

TECH, IP AND TELECOMS LAW UPDATES

March 2023 (Vol.2)

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
Senior Associate
kaei.ro@mhm-global.com

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

Lexi Takamatsu
Foreign Lawyer
lexi.takamatsu@mhm-global.com

Risa Suzuki
Associate
risa.suzuki@mhm-global.com

1. Personal Information Protection Commission Releases its “*Draft Report of the Expert Panel on the Use of Camera Images for Crime Prevention and Security*”
2. Ministry of Economy, Trade and Industry Releases its “*Report of the Study Group on Strengthening Security Measures for Credit Card Payment Systems*”
3. Revisions to the “*Telecommunications Business Entry Manual (Supplement)*” and the “*Telecommunications Business Entry Manual (Supplement) Guidebook*”
4. The Supreme Court Accepts a Request for the Disclosure of the Phone Number of a Perpetrator of Online Defamation Committed before MIC Ordinance Revision
5. Japan Fair Trade Commission Releases its Investigation Report on Mobile OS
6. Metaverse Government Policy Discussion Update

We are pleased to present the March issue (Vol.2) of “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. Personal Information Protection Commission Releases its “*Draft Report of the Expert Panel on the Use of Camera Images for Crime Prevention and Security*”

Recent years have seen an increase in business and other use of camera systems with facial recognition functions for the purpose of crime prevention and safety assurance. Against that backdrop the Personal Information Protection Commission (“PPC”) established an expert panel and subsequently released in December 2022 its “[*Draft Report of the Expert Panel on the Use of Camera Images for Crime Prevention and*](#)

TECH, IP AND TELECOMS LAW UPDATES

[Security](#)". The expert panel established by the PPC has been working on, and has compiled in the Draft Report, points for businesses (and others) to keep in mind in: (i) complying with the Act on the Protection of Personal Information ("**APPI**"), (ii) preventing violations of portrait rights and privacy, and (iii) carrying out voluntary measures aimed at increasing the understanding of the subjects of the photographs/images and broader society about these issues.

What is particularly noteworthy about the Draft Report is that it (i) examines the relationship between portrait rights and privacy infringement and the APPI, which has not always been clear in the past, based on trends in court precedents and the history of the revision of APPI. The Draft Report considers that, when using camera systems with facial recognition functions, portrait rights and privacy protections should be taken into account in interpreting the prohibition of inappropriate use (Article 19) and the appropriate acquisition provision (Article 20, Paragraph 1) of the APPI. It is also noteworthy that in the authors' view (ii) the scope of joint use should be limited to what is truly necessary, with recommendations for the creation of uniform operational standards are provided in the Draft Report, and (iii) recommendations for the outsourcing of personal data handling related to camera systems with facial recognition functions (which is considered to be common in practice) are provided for reference.

The Draft Report was open for comments from 12 January to 23 February 2023, and will be finalized based on the results of the feedback received on the Draft Report. Regarding the utilization of camera images for commercial purposes, the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications published in 2022 the "[Camera Image Utilization Guidebook ver. 3.0](#)". This guidebook sets out application cases, such as customer attributes, traffic line analysis, and repeat analysis, and outlines necessary considerations for compliance with the APPI, the protection of privacy of people reflected in images, communications with individuals, and still other cases. Together with the Draft Report, this guidebook is a potentially useful reference document when handling camera images.

2.Ministry of Economy, Trade and Industry Releases its "Report of the Study Group on Strengthening Security Measures for Credit Card Payment Systems"

On 20 January 2023, the Ministry of Economy, Trade and Industry ("**METI**") published its Report of the Study Group on Strengthening Security Measures for Credit Card Payment Systems.

TECH, IP AND TELECOMS LAW UPDATES

The report is based on discussions of an expert panel, including from a technical perspective, in line with the three tracks of (1) strengthening the appropriate management of credit card numbers and other information (i.e. leakage prevention), (2) preventing the unauthorised use of credit card numbers and other information, and (3) raising awareness of safe and secure credit card use and deterring crime. The report outlines specific initiatives and future tasks for strengthening security measures for credit card payment systems.

Initiatives based on this report show substantial diversity which defies short summaries, but they include, for example, revisions to the Credit Card Security Guidelines (the latest version being 3.0 of March 2022) to make it mandatory for all electronic commerce (“**EC**”) merchants to take measures against vulnerabilities in their systems and EC websites (including measures against inadequate settings, vulnerability diagnoses, and malware countermeasures) and, in principle, to introduce EMV 3DS (3D Secure 2.0) – a new standard in payment authentication and security.

The Guidelines are positioned as practical guidance to the obligations on businesses to take appropriate management measures for *inter alia* credit card numbers (see Article 35-16 of the Instalment Sales Act (“**ISA**”)) and to prevent fraudulent use (see Article 35-17-15 of the ISA). If the measures listed in the Guidelines (or equivalent or higher measures) are properly taken, then they are deemed to meet the obligatory standards for security measures set out in the ISA. In other words, revisions to the Guidelines, practically speaking, can be seen as a revision of the obligations one must meet under the ISA.

Finally, a number of further matters requiring consideration have been identified including, but not limited to, the need for institutional measures for reporting to relevant authorities in the event of a data leakage of *inter alia* credit card numbers.

Reflecting these developments and parts of the Study Group’s Report, on 15 March 2023, version 4.0 of the Credit Card Security Guidelines was published.

3. Revisions to the “*Telecommunications Business Entry Manual (Supplement)*” and the “*Telecommunications Business Entry Manual (Supplement) Guidebook*”

On 30 January 2023, the Ministry of Internal Affairs and Communications (“**MIC**”) [released](#) a revised version of the “[Telecommunications Business Entry Manual \(Supplement\)](#)” (“**Manual Supplement**”), an important reference document when considering the application of the Telecommunications Business Act, and the

TECH, IP AND TELECOMS LAW UPDATES

[“Telecommunications Business Entry Manual \(Supplement\) Guidebook”](#) (“**Supplement Guidebook**”), which explains the Manual Supplement by visualization. These revisions have been introduced mainly to address the two new regulations on user information introduced by the revised Telecommunications Business Act of 2022 (to be enforced beginning on 16 June 2023).

The first of these two regulations is the External Data Transmission Rule, covered in the [first volume of this newsletter](#). The External Data Transmission Rule partly shares fundamental ideas with the *ePrivacy Directive/Regulation*. It requires businesses to notify or publicly announce when user information (such as cookies, other identifiers, or browsing history information) recorded on a user's device is transmitted to an external party. However, this rule is part of the Telecommunications Business Act, which only applies to businesses who are engaged in a “*telecommunications business*”. Accordingly, this rule does not apply to businesses not engaged in a “*telecommunications business*”.

In some cases, it is difficult to determine whether a website or app falls under the category of a “*telecommunications business*”. The revised guidebook seeks to address this difficulty and clarifies that when a business provides a homepage in order to (i) publicize and advertise its profile, products or services or (ii) in order to sell its products or services, it is providing telecommunications services as a mere means of conducting its own original business. As this business does not necessitate providing telecommunications services themselves then it is not a “*telecommunications business*” within the meaning of the law. On the other hand, the revised guidebook says that where a business aims to provide telecommunications services (sending information) themselves, such as online news or video distribution, it is considered a telecommunications business.

The second of these two regulations is the Rule on the Proper Handling of Specified User Information. This Rule