

TECH, IP AND TELECOMS LAW UPDATES

November 2024 (Vol.12)

Atsushi Okada
Partner
atsushi.okada@mhm-global.com

Daisuke Tsuta
Counsel
daisuke.tsuta@mhm-global.com

Colin Trehearne
Foreign Law Counsel
colin.trehearne@mhm-global.com

Kaei Ro
Counsel
kaei.ro@mhm-global.com

Kohei Wachi
Senior Associate
kohei.wachi@mhm-global.com

Masumi Sato
Associate
masumi.sato@mhm-global.com

Hiromu Nagira
Associate
hiromu.nagira@mhm-global.com

1. Recent Trends in Dark Patterns: Updates to the Ministry of Internal Affairs and Communications' "*Smartphone Privacy Initiative*" and Other Developments
2. AI Policy Updates
3. FSA Publishes its "Guidelines on Cybersecurity in the Financial Sector"
4. Publication of the "Labelling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) "

We are pleased to present the November issue (Vol.12) of our "TECH, IP AND TELECOMS LAW UPDATES," a collection of the latest information about Japanese technology, intellectual property, and telecommunications law. We hope that you will find it useful to your business.

1. Recent Trends in Dark Patterns: Updates to the Ministry of Internal Affairs and Communications' "*Smartphone Privacy Initiative*" and Other Developments

In recent years, there has been growing awareness of the issues surrounding "Dark Patterns". These are techniques designed to deceive or manipulate users, impairing or distorting their choices. Across Europe and the U.S., explicit bans have been introduced and enforcement undertaken pursuant to legal frameworks such as the EU's Digital Services Act, along with guidelines and reports from organizations such as the European Data Protection Board, the U.S. Federal Trade Commission, and the Organization for Economic Co-operation and Development.

In light of these developments, Japan has also begun addressing Dark Patterns in various government guidelines and documents. For example, [the draft report of the](#)

TECH, IP AND TELECOMS LAW UPDATES

[Working Group on User Information](#) by the Ministry of Internal Affairs and Communications (MIC) (open for [public comment](#) until November 8, 2024) includes a proposed revision to the “Smartphone Privacy Initiative” (to be renamed the “Smartphone Privacy and Security Initiative”). The draft outlines specific examples of Dark Patterns in the handling of user information and states that app providers should avoid such practices.

Additionally, the [revised](#) “Guidelines on Consumer Protection Rules under the Telecommunications Business Act”, published by the MIC on October 31, 2024, include recommendations to ensure that users are not misled by Dark Patterns when confirming basic information or selecting plans on web pages for certain telecommunications services. The guidelines provide examples of desirable and undesirable web page designs.

The “[Interim Report on the Paradigm Shift in Consumer Law](#)”, released by the Cabinet Office's Consumer Law Committee on October 17, 2024, also highlights the increasing prevalence and severity of Dark Patterns in digital transactions. It calls for strict measures against malicious practices, the design of incentives to promote sound business activities, and balanced regulations. The report further emphasizes the need for effective enforcement, considering cross-border transactions and the significant presence of overseas digital platforms. Moreover, it highlights the importance of leveraging the contributions of diverse organizations, including consumer groups.

In the private sector, the [Association for Countermeasures against Dark Pattern](#) was established in October 2024. The association plans to draft guidelines and implement a Non-Deceptive Design certification system to evaluate and certify websites that avoid Dark Patterns.

2. AI Policy Updates

Recently, there have been various updates across different legal fields regarding the regulation of AI. On October 2, 2024, the Japan Fair Trade Commission (JFTC) released a discussion paper titled “[Generative AI and Competition](#)”, seeking input from stakeholders regarding the generative AI market. This paper breaks down the market structure of generative AI into infrastructure (computing resources, data, specialized personnel), models, and applications, and highlights several potential antitrust and competition policy issues. Specific topics include access restrictions and exclusion of competitors, self-preferencing, tying arrangements, parallel conduct using generative AI, and acquiring specialized talent via partnerships. Based on the information gathered, the JFTC plans to organize the acquired information and, if necessary, provide guidance on antitrust and competition policy. Although the investigation is still in its early stages, given

TECH, IP AND TELECOMS LAW UPDATES

the regulatory powers of the JFTC it will be important to closely monitor the JFTC's actions moving forward.

Additionally, on November 15, 2024, the Intellectual Property Strategy Headquarters of the Cabinet Office published the [“Guide for Rights Holders: the Interim Report of the Intellectual Property Rights Examination Committee for the AI Era”](#). This guide explains the key points of the interim report published in May 2024 from the perspective of rights holders. It outlines the legal, technical, and contractual measures that rights holders can take if they wish to provide data for AI training or prevent their content from being used in AI training. For example, technical measures to prevent data from being used in AI training include setting a robots.txt file on websites to refuse collection by crawlers and adding noise to images to disrupt AI training. Like the interim report, this guide does not have legally binding force.

