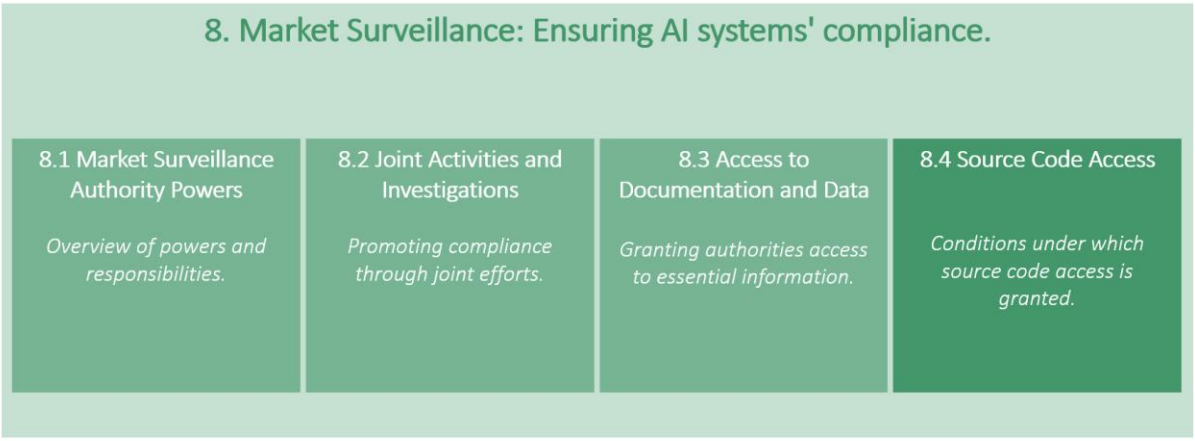
Decoding Compliance: Navigating Source Code Access in AI Market Surveillance

Co-authored with Vibhav Mithal, **Anand and Anand**, *Associate Partner*

20 January 2025



Introduction

This is the final article in our series about market surveillance under the EU AI Act. Previous articles in this series include Market Surveillance Powers with Dr. Derek Warden, swiftly followed by Joint Activities and Investigations with Prof. Dr. Ingrid Vasiliu-Feltes, and added to by Charles Kerrigan with The Critical Role of Documentation and Data Access.

To begin, we look at the basics: **What is the EU AI Act?** The EU AI Act is a landmark regulation designed to govern AI systems, ensuring safety, compliance, and innovation across the European Union.

Market surveillance authorities are granted access to the source code of high-risk AI systems under specific conditions outlined within the EU AI Act. These conditions typically entail situations where there is a need to assess the system's compliance with regulatory requirements or to investigate potential risks posed by the AI technology.

Source code access facilitates a thorough evaluation of AI systems, allowing authorities to scrutinize the underlying algorithms and mechanisms driving these technologies. By delving into the source code, market surveillance authorities can effectively identify any vulnerabilities, biases, or non-compliance issues, thereby safeguarding consumer safety and data privacy. At the same time, balancing the requirement of disclosure with protection of intellectual property rights, the EU AI Act also states that the market surveillance authorities shall respect the confidentiality of information and data in carrying out their tasks and activities in such a manner as to protect, in particular the intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code.

Understanding the nuances surrounding source code access in AI market surveillance is crucial for both regulatory bodies and AI developers. It underscores the importance of transparency and accountability in the deployment of AI technologies, fostering trust and confidence in their usage across various sectors.

The EU AI Act and Market Surveillance

The EU AI Act stands as a pivotal regulatory framework aimed at overseeing AI technologies within the European Union. With a primary focus on ensuring safety, compliance, and fostering innovation, this legislation outlines stringent guidelines for AI systems' deployment.

Central to the enforcement of the EU AI Act are market surveillance authorities, tasked with vigilantly monitoring AI systems to ensure adherence to regulatory standards. These authorities wield significant powers, including access to documentation and data vital for assessing AI systems' compliance.

In navigating source code access within AI market surveillance, understanding the pivotal role of market surveillance authorities is paramount. These authorities play a crucial role in overseeing the compliance of AI systems, ensuring they meet the stringent requirements outlined in the EU AI Act.

The access to documentation and data granted to market surveillance authorities serves as a cornerstone in their efforts to assess the compliance of AI systems. By leveraging this access, authorities can effectively evaluate the underlying mechanisms and algorithms driving AI technologies, thereby safeguarding consumer safety and privacy.

In essence, the establishment of market surveillance authorities and their powers under the EU AI Act underscores the commitment to ensuring transparency, accountability, and regulatory compliance in the deployment of AI technologies across the European Union.

Understanding Source Code Access

Source code access for high-risk AI systems under the EU AI Act is subject to specific conditions, ensuring a balanced approach between regulatory oversight and protecting proprietary information. Market surveillance authorities are granted access to source code upon a reasoned request, but only when deemed necessary to assess conformity with the Act's requirements.

