increased caution and enhance their attentiveness to privacy policies, particularly when the app is deemed highly essential” (2024) demonstrating that some believe the users are meant to defend themselves. Liu (2025) challenges users to be mindful of their privacy, and Weinberger et al., argue that consumers must read privacy policies to ensure their own security before adopting this technology. Finally, there is a growing perspective that like companies must take further action to protect their consumers since they are collecting this sensitive information. Dobson et al., say that “researchers must consider that wearable companies’ practices and ethos may change at any time, with implications for the products they sell and customer treatment” (2023). This is a hopeful take on the matter, and may come across as naïve since the solution seems to be that companies will change naturally. Pan et al. were

more practical and made recommendations for app providers to adjust the way they present their products to encourage users to take the time to consider their own privacy (2024).

Figure 2: *Solution frequency chart*



Advanced Findings

In figure 3 you can find a completed technoethics coding table, complete with theoretical perspectives, historical perspectives, political perspectives, socio-cultural perspectives, economic perspectives, stakeholders’ perspectives, and the intended ends and possible side effects.

Figure 3: *TE Coding Table*

<u>Theoretical Perspectives?</u> Surveillance Capitalism Critique: The amount of sensitive data being collected by these devices is the main risk identified by the authors of the articles used for this case study. “This new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control” (Zuboff, 2015, p.75)

Deontological (duty-based) Ethics: Concerned with what people do, not with the consequences. In the context of wearable technology, we ask whether selling data, or even collecting data is immoral no matter what the consequences are for the person whose data was collected. (Rawlings, 2023).

Informed Consent: Providing someone with all the information required to make an informed decision. In the context of wearable technology, we should focus on whether users are aware of the risks they are taking on by volunteering their information to corporations. (Arellano, 2023)

Historical Perspectives?

The field of consumer wearable technology is still emerging, but we can learn from the original use of these devices in the healthcare field.

“The use of wearable technology has been mainly associated with healthcare, and applications in the marketing domain is emerging” (Ameen et al., p.3, 2021)

Political Perspectives?

Governments assume a responsibility for protecting their citizens. Many authors of the articles used in this case study call for additional government intervention to address the concerning amount of data being collected and handled by private companies.

“As such, a digital contact tracing system will be much more defensible if managed and enforced by a government rather than an employer.” (Schaefer & Ballantyne, p.614, 2022)

Socio-Cultural Perspectives?

Wearable technology is becoming more popular in the fashion and fitness parts of society. These devices are significantly affecting the way we live, especially in western culture.

“AI and ML algorithms, when trained on data from wearable sensors, could inadvertently perpetuate or even exaggerate societal biases” (Radanliev, 2025)

“At a societal level, this aggregated data holds promise for public health initiatives, providing insights into physical activity trends, disease risks, the early detection of pandemics and the health effects associated with climate change” (Doherty et al., 2025)

Economic Perspectives?

If consumers trend towards caring more about their privacy and data, the economic market will shift towards favouring positive practices in this area.

“For example, college students have a greater propensity and ability to read, which may result in college students being more likely to pay attention to privacy policy. Yet, their relative lack of social experience might lead them to prioritize privacy concerns without fully considering the economic implications.” (Pan et al., 2024)

Stakeholders’ perspectives (values and interests)?

Government – protecting citizens from predatory data collection

“In response, various governmental regulations set baseline protections for consumer data. Frameworks such as the European Union’s General Data Protection Regulation (GDPR), the United States’ Health Insurance Portability and Accountability Act (HIPAA), the California Consumer Privacy Act (CCPA), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and the Asia-Pacific Economic Cooperation’s Cross-Border Privacy Rules form a global patchwork of protections aimed at balancing privacy with innovation and interoperability.” (Doherty et al., 2025)

Data company – collecting data to improve user experience

“In practice, app providers use this data to offer personalized services, but this has led to heightened user concerns about data leakage and misuse” (Pan et al., 2024)

Consumer – purchasing the devices for fashion or utility

“For instance, wearable devices like the Fitbit are capable of monitoring and encoding users’ biometrics into data, real-time physical conditions including heartbeat rate and blood pressure can be converted into data visualisation. Fitness and dietary recommendations are then automatically devised by algorithms, persuading users to adhere to such advice with the aim of enhancing their health status.” (Liu, 2025)

Intended ends and possible side effects?

Intended to improve the lives of consumers, however privacy concerns have risen.

