Ethical Analysis of "TrackWell" Mobile Application: A Hypothetical Case Study

Contents

Intro

Trackwell is a Health and lifestyle app, designed for employers to monitor their employees in a variety of ways. One is monitoring the employee's health condition in real time. Creating a medical record of the employee in the database. It also tracks the employee's live location and their work efficiency and uses the combination of data to create suggestions to improve the employee's work performance such as shift rotations, task reassignments and rest periods. These calculations are deduced by AI software. Also, an additional feature of the app, named "Lifewell" focuses on monitoring and storing the data of the employee from their personal life. Such as dietary habits, sleep patterns, exercise consistency etc… and uses the data gathered to provide personalised tips to improve health and quality of life.

The potential ethical issues that may arise from this app is a breach of privacy. A question of what data should a business concern themselves with about an employee, and especially if this business is monitoring it in real-time and storing this data. This could lead to unfair discrimination in the workplace. Another potential issue (possibly in the legal sense too) is the storing of unnecessary data. This is increasing the risk of the people the data concerns for no reason. If there is a security breach, sensitive info of the employees may be leaked. This is especially concerning when the app knowingly and publicly co-operates, connects and shares data with third parties, such as other apps on your phone. A third ethical issue is the heavy use of AI software. Guarantees and precautions must be exercised and presented to keep the confidence of employees whose data is being fed into the AI.

However, there are the counterarguments as to why these may be ethical. Such as when the employee signs up to work somewhere, should and can they be allowed to sign a contract to provide their consent for their data to be collected, stored and used in calculations through AI? A 2nd counter argument is the businesses right to try and increase productivity of their workforce. And how much does an employee's private life affect the business.

In this case study I will be focusing on potential ethical issues this app and its features/functions may be violating. Taking into consideration the legal standpoints too. Especially the laws and regulations that focus on the data that is stored by businesses (such as the GDPR). Though ethics is a complex concept to put into law and can vary from person to person since people can value different morals, we can still evaluate different perspectives depending. I will argue the for and against sides, and see which side holds firm against the criticisms.

Big Data in Mobile App Development

TrackWell uses big data by collecting and storing an extremely large amount of data, and uses this dataset to detect trends and patterns, and also to calculate and produce personalised ads for the employees its concerns. The issue with storing such an abundant of data is the risk of holding unnecessary data. This is unlawful and unethical. It is unlawful due to the Minimisation principle found in the General Data Protection Regulation (GDPR). 1. "Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)". Though we are focusing on the ethical arguments mainly, I believe it is important to make it clear it also is potentially illegal if the data that is being stored is not 1. "…adequate, relevant and limited to what is necessary…". The unethical side is for two main reasons.

The first reason is it puts the employees in unnecessary risk. If the system is breached and data is leaked through malware, valid user incompetence, brute force attack, ransomware etc… The employees will have their sensitive data made public. The sensitive data in this sense is numerous. Such as medical information, data of live location tracking, dietary patterns ... the app collects, which for many people is considered personal and would see it as a violation of privacy and an overextension of the business. Risk of exposed personal data is the first main issue. In the UK, the right to privacy is encoded in article 8 in the Human rights Act of 1998 2. "Article 8 protects your right to respect for your private life, your family life, your home and your correspondence" . This is especially a risk since the app knowlingly shares this data with other apps and third parties on the device.

The second ethical issue is if the business switches to using this data for hiring, firing, promoting and demoting employees rather than just providing improving healthcare tips. When it comes to what companies should take into consideration when altering the hierarchy of employees, it can be seen as unethical and unfairly discriminatory if the wrong data is used. Such as, for example, the age of the employee. Many do not believe that this is a fair metric to add into the equation. When it comes to the metrics Trackwell stores, it is rather uncertain whether it would be ethical to use this data when amending employee contracts.

On one hand, the employees physical and mental health is important and relevant to the business. This is for 3 reasons

- The business may be held liable if the employee is injured

- Depending on the type of work the employee is doing (for example if they are lifting heavy items out of a lorry into a warehouse) the physical health of the employee must be considered.

And the third probable reason is that the business' overall goal is to maximise profit. For that, they must increase productivity from their employees. And for that, their employees must be physically healthy, and if their health decreases, so will the businesses profits. Does the business have the right to hire the most physically able employees? And additionally, does this allow the business to monitor the health of their employees in real time? Perhaps this decision can be left between the individual employees and the business, where the workers must provide their consent and be informed with exactly what data will be collected and what purposes they will be used for.

What must be consistent is the employees must always be aware of the data that is being collected and stored, and always have the ability to request all data is removed. This is also found in the article 17 of the GDPR, under 3. "Art. 17 GDPR ,Right to erasure ('right to be forgotten')" and it states 3." The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay". With the abundance of personal data stored, this feature must always be available and effective to remain in the legal AND ethical stance.

