ISSHIKI & PARTNERS

Managing the Risk of Information Contamination

Contents

Managing the Risk of Information Contamination

By Taro Isshiki
Isshiki & Partners

1 Introduction

In recent years, amid the rise of open innovation, companies have increasingly received technical information and know-how from business partners. At the same time, the risk of "information contamination" — the mixing of received confidential information with a company's own development efforts or other proprietary information — has become more pronounced.

When information contamination occurs, it becomes difficult to prove the independence of a company's in-house development, raising the possibility of contractual breach or allegations of misappropriating trade secrets. This risk is particularly significant in transactions with U.S. entities, where the ease of filing lawsuits and the expansive discovery process can elevate the issue into a major business threat.

This article examines the risks of information contamination involving properly received confidential information from business partners and outlines measures to prevent and address such risks.

2 What Is Information Contamination Risk?

2.1 Typical Risks of Unauthorized Use

Confidential information received under a non-disclosure agreement (NDA) is generally limited to use for the specific purpose defined in the contract. Use beyond that scope may constitute not only a contractual breach but also trade secret misappropriation.
Examples where contamination commonly arises include:

- Using technical information received for joint development in a company's own independent product development
- Applying information obtained during investment or acquisition due diligence to one's own business strategy
- Using product specifications learned through contract manufacturing in products for other customers

2.2 Delays in Establishing Internal Controls and Underlying Factors

Despite frequent receipt of technical information from partners, many companies lack sufficient contamination safeguards. This is often due to:

- **Lack of risk awareness**: At the time of NDA execution, companies often do not anticipate future misuse scenarios or contamination risks. When risks materialize later during in-house development, frontline personnel may be unaware of the original contractual limits.
- **"Black box" development**: Because the use of information in product development is not externally visible, third parties cannot verify whether contamination has occurred. This opacity may lead to underestimation of

the risks.

- **Confidential dispute resolution**: Contamination-related disputes are often handled privately through negotiation or arbitration, limiting public awareness and further downplaying the risk.

2.3 Risks in U.S. Transactions and Delayed Response in Japan

The risk of information contamination is particularly significant in technology transactions with U.S. companies and universities. In the United States, lawsuits can be initiated relatively easily, and once litigation begins, the discovery process requires broad disclosure of internal materials, including emails, meeting records, and development documents. This enables a detailed investigation into whether confidential information was misused and increases the likelihood that such misuse will be found. Accordingly, when entering into transactions with U.S. counterparts, it is essential to establish robust internal procedures and conduct thorough risk assessments from the outset—not merely to rely on contractual safeguards.

In contrast, Japanese companies often underestimate the risk of contamination, in part due to the absence of a discovery system under Japanese civil procedure. However, this risk should not be dismissed. The Japan Fair Trade Commission has noted that the unauthorized use of confidential information in breach of a non-disclosure agreement may constitute interference with business under Japanese competition law. Its 2020 survey on startup business practices further suggests that contamination cases are not uncommon in Japan. Companies should therefore recognize the seriousness of this issue and implement appropriate measures domestically, just as they would for cross-border transactions.

3 Measures to Prevent Information Contamination

Preventing information contamination requires not only carefully drafted contract terms but also the implementation of operational procedures after contract execution. This section outlines key practical steps that companies should take following the conclusion of confidentiality agreements.

3.1 Establishing Dates for Pre-Existing Information

A powerful defense against contamination claims is demonstrating that the company possessed similar technology before receiving the confidential information. To do so, companies must clearly record the existence of such technology and objectively verify the date.

Options include using notarization systems, patent filings, or time-stamping digital documents. These records serve as valuable evidence supporting independent development in the event of a dispute.

3.2 Clarifying the Information Receipt Process

Because disputes may arise years after information is received, it is critical to maintain clear records of what was received and under what circumstances. For example, companies can use dedicated shared email addresses for projects, ensuring centralized receipt and preserving audit trails. Avoid relying on individual email addresses, as

personnel transfers or resignations can hinder tracking.

Moreover, companies should avoid receiving information unrelated to the contract's stated purpose. If such information is received accidentally, it should be promptly returned or destroyed, and the incident should be documented.

3.3 Segregated Storage and Access Controls

If confidential information is stored together with internal materials, it becomes difficult to prove non-use later. To avoid this, received information should be stored separately from internal data.

For digital files, this means storing external data in dedicated folders or servers, with access strictly limited to personnel on a need-to-know basis. Maintaining access logs is essential to ensure and demonstrate that no unauthorized access has occurred.

3.4 Disposal and Recordkeeping

Most NDAs require the return or destruction of confidential information (and derivatives) at the end of the contract. In practice, however, complete deletion can be challenging. Backup servers may not allow selective deletion, and traces may remain in personal emails.

If a contamination claim is made, the company must be able to identify the received data and demonstrate that it was not used. Destroying all data at the contract's end can hinder such efforts and actually increase litigation risk.

Unless a contract explicitly prohibits retention, it is advisable for the legal or IP department to retain a complete set of the information under strict internal controls for recordkeeping purposes. Demonstrating that the data remained unaccessed may reduce liability by showing no harm was caused.

3.5 Additional Measures During Internal Development

The risk of information contamination increases significantly when a company develops technology similar to one that was co-developed with a third party, or when it undertakes a separate project with another partner in a related technical area.

To prove that confidential information was not used, companies must implement stricter internal protocols. Ideally, employees exposed to third-party confidential information would not be involved in the development project. If this is unavoidable, the company must thoroughly screen their working environment and ensure that no third-party information resides in their folders or emails.

Companies should also consider implementing "clean room"-style protocols by predefining what technical information will be used, documenting the development process, and recording sources. These steps serve as key

evidence of independent development.

Additionally, obtaining written declarations from developers stating that they will not use third-party confidential information helps raise internal awareness and provides external reassurance. If any team members overlap between joint and in-house projects, it is advisable to obtain mutual confirmations from both teams affirming that no information exchange occurred.

If a company can demonstrate that such measures were in place, it may be able to prevent or swiftly resolve disputes even if contamination concerns are raised.

4 Conclusion

Information contamination is a management risk that can arise during everyday business operations and organizational processes. To effectively address this risk, companies must proactively design and operate explainable procedures for each phase — from receipt and storage to use and disposal of information.

By implementing the measures outlined in this article, companies can build internal safeguards that enable them to provide a "reasonable explanation of non-use." At the same time, overly rigid or formalistic implementation may undermine operational flexibility or healthy information sharing. Therefore, companies should tailor their response to each situation, taking into account the nature of the partner, the sensitivity of the technology, and the potential impact of a dispute.

It is our hope that this article serves as a practical guide for reviewing and strengthening corporate information management systems.

(July 2025)

About the Authors and Firm

Taro Isshiki
Managing Partner
Attorney at Law
California and District of Columbia
tisshiki@isshiki-law.com

Taro Isshiki is a U.S. attorney and a managing partner of Isshiki & Partners. He was previously a partner at Morrison & Foerster before founding his own firm in 2011. He has extensive experience handling U.S. litigation and a broad range of cross-border disputes. Taro also works closely with Isshiki Patent & Trademark Firm to support clients across a wide spectrum of intellectual property matters.

Isshiki & Partners is a Tokyo-based law firm specializing in cross-border matters. Our attorneys, many of whom previously practiced at leading global law firms, excel at representing international clients in a broad array of litigation, intellectual property and corporate matters. We work closely with our affiliate Isshiki Patent & Trademark Firm to provide comprehensive IP services, handling every phase of intellectual property matters from initial filings to Supreme Court appeals.