“In practice, app providers use this data to offer personalized services, but this has led to heightened user concerns about data leakage and misuse” (Pan et al., 2024)

Historical Perspectives

Wearable devices has long been available in the field of healthcare with some crediting 13th century eyeglasses as being the first “wearable technology” (Ometov, p.3, 2021). This is being reflected in the development of consumer wearable technology as rings and watches are designed to track heart rates, blood flow, and sleep patterns, meanwhile cameras are being implanted in smart glasses. Despite these exciting advancements, we are witnessing the same ethical issues arise in the consumer market as the healthcare field did with the growth of the technology on their side. Ameen et al. found that the market for consumer wearable devices is rapidly growing, yet the most popular use is for personal health and fitness tracking (p.3, 2021). These historical privacy concerns will continue to be a threat to consumers unless changes are implemented to resolve the same problems healthcare has been facing for years.

Socio-Cultural Perspectives

This systematic literature review revealed how wearable technology is fundamentally altering society as it becomes increasingly integrated into our culture. One of the most concerning consequences of these changes is the possibility of systematic biases being reinforced by the data collected by these devices (Radanliev, p.2, 2025). They may reinforce negative stereotypes, or they could lack diverse datasets as Predel et al. found that “[t]he use of wearable sensors such as smartwatches shows major demographic and socioeconomic differences. Mainly young, wealthy people buy smartwatches” (p.5, 2022). On the other hand, Doherty et al. suggested that the data collected could have positive effects on society such as “public health initiatives, providing insights into physical activity trends, disease risks, the early detection of pandemics and the health effects associated with climate change” (p.1, 2025). These opposing views offer important perspectives on the socio-culture changes that this technology is bringing.

Economic Perspectives

Earlier we discussed the theoretical perspective of surveillance capitalism. When it comes to the health data that these devices collect, they can be worth up to 250\$ according to estimates uncovered by Doherty et al (p.1, 2025). This new market for personal data, combined with surveillance capitalism theory is where our economic perspective comes from. However, increasing awareness of the issue has proven to be the most effective tool in resolving the problem. Pan et al. believe that greater social experience may alter the attitudes of people towards privacy policies that have economic implications for themselves (p.13, 2024).

Stakeholders' Perspectives

The first stakeholder is the government, which also has a political perspective in the sense that it has a responsibility to protect its citizens, and this should include their personal data. Authors such as Schaefer & Ballantyne suggest that data should not be held by private corporations at all, and the government should be the only ones permitted to retain this sensitive information on the premise that the government would not use it for its own gain (p.614, 2022). While preventing private companies from holding onto the data of consumers may be unrealistic, Doherty et al., points out that existing regulations such as the *European Union's General Data Protection Regulation*, the *United States' Health Insurance Portability and Accountability Act*, and *Canada's Personal Information Protection and Electronic Documents Act* are all successful frameworks that can be amended as the technology advances to continue to protect citizens from predatory data collection (p.2, 2025).

The stakeholder that is criticized the most for creating the technoethical issues that we are discussing is the data companies, or manufacturers of these devices. Their perspective is

interesting since they are seeking a balance between innovation and privacy concerns. Walking this line according to Pan et al., looks like “app providers often include privacy policies during app installation, outlining their data collection and usage rights” however, “these policies are frequently overlooked by users due to their length and complexity or because of users’ attitudes and mental fatigue” (p.2, 2024). The companies behind this technology have a constant tension between financial interests and consumer trust when it comes to data collection, and the more popular this topic becomes, the more the manufacturers will have to prioritize good data protection practices.

The third stakeholder is the consumer, those who are purchasing the devices. From their perspective, they are victims of the opaque system that these manufacturers operate in and a lack of reliable protection from their governments. When researching wearable technology in the workplace, Plester, et al. suggested that consumers could “draw attention to justifications for surveillance health-technology and how these justifications can obscure processes of surveillance capitalism” (p.375, 2024) to push for change in the system. This is of course assuming that consumers are made aware of the privacy threats, which we have seen is not true.

Discussion & Conclusion

Limitations

While this case study was completed with rigour and vigilance, there remains limitations to the project. Firstly, the depth of literature that was searched did not reflect all of the existing knowledge on the subject. Only English language articles available through the University of Ottawa digital library and 6 subscribed databases were searched with highly specific search strings. I recognize that knowledge outside of these constraints exist. Secondly, subconscious

biases may be reflected as this project was conducted by a single researcher, all of the interpretations and discussions only portray my point of view.

Conclusion

The first finding that the existing literature on this topic is heavily associated with healthcare coincides with the fact that “[t]he use of wearable technology has been mainly associated with healthcare, and applications in the marketing domain is emerging” (Ameen et al., 2021). If we wish to avoid some of the problems that the healthcare field has experienced by deploying this technology, research should be a primary focus going forward to avoid falling behind as we have in healthcare.

The ethical concerns remain consistent across most research done on these technologies. They all seek to address privacy concerns related to the data collection of the wearable devices. Sui et al., go a step further to address human rights issues related to the AI integration with wearable devices (2023). Doherty et al., raise the more common ethical concerns such as “cybersecurity breaches, data misuse, consent violations, discrimination against vulnerable populations, biometric persecution, and widespread surveillance” (2025). So, across the applications of the technology, the problems remain the same.

As mentioned in the findings, the lack of awareness by consumers is holding back a positive shift towards better protection against privacy threats. The study that found that companies data security infrastructure and policy are directly correlated with consumer concerns should exemplify why it is so important that consumers understand the situation they are in (Ameen et al., 2021). The high level of trust towards data handling companies by participants in the Weinberger et al. (2025), study is confusing considering Doherty et al., reported that “a

security incident exposed over 61 million fitness tracker records, and a breach involving UnitedHealth compromised the health information of 100 million individuals” (2025). These significant breaches should in theory lead to a higher level of concern by consumers who are at risk of being included in future data breaches, but the level of concern is not there yet.

The solutions offered were underwhelming considering the gravity of the problem as seen in the findings. There is a lack of consensus amongst researchers, with the blame being pointed in many directions. The most common theme found in the articles was for consumers to protect themselves. This comes off as almost lazy since many of these articles also addressed the issues regarding a lack of awareness of the issue by consumers to begin with. Radanliev was the only author to suggest a unique solution when he said:

“diverse data collection is crucial to ensure that datasets include a variety of individuals in terms of age, gender, ethnicity, and health status. Additionally, machine learning techniques like adversarial training or re-sampling methods can help detect and counteract biases in training data. Manufacturers and researchers should also be transparent about potential limitations or biases in wearable devices to ensure transparent reporting.” (2025)

These innovative strategies will hopefully become more common as the field of technoethics, and consumer wearable technology evolves.

Future Direction

Looking to the future, Dobson et al., focus on the role of researchers to carefully address the ethical issues with this technology and say that without adequate research done on this topic, “government policies and company practices cannot effectively adapt to protect digital health equity, individuals’ privacy and access to data, and to ensure that wearables provide the desired level of information and support to their users” (2023). So, while there does not seem to be a proper solution in sight, there is still a clear path to discovering it. There is a significant need for

further research specifically in the field of consumer wearables as this systematic review revealed that the industry and adoption rate are growing but policy and framework has not kept pace. Literature regarding “smart hearing” devices and “smart glasses” was rarely found throughout this research project, therefore I would recommend this as a potential area of focus for future researchers. Additionally, there has been a focus on adult consumers and elderly patients in healthcare, yet very few articles discussed the implications of wearable technology on youth and children. My final recommendation for future research is to explore the technoethical challenges that children face in this new age of data collection through wearable technology.

