Surveillance and Privacy: The Ethical Implications of AI

Over the years, technology has gone through many advancements where artificial intelligence (AI) has become a reality and is slowly being implemented in the workforce. With the rapid advancement of AI however, we see how AI has already been implemented in different aspects of our lives such as household items. Even though AI offers benefits to our society in enhancing efficiency and accuracy, it also raises significant ethical concerns especially within the area or surveillance. Take facial recognition for example, it has become increasingly seen in public spaces, which sometimes sparks debates about the balance of security and someone's privacy. Facial recognition is a way of using software and algorithms to determine the similarity between two face images to evaluate a claim. This technology can be used in a variety of aways such as being used to sign a user in to their phones to search for a particular person in a database of photos. (Lewis, J. A., & Crumpler, W.) Since its implementation around the 1960s, facial recognition has become faster and more accurate in searching for faces from a single picture to the point that it is used by government and private organizations alike. This technology helps identify people who have committed crimes, improved public safety, and streamlined various processes.

Although the idea of public safety is on the mind of those who create the software and are using it, there are users who worry about the different misuses or the lengths that are intrusive on someone's privacy. One event that happened in London earlier this year sought Gorilla Technology Group Inc. for their use of AI software which was used to help assist London's Metropolitan Police in securing a successful conviction in a complex homicide investigation. Although the use of AI to secure and aid police investigations is very helpful for the public, there are those who boast concerns on the potential for mass surveillance, discrimination, and the erosion of civil liberties

(Gorilla Technology Group Inc).

Case Study

In January 2024, Gorilla Technology Group Inc. stepped in with an AI-powered surveillance system to help London's Metropolitan Police tackle a high-profile homicide case. This cutting-edge tech made evidence collection faster, identified key suspects, and played a major role in securing a conviction (Gorilla Technology Group Inc., 2024). It was a clear example of how AI can transform the criminal justice system.

While the case was celebrated for its speed and success, it also raised some serious ethical questions. Advocacy groups and citizens alike voiced concerns about whether facial recognition tools violate privacy rights or open the door to mass surveillance. Some even warned that if these technologies go unchecked, we might be heading toward a dystopian world where constant monitoring becomes the norm. This case shines a spotlight on a big debate: how do we balance public safety with protecting individual freedoms when it comes to AI-driven surveillance?

Ethical Analysis

1. **Mass Surveillance:** The widespread use of facial recognition in public spaces can create a state of mass surveillance, where individuals are constantly monitored or tracked without their consent. Thus, raising questions about the uses and balance between security and individual freedom. As noted by Edwards, the potential for mass spying through AI-powered surveillance is a significant concern. Mass surveillance can further expand on the erosion of trust in government institutions, create a sense of fear, and limit individuals' ability toe actively participate in activities without the fear of being monitored.
2. **Discrimination and Bias:** With the continued use of facial recognition, the algorithms that have been used and created depict bias, particularly with individuals with darker skin tones.

This bias can lead to discriminatory practices, such as racial profiling. As noted by Findley (2020), there are several factors which contribute to this bias such as:

   a. **Training Data:** Facial algorithms are trained on huge datasets of images. If these datasets aren't diverse in terms of representation of more than one skin tone, the algorithms will pick up on these biased patterns which lead to inaccurate identification of people with darker skin tones.
   b. **Algorithm Design:** The way these algorithms are designed can also contribute to bias. For example, some algorithms are only used to focus on certain facial features that are depicted more in certain racial groups.

3. **Chilling Effect on Free Expression:** A "chilling effect" is dubbed as "the idea or theory that laws, regulations, or state surveillance can deter people form exercising their freedoms or engaging in legal activities on the internet." (Butoiu) Surveillance tools paired with AI has been used to spot crime as seen in at one of London's underground stations. Transport for London used a computer vision system to try and detect crime and weapons, people falling on the tracks, and far dodgers. (Burgess)

Proposed Solutions

Dealing with the ethical challenges of AI surveillance isn't simple—it calls for a big-picture approach that blends technology, regulations, and community involvement.

Regulatory Oversight

Governments need to step up and create clear, enforceable rules for how AI surveillance tech is used. These rules should spell out what's allowed, ban overly invasive practices, and make sure violations are dealt with. Independent watchdog groups can step in to monitor compliance and handle misuse complaints. A great example is the EU's General Data Protection Regulation (GDPR).