Furthermore, on October 30, 2024, the Ministry of Economy, Trade and Industry held [a meeting to discuss considerations for contracts related to AI utilization](#). The meeting aims to discuss the potential contents of a checklist of considerations for AI-related contracts. The final version of the checklist is expected to be published after January 2025.

Finally, the Patent Office plans to discuss necessary legal revisions to the Design Act and Patent Act to ensure the protection of legitimate inventors' rights, even when a large number of designs and inventions may be published using generative AI. It is anticipated that various ministries and industry groups will continue to address issues arising from the use of AI by variously enacting new laws and guidelines. We will continue to keep you updated on the latest developments in this rapidly evolving area.

3. FSA Publishes its “Guidelines on Cybersecurity in the Financial Sector”

On October 4, 2024, the Financial Services Agency (FSA) published its [“Guidelines on Cybersecurity in the Financial Sector”](#). From June 28 to July 29, 2024, the FSA invited public comments on the draft guidelines, and as a result of this, some supplementary explanations and footnotes were added to the guidelines but without substantive changes to the content.

These guidelines are made up of three sections, and in particular, Section 2 “Cybersecurity Management Framework” clarifies the “basic response items” and “response items that are desirable” for financial institutions, etc., regarding governance, identification, protection, detection, response, recovery, and third-party risk management.

It is noteworthy that, in all cases, financial institutions are not required to take uniform measures, but rather are required to identify and assess cyber security risks based on their business environment, management strategy, risk tolerance, etc., and to take

TECH, IP AND TELECOMS LAW UPDATES

measures to reduce risks commensurate with those risks (i.e., to adopt a so-called “risk-based approach”).

For more details on these guidelines, please also refer to our Financial Regulatory Bulletin: [Data Security / FINANCIAL REGULATION BULLETIN “Guidelines on Cybersecurity in the Financial Sector” \(October 2024\)](#) (at this time only available in Japanese.).

4. Publication of the “Labelling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR)”

On September 30, 2024, the Information-Technology Promotion Agency (IPA) published the “[Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements \(JC-STAR\)](#)”. This scheme is based on the “[Policy for Establishing a Security Compliance Evaluation System for IoT Products](#)” published by the Ministry of Economy, Trade and Industry in August of the same year. The primary purpose of this scheme is to enable procurers to easily select IoT products that meet their required security standards and to promote the widespread adoption of IoT products with appropriate security measures.

Main Objectives and Overview

The main objectives of this scheme are as follows:

1. To evaluate and visualize the security functions of products procured by government agencies and companies using a common standard.
2. To ensure that only IoT products with sufficient security measures are adopted in specific fields.
3. To reduce the burden on vendors exporting IoT products by achieving mutual recognition with overseas systems.

Target Products and Compliance Evaluation Levels

This scheme targets a wide range of IoT products for both consumers and businesses, with the following compliance levels:

- ★1: Common compliance and evaluation standards to address the minimum threats common to IoT products.
- ★2 to ★4: Compliance and evaluation standards tailored to the characteristics of each type of IoT product.

For compliance levels ★1 and ★2, vendors can declare self-compliance through self-assessment to promote the scheme's adoption. For levels ★3 and ★4, third-party certification is required.

TECH, IP AND TELECOMS LAW UPDATES

Compliance Standards

The required compliance standards are independently defined while also harmonized with domestic and international standards such as ETSI EN 303 645 and NISTIR8425. With the announcement of this scheme, the compliance standards and evaluation methods for level ★1 (JST-CR-01-01-2024) have been established for the first time. Threats to be considered at this level include information leakage due to unauthorized access, functional abnormalities, communication eavesdropping, information leakage from discarded devices, and functional abnormalities during power outages.

JC-STAR Publication and the Future Implementation Schedule

Compliant products will be labeled with a QR code, making it easy to obtain information on compliance evaluations. Applications for level ★1 compliance will be accepted starting in March 2025. The scheme for level ★2 and above is expected to start in the second half of fiscal year 2025, and to target specific product types.

International Efforts

Similar evaluation systems are being considered and implemented in other countries, making mutual recognition with Japan's system crucial. In the UK, the PSTI Act, which includes legal obligations, came into effect in April 2024. In the US, the voluntary U.S. Cyber Trust Mark is expected to be operational by 2024. In the EU, the Cyber Resilience Act, which includes legal obligations, was adopted in October 2024.

Finally, on November 6, 2024, the Ministry of Economy, Trade and Industry published the "[JC-STAR System Utilization Guide for IoT Products in Specific Fields \(Version 1.0\)](#)", which guidance should be referred to in conjunction with this Scheme.