References

Articles used for systematic literature review

- [1] Schaefer, G. O., & Ballantyne, A. (2022). Ethics of digital contact tracing wearables. *Journal of Medical Ethics.*, 48(9), 611–615. <https://doi.org/10.1136/medethics-2020-106958>
- [2] Ameen, N., Hosany, S., & Tarhini, A. (2021). Consumer interaction with cutting-edge technologies: Implications for future research. *Computers in Human Behavior.*, 120, Article 106761. <https://doi.org/10.1016/j.chb.2021.106761>
- [3] Pan, Y., Ruan, Y., Chang, M., Lyu, D., & Li, Y. (2024). Read or skip privacy policies when installing apps on wearable devices: the roles of perceived necessity and threat clues. *Humanities and Social Sciences Communications.*, 11(1), Article 665. <https://doi.org/10.1057/s41599-024-02989-4>
- [4] Liu, Z. (2025). Toward Datafied Human Enhancement: Concept, Functional Classifications and Ethical Issues. *Filosofija. Sociologija = Philosophy. Sociology.*, 36(1), 85–93. <https://doi.org/10.6001/fil-soc.2025.36.1.10>
- [5] Eckhaus, E., & Sheaffer, Z. (2022). Adoption of wearable technology: Risk and success factors. *Fashion, Style & Popular Culture.*, 9(4), 457–481. https://doi.org/10.1386/fspc_00156_1
- [6] Doherty, C., Baldwin, M., Lambe, R. *et al.* (2025). Privacy in consumer wearable technologies: a living systematic analysis of data policies across leading manufacturers. *npj Digit.Med.* 8, 363. <https://doi.org/10.1038/s41746-025-01757-1>
- [7] Radanliev P. (2025). Privacy, ethics, transparency, and accountability in AI systems for wearable devices. *Frontiers in digital health*, 7, 1431246. <https://doi.org/10.3389/fdgth.2025.1431246>
- [8] Weinberger, N., Baumann, M. F., & Maia, M. (2025). Self-monitoring of health - user viewpoints on gathering data using consumer health technologies during leisure time. *Frontiers in Digital Health*, 7, 1588183. <https://doi.org/10.3389/fdgth.2025.1588183>
- [9] Sui, A., Sui, W., Liu, S., & Rhodes, R. (2023). Ethical considerations for the use of consumer wearables in health research. *Digital Health*, 9 <https://doi.org/10.1177/20552076231153740>
- [10] Dobson, R., Stowell, M., Warren, J., *et al.* (2023). Use of Consumer Wearables in Health Research: Issues and Considerations. *Journal of Medical Internet Research*, 25(1). <https://doi.org/10.2196/52444>
- [11] Plester, B., Sayers, J., & Keen, C. (2024). Health and wellness but at what cost? Technology media justifications for wearable technology use in organizations. *Organization (London, England)*, 31(2), 358–380. <https://doi.org/10.1177/13505084221115841>

- [12] Vänskä, A., Mickelsson, S., Morozova, D., et al. (2023). Arctic childhood in data-driven culture: Wearable technology and children's right to privacy in Finland. *Critical Studies in Fashion & Beauty*, 14(2), 261–283. https://doi.org/10.1386/csfb_00067_1
- [13] Canali, S., Schiaffonati, V., & Aliverti, A. (2022). Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. *PLOS Digital Health*, 1(10), Article e0000104. <https://doi.org/10.1371/journal.pdig.0000104>
- [14] Hokka, J. (2024). Gender and the Diversity of the Human Body as Challenges for the Inclusive Design of Wearable Technology. *Fashion Practice*, 16(1), 108–133. <https://doi.org/10.1080/17569370.2023.2250153>
- [15] Canali, S., Ferretti, A., Schiaffonati, V., & Blasimme, A. (2024). Wearable Technologies for Healthy Ageing: Prospects, Challenges, and Ethical Considerations. *The Journal of Frailty & Aging*, 13(2), 149–156. <https://doi.org/10.14283/jfa.2024.19>
- [16] O'Leary, A., Lahey, T., Lovato, et al. (2024). Using Wearable Digital Devices to Screen Children for Mental Health Conditions: Ethical Promises and Challenges. *Sensors (Basel, Switzerland)*, 24(10), 3214. <https://doi.org/10.3390/s24103214>
- [17] Chang, V., Doan, L. M. T., Ariel Xu, Q., et al. (2023). Digitalization in omnichannel healthcare supply chain businesses: The role of smart wearable devices. *Journal of Business Research*, 156, Article 113369. <https://doi.org/10.1016/j.jbusres.2022.113369>
- [18] Rees, J., Matcham, F., Probst, et al. (2023). Wearables, sensors and the future of technology to detect and infer loneliness in older adults. *Gerontechnology*, 22(2), 1–4. <https://doi.org/10.4017/gt.2023.22.2.ree.08>
- [19] Banerjee, A., Choiniere, J., & MacDonald, M. (2025). Your days are numbered: active ageing, wearable technologies and surveillance capitalism. In T. Daly & S. Braedley (Eds.), *Ageing Equitably with Care* (pp. 239–255). Policy Press. <https://doi.org/10.51952/9781447375067.ch014>
- [20] Predel, C., Timmermann, C., Ursin, F., et al. (2022). Conflicting Aims and Values in the Application of Smart Sensors in Geriatric Rehabilitation: Ethical Analysis. *JMIR mHealth and uHealth*, 10(6), e32910. <https://doi.org/10.2196/32910>
- [21] Tham, A., Schaffer, V., & Sinay, L. (2021). The ethics of experimental research employing intrusive technologies in tourism: A collaborative ethnography perspective. *Tourism and Hospitality Research*, 21(3), 303–316. <https://doi.org/10.1177/1467358421993893>