It enforces transparency, limits unnecessary data collection, and requires informed consent—ideas that could apply to AI surveillance too (GDPR.eu). Meanwhile, the U.S. could benefit from nationwide legislation to ensure consistent AI ethics and accountability across all states.

Fighting Algorithmic Bias

To tackle bias in AI systems, developers need to prioritize diversity and inclusion when designing and training their models. That means using data that truly represents different racial, gender, and socioeconomic groups. Groups like the National Institute of Standards and Technology (NIST) already offer tools and guidelines to help identify and fix bias—these should become standard practice. But it's not just about the data. Developers should also use fairness metrics and test rigorously during the design process to catch biases early. Partnerships between researchers, tech companies, and advocacy organizations can spark new ideas for spotting and correcting bias.

Transparency and Public Engagement

Before rolling out AI surveillance tech, it's critical to get the public involved. Building trust starts with being upfront. Governments and companies need to explain how these systems work, what data they collect, and how they store it. Public input matters. Holding community meetings, public hearings, and conducting impact assessments gives people a chance to voice concerns and shape policy. On top of that, individuals should have the choice to opt out of systems like facial recognition whenever possible.

Protecting Privacy

We can also fight the risks of AI surveillance with smarter tech. Privacy-enhancing technologies (PETs), like differential privacy, add statistical "noise" to data to hide individual identities while still allowing useful analysis (*van Blarkom*). Another option is federated learning, where data stays on personal devices rather than being centralized, reducing the risk of breaches. By building these

safeguards into AI surveillance systems, developers can show they're serious about ethics and privacy.

Ethical AI Frameworks: A Guiding Light

Any organization deploying AI needs to follow clear ethical guidelines, like the EU's framework for trustworthy AI or the IEEE's principles for ethically aligned design. These frameworks emphasize fairness, accountability, transparency, and respect for human rights (Human Rights Watch). They give organizations a solid foundation for responsible AI use.

Conclusion

AI surveillance is a double-edged sword. On one hand, tools like facial recognition can improve public safety and streamline operations. On the other, they raise tough ethical questions. Take London's Metropolitan Police, for instance—AI has helped solve crimes, but it also reveals how easily these tools could be misused without safeguards. The way forward is clear: ethics need to take center stage in the design, deployment, and regulation of AI surveillance systems. That means reducing bias, being transparent, and earning public trust through open conversations. With strong regulations and smart privacy tech, we can enjoy the benefits of AI while protecting fundamental rights.

Sure, the ethical challenges of AI surveillance are tricky—but they're not impossible to overcome. When governments, developers, and communities work together, we can find a way to balance tech innovation with the freedoms we all value.

Sources

Burgess, M. (2024, February 8). London Underground AI surveillance documents. Wired. https://www.wired.com/story/london-underground-ai-surveillance-documents/

Edwards, B. (2023, December 5). Due to AI, we are about to enter the era of mass spying, sa ys Bruce Schneier. Ars Technica. Retrieved from https://arstechnica.com/information-technology/2023/12/due-to-ai-we-are-about-to-enter-the-era-of-mass-spying-says-bruce-schneier/

Gorilla Technology Group Inc. (2024, January 04). Gorilla Technology Group's AI Solution Ass ists London's Metropolitan Police Secure Successful Convictions in Complex Homicide Investigatio n. GlobeNewswire. https://www.globenewswire.com/news-release/2024/01/04/2803958/0/en/Gorilla-Technology-Group-s-AI-Solution-Assists-London-s-Metropolitan-Police-Secure-Successful-Convictions-in-Complex-Homicide-Investigation.html

Lewis, J. A., & Crumpler, W. (2021, June 10). How does facial recognition work? CSIS. https:/ /www.csis.org/analysis/how-does-facial-recognition-work

Findley, B. (2020, November 3). Why racial bias is prevalent in facial recognition technology. Har vard Journal of Law & Technology Digest. Retrieved from https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology

Human Rights Watch. (2014, July 28). *With liberty to monitor all: How large-scale US surveillance is harming journalism, law, and American democracy*. Human Rights Watch. https ://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

GDPR.eu.(n.d.). **General Data Protection Regulation (GDPR).** Retrieved from https://gdpr-info.eu/

van Blarkom, G.W.; Borking, J.J.; Olk, J.G.E. (2003). "PET". Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents). ISBN 978-90-74087-33-9.