Access to source code is authorized under Chapter III, Section 2 of the EU AI Act, which delineates guidelines for high-risk AI systems. This access is contingent upon exhausting or finding the data and documentation provided by the AI system provider insufficient through testing or auditing procedures.

In essence, source code access is not granted arbitrarily but is based on a thorough evaluation of the AI system's compliance status. It serves as a critical tool for market surveillance authorities to delve deeper into the underlying mechanisms of high-risk AI systems, ensuring they meet the stringent regulatory standards set forth in the EU AI Act. The market surveillance authorities also have an obligation to respect the confidentiality of the data and information obtained in carrying out their tasks and activities, which includes maintaining the confidentiality of the source code.

By adhering to these conditions, market surveillance authorities can effectively navigate source code access in AI market surveillance, promoting transparency, accountability, and regulatory compliance within the AI ecosystem while safeguarding proprietary information and fostering innovation.

The Dual Conditions for Source Code Access

Access to the source code of high-risk AI systems by market surveillance authorities hinges on two pivotal conditions: necessity and exhaustion. Firstly, authorities must demonstrate the necessity of accessing the source code to evaluate the system's compliance with the EU AI Act. This requirement ensures that access is warranted and proportionate to the assessment objectives, preventing arbitrary or unjustified intrusion into proprietary information.

Secondly, access to the source code is contingent upon the exhaustion of other testing or auditing procedures based on the data and documentation provided by the AI system provider. This condition mandates that market surveillance authorities explore alternative avenues before resorting to source code access, fostering transparency and accountability in the compliance assessment process.

These dual conditions carry significant implications for AI providers, underscoring the importance of robust documentation and comprehensive testing procedures to demonstrate compliance without necessitating source code disclosure. Additionally, safeguards are in place to protect sensitive information, including confidentiality obligations outlined in the EU AI Act, ensuring that proprietary algorithms and intellectual property rights remain safeguarded during market surveillance activities.

By adhering to these conditions and safeguards, AI providers can navigate source code access in AI market surveillance with confidence, knowing that regulatory oversight is balanced with the protection of proprietary information, fostering trust and collaboration within the AI ecosystem.

Confidentiality and Data Protection

The EU AI Act incorporates robust confidentiality obligations to safeguard information and data obtained during market surveillance, including source code access. These obligations ensure that sensitive proprietary information remains protected while facilitating regulatory oversight.

Market surveillance authorities are bound by these obligations to maintain the confidentiality of acquired information, preventing unauthorized disclosure or misuse. This ensures the protection of intellectual property rights and confidential business information, fostering trust and cooperation between authorities and AI providers.

Balancing regulatory oversight with the protection of proprietary information is paramount for fostering innovation and compliance within the AI ecosystem. The confidentiality provisions outlined in the EU AI Act strike this balance, enabling market surveillance activities to proceed effectively while safeguarding the interests of AI providers. In upholding these confidentiality obligations, market surveillance authorities can navigate source code access in AI market surveillance with integrity and transparency, promoting a regulatory environment conducive to innovation and compliance.

Challenges and Best Practice

Accessing and handling source code presents several challenges for market surveillance authorities in AI regulation. Firstly, the complexity of AI algorithms and systems can make it difficult for authorities to interpret and analyse the source code effectively. Additionally, AI providers may be hesitant to disclose their source code due to concerns about intellectual property protection and competitive advantage.

To navigate these challenges, market surveillance authorities can implement several best practices. Firstly, establishing clear guidelines and protocols for requesting and handling source code can promote transparency and cooperation between authorities and AI providers. Secondly, fostering open communication channels and collaboration between authorities and providers can help address concerns and facilitate the exchange of necessary information. Thirdly, implementing robust data protection measures and confidentiality agreements can reassure AI providers that their sensitive information will be safeguarded. Finally, investing in training and capacity-building programs for market surveillance authorities can enhance their technical expertise in analysing source code effectively.

By adopting these best practices, market surveillance authorities and AI providers can work together to ensure compliance with AI regulations while protecting sensitive information and fostering a culture of transparency and trust within the AI ecosystem.

Conclusion

In summary, source code access plays a crucial role in ensuring compliance with the EU AI Act. By granting market surveillance authorities access to source code under specific conditions, such as necessity and after exhausting other testing procedures, the Act establishes a framework for effective oversight while protecting intellectual property rights. Confidentiality obligations further safeguard sensitive information obtained during market surveillance activities. Adhering to these conditions and obligations promotes transparency and trust between authorities and AI providers, facilitating the assessment of AI systems' compliance. Ultimately, navigating source code access in AI market surveillance requires a delicate balance between regulatory oversight and protecting proprietary information, ensuring a fair and transparent regulatory process within the AI ecosystem.

Glossary

Act or EU AI Act: European Union Artificial Intelligence Act

AI: Artificial Intelligence

Board: European Union Artificial Intelligence Board

EU: European Union

SME: Small and Medium-Sized Enterprise

How can we help?

AI & Partners
Amsterdam - London - Singapore

AI & Partners ' –AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.