Other sources used

- Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75-89.
<https://doi.org/10.1057/jit.2015.5>
- Arellano, L., Alcubilla, P., & Leguizamo, L. (2023). 'Ethical Considerations in Informed Consent'. *IntechOpen*. doi:10.5772/intechopen.1001319.
- Rawling, P. (2023). Deontology (First edition.). *Cambridge University Press*.
<https://doi.org/10.1017/9781108581196>
- Luppigini, R. (2010). Technoethics. *IGI Global Scientific Publishing*. <https://doi-org.proxy.bib.uottawa.ca/10.4018/978-1-60566-952-6.ch002>
- Luppigini, R., & So, A. (2016). A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society*, 46, 109–119.
<https://doi.org/10.1016/j.techsoc.2016.03.003>
- O'Brien, A. M., & Mc Guckin, C. (2016). The systematic literature review method : trials and tribulations of electronic database searching at doctoral level. *SAGE Publications*.
<https://doi.org/10.4135/978144627305015595381>
- Tambone, V., Campanozzi, L. L., Di Mauro, L., et al. (2025). Technological Advances in Healthcare and Medical Deontology: Towards a Hybrid Clinical Methodology. *Healthcare (Basel)*, 13(14), 1665. <https://doi.org/10.3390/healthcare13141665>
- Mertzani, A., & Pitt, J. (2022). Social Influence and the Normalization of Surveillance Capitalism: Legislation for the Next Generation. *IEEE Technology & Society Magazine*, 41(2), 57–63. <https://doi.org/10.1109/MTS.2022.3173321>
- Daga, N., Shukla, D., & Joseph, G. K. (2025). Living Under the Stare: Ethical Implications of AI Technologies in Surveillance Capitalism. *IEEE International Conference on Advanced Video and Signal Based Surveillance (Online)*, 2025, 1–6.
<https://doi.org/10.1109/AVSS65446.2025.11149955>
- Robson, G. (2023). Big Nihilism: Generation Z, Surveillance Capitalism, and the Emerging Digital Technocracy. *Information & Culture*, 58(2), 180–204.
<https://doi.org/10.7560/IC58204>
- Cascao, R. (2023). INFORMED CONSENT, DATA PROTECTION, AND TECHNOLOGICAL CHANGE IN EUROPE. *Medicine and Law*, 42(1), 79–96.
<https://research.ulusofona.pt/en/publications/informed-consent-data-protection-and-technological-change-in-euro-2/>
- Venkatachalam, S., Padmavathi, T., Vinodh, N., Thilagavathi, J., Joshi, G., Ramachandran, G., & Rajasekaran, B. (2023). Analysis of Ethical Issues Associated with Wearable Medical Devices. *International Conference on Smart Systems and Inventive Technology (Online)*, 17–22. <https://doi.org/10.1109/ICSSIT55814.2023.10061037>

- Rehak, R., & Kuhne, C. R. (2022). The Processing goes far beyond “the app” - Privacy issues of decentralized Digital Contact Tracing using the example of the German Corona-Warn-App. *2022 6th International Conference on Cryptography, Security and Privacy (CSP)*, 16–20. <https://doi.org/10.1109/CSP55486.2022.00011>
- Wang, L., Zhou, T., Wang, H., Liu, X., & Wang, Y. (2025). SCOPE: Evaluating and Enhancing Permission Explanation Transparency in Mobile Apps. *IEEE/ACM International Conference on Automated Software Engineering : [Proceedings]*, 3650–3660. <https://doi.org/10.1109/ASE63991.2025.00302>
- Schmidt, R., Schiering, I., Zwingelberg, H., & Friedewald, M. (2025). Challenges and Solutions in Implementing Informed Consent in Digital Environments: A Scoping Review. *IEEE Access*, 13, 71965–71983. <https://doi.org/10.1109/ACCESS.2025.3562773>
- Ometov, A., Shubina, V., Klus, L., et al. (2021). A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. *Computer Networks (Amsterdam, Netherlands : 1999)*, 193, Article 108074. <https://doi.org/10.1016/j.comnet.2021.108074>