- Healthcare data - health insurance portability and accountability act

Surveillance and Society

There is constant discussion on how much the government should be involved in your personal affairs. One affair is where the individual current and previous places they have travelled / visited. In the US constitution, in article IV they do address of the US citizens right to travel 4." The Citizens of each State shall be entitled to all Privileges and Immunities of Citizens in the several States. " In other words, citizens are free to move from state to state and live anywhere in the country. This addresses the right to move location, but it does not address the right for the Government to track and store data about the citizens location. For many, the Government knowing the location of your home address is seen as reasonable and sensible. Simply for services such as taxes and Mail. But when it comes to places you visit during the day, or during your time out of your work, many would not see it as ethical that the government collects this information. Can the same standards be applied to businesses? And what laws must they head too in this matter? And is the law enough to keep the businesses actions ethical in the public eye?

The business you work for must know your home address for multiple reasons. To verify you are being truthful about who you are, to send mail, if need be, etc... But what about what bars and restaurants you go to? Friends and family houses you go round to? During office hours, it may seem perfectly normal for a business to know where you are, to check you are where you are meant to be. Legally, it is not legal to track someone without their consent. So, if a business wants to track someone that individual must be made aware of this. When a business is collecting this data, they must make the individual aware this data is stored. Additionally, the business must make 4.) "Specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" . There must be a valid reason as to why the location of employees is being tracked. In this instance, it is to create detailed reports to management so they can alter shifts if necessary.

Tracking the location of employees outside of workhours without a strong reason can be seen as an intense violation of privacy and a huge overstep of the business into the employee's personal life. Also, it can be a serious safety hazard. If this data is leaked, or shared to someone with malicious intent, it could put the employees in danger. Since now this person knows the location of where the employee goes to regularly.

Another, much more broad, potential issue is the concept of allowing an organization this power. If a business is granted access to do this without providing full transparency and accountability, with a valid as to why they are acting in this way. People may become comfortable with an organisation monitoring them outside of work hours. This may lead to more serious infringement of privacy further down the road.

However, tracking of people outside workhours does already exist in a way. CCTV cameras can detect faces, and can store that data, along with details of the vehicle if you are driving one. Too much surveillance in the country can only lead to an invasion of privacy, and this can be from a private company, the government or any other organisation. An example of this is China. China is very often regarded as surveillance state, where the government has free reign over monitoring and controlling the autonomy of its population. Currently, China currently has 6.) "... now 700 million CCTVs in China. ". That is around 1 camera for every 2 people. In the UK there is around 5.) "7.5 million cameras in the UK, which is around one camera, for every eleven people. ". Tho we are far from the level other countries are, we should still be wary when widening the social norm of organisations surveying people during their personal time.

Even when tracking people during work hours, it could create a sense of mistrust between the employee and management. The employee may feel constantly uneasy while at work and may become mentally and/ or physically stressed from them pushing themselves. Terrified that management will be unhappy with their workload.

The Ethics of AI in Decision-Making:

When it states TrackWell uses an AI Algorithm, this means 7.) "a set of instructions or rules that enable machines to learn, analyze data and make decisions based on that knowledge". The use of AI in the trackwell app may be a cost and time effective choice, but it does raise some ethical considerations. The AI must be guaranteed to be using the data for the purpose that was publicly announced by the business. In this instance, it should only be using the data for creating personalized recommendations for the employee. There it cannot Once again, in regard to the GDPR 1.) "You must be clear about what your purposes for processing are from the start." For this, the program must be maintained by staff, and proof must be provided that the AI is using the data correctly. Maybe even, the program itself may be made public. An open-sourced AI algorithm would be achieving full transparency. However, the business may be very hesitant on this decision since it may be exposing company secrets.

Transparency of the algorithm would also cover the question of unfair discrimination. The Algorithm must be creating fair recommendations using fair metrics. For example, skin colour, hair colour, gender, ethnic background etc... are seen as incredibly unethical to take into consideration when deciding on rota shifts, salary and employment status for individuals. For they are unfair to judge one someone for their value to the business as a worker. The algorithm should be audited by a third party that has no bias whether the business does well or not. in the last decade the use of AI algorithms has risen exponentially, especially when handling and processing big data (extremely large data sets). Since traditional methods are time-consuming and ineffective when handling them. National Governments have been rushing to set up systems to begin governing, maintaining and guiding organizations to use AI algorithms ethically. In the Uk government, there is currently no strict legislation or branch that governs AI in the private sector. 8.) "The UK recognizes that legislative action will ultimately be necessary, particularly with regard to General Purpose AI systems (GPAI). However, it maintains doing so now would be premature, and that the risks and challenges associated with AI, regulatory gaps, and the best way to address them, must be better understood.". Though it seems there are future plans, currently it seems these algorithms are being monitored as closely as they should be. This could leave the individuals that the algorithms data concerns to unfair treatment.

Because it is an algorithm making the decisions, and not a human. The results may be lacking the human touch of empathy and understanding. For example, if the Ai algorithm recommends that an employee can be increased in shifts, yet the state of that person's mental health may not add to the equation by the algorithm. This may only be known / understood by a human manager who interacts with this employee. Therefore, the AI decision may seem effective at first but would only cause harm to both the employee and the business.

