Pokémon GO: A Data Goldmine for AI Training

By Elena Andreou, associate *at* *Elias Neocleous & Co LLC* *law firm*

In 2016, the augmented reality (AR) game Pokémon GO became a global sensation, blending physical exploration with virtual gameplay. Behind the scenes, the game's immense popularity also served as a unique opportunity for its developer, Niantic, to collect vast amounts of data from millions of users. While this data drove innovation in AR and machine learning, it also raised significant questions about privacy and compliance with evolving data protection laws.

This article explores how Niantic leveraged player data to train artificial intelligence (AI) systems and considers the critical privacy implications for organizations developing AI-driven products.

Introduction

Pokémon GO's core gameplay relies on geolocation and AR technology, requiring players to interact with real-world locations via their smartphones. As players traversed their neighbourhoods and beyond, Niantic collected extensive data, including:

- Geospatial data: Mapping where and how players moved in physical space.
- User interaction data: Tracking interactions with in-game objects, such as catching Pokémon, visiting PokéStops, and participating in battles.
- Device sensor data: Utilizing gyroscope, accelerometer, and camera data to enhance AR experiences.

This dataset proved invaluable for training AI models. For example, geospatial data helped improve mapping algorithms, enabling Niantic to refine AR rendering and enhance real-world navigation tools. Additionally, aggregated player behaviour patterns likely informed predictive algorithms for game design and urban planning applications.

While Niantic's innovative use of data demonstrates the transformative potential of AI, it also underscores the complex interplay between AI development and privacy laws.

1. Lawful Basis for Data Processing

Under data protection laws like the GDPR, organizations must have a lawful basis for collecting and processing personal data. Niantic likely relied on user consent obtained through Pokémon GO's terms of service and privacy policy. However, questions arise about whether this consent was informed and specific enough to cover secondary uses, such as AI training.

2. Data Minimization and Purpose Limitation

The GDPR emphasizes that data collection should be limited to what is necessary for specified purposes. Niantic's dual use of data for gameplay and AI training may stretch the principle of purpose limitation. Could players reasonably foresee that their gaming data would contribute to broader machine learning initiatives?

3. Data Anonymization

Niantic likely aggregated and anonymized player data before using it for AI training, reducing privacy risks. However, with advances in re-identification techniques, questions about the robustness of anonymization practices persist.

Key Takeaways for Organizations Leveraging User Data in AI Development

Transparency is non-negotiable: Companies must inform users not only about data collection but also about downstream uses, such as AI training.

Privacy by design: Companies should embed privacy safeguards at every stage of AI development, from data collection to model deployment.

Proactive governance: Regular audits of AI training datasets ensures compliance with privacy laws and mitigates risks of data misuse.

Consultation with regulators: Organizations should proactively align with emerging legal frameworks, such as the EU's proposed AI Act, which underscores their responsibility to ensure compliant and ethical AI deployment.

Conclusion

Niantic's use of Pokémon GO data to train AI systems illustrates the transformative potential of user-generated data while exposing privacy risks that demand careful legal scrutiny. For organizations at the intersection of AI innovation and data protection, achieving compliance is not merely a regulatory obligation but a cornerstone of ethical business practice.

As lawmakers continue to grapple with the implications of AI and data use, businesses must prioritize transparency, minimize data risks, and embed privacy into the DNA of their operations. Doing so ensures not only legal compliance but also the trust of an increasingly privacy-conscious public.

For more information, please contact Elena Andreou at elena.andreou@neo.law
Elena Andreou is an associate *at Elias Neocleous & Co LLC law firm*

ELIAS
NEOCLEOUS
& Co LLC