The counterarguments to the criticisms are rather straightforward, the first is due to the enormous amount of data, it would take a long time for a human controller to create such accurate and well detailed reports for the employees. An AI algorithm may be the only reasonable decision in this situation. Another counter is also human controllers can also act out unfair decisions to employees with diverse backgrounds. For AI, you can make certain it would not be auditing the program, while it can be almost impossible to check that a person does not hold unfair biases. Apart from checking their work over by another human.

Big Data and Organizational Decision-Making

There are already many companies that use Big data and AI algorithms. Some are the largest in the world, such as 9.) "Top 9 Companies That are Using AI for Recruitment ... Amazon, Delta Airline, Dominos" with such an abundance and variety of data, the chances of management decisions using inappropriate information to make life changing decisions. Maybe a strategy of only gathering data that is relevant to management decisions would decrease the reliance of AI algorithms and the risk of using unethical information. Since if the data gathered decreased, it may become possible for a human operator to process. Or decrease dependency by making recommendations from the big data structures as one of many devices to use during decision making, and not going by just these reports alone. Another ethical issue is transparency with the employees. When changes are made, the individuals it affects may have questions about why these decisions were made. If management were heavily influenced by the AI reports produced from the big data, would they have to go into detail about these reports? And the data it uses?

The issue with management depending so heavily on these reports is if the employee decides to be removed from the data pool, which is found in multiple data laws around the world (such as the California Consumer Privacy Act – CCPA 9.)" Right **to delete**: You can request that businesses delete personal information they collected from you and tell their service providers to do the same, subject to certain exceptions (such as if the business is legally required to keep the information).".
This right is also protected under the GDPR. If the employee has their data deleted, then management would not receive personalized reports about that individual. And therefore, if they have no other sources of information, would not know how to improve their work life and general health. It could be seen as unfair and unethical that just because the employee does not want their personal data collected and stored, that now they do not receive support and recommendations to improve their lifestyle.

Though these ethical concerns are valid, the advantages management can gain from using the big data structure are enormous. In general, the more information you know about something, the more accurate your conclusions will be. The more info management has on their employees, the greater accuracy of recommendations they can provide. Also, with using an AI algorithm, they can identify patterns that a human controller may struggle discovering. Also, an algorithm can process infinitely more information that a human can in a fraction of the time. When it comes to the lack of empathy and human understanding, this can be rectified when the reports reach the human managers, they can implement the 'human touch' per say.

Conclusion

There is a constant discussion in human society on how much the governing body should know about you, and how much they should leave be and not monitor. However, the rules are rather more complex for private businesses. They are not the governing body; they do not control the police or the judiciary so with them having your data is not seen as threatening. Yet, there are not powerless, they do control peoples employment, salary and in result, their livelihood. So we still must remain vigilant that businesses are held accountable legally and morally when handling sensitive data.
It seems many of the ethical issue stems from lack of transparency. The main goals of the laws put in place (such as the GDPR, DPA 2018, CCPA) is to give the individuals more power and control over their personal data, especially when a large organisation is collecting and storing it. It is when the individual does not know that their data is being collected, shared and processed that the actions of the business can be seen as unethical. The app itself I believe is not illegal and can be used fairly if you are diligent in your actions. The individuals that the data you are collecting refers too are providing you,

their trust.

<u>References</u>

1.) Principle (c): Data minimization. (2023, May 19). Ico.org.uk. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data- protection-principles/a-guide-to-the-data-protection-principles/the- principles/data-minimisation/#data_minimisation

2.) Equality and Human Rights Commission. (2018, November 15). The Human Rights Act. Www.equalityhumanrights.com. https://www.equalityhumanrights.com/human-rights/human-rights-act

3.) GDPR. (2013). Art. 17 GDPR – Right to erasure ("right to be forgotten") | General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-17-gdpr/

4.) Security, R. (2019, February 8). United Kingdom Laws on GPS Vehicle Tracking & GDPR. Rewire Security. https://www.rewiresecurity.co.uk/blog/the- united-kingdom-gps-tracking-laws

5.) CCTV Usage in the UK // How many CCTV cameras are there in the UK? (2021, February 9). Clearway. https://www.clearway.co.uk/news/cctv-usage-in- the-uk/

6.) The surveillance state. (n.d.). https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/Peterson%20Testimony.pdf

7.) Tabsharani, F. (2023, May 5). Types of AI Algorithms and How They Work. Enterprise AI. https://www.techtarget.com/searchenterpriseai/tip/Types- of-AI-algorithms-and-how-they-work

8.) Gallo, V., & Nair, S. (2024, February 21). The UK's framework for AI regulation | Deloitte UK. Www.deloitte.com. https://www.deloitte.com/uk/en/Industries/financial-services/blogs/the- uks-framework-for-ai-regulation.html

9.) KAUSHIK, A. (2024, February 27). Companies that are Using AI for Recruitment. Www.wecreateproblems.com. https://www.wecreateproblems.com/blog/companies-using-ai-for- recruitment

10.) State of California Department of Justice. (2024, March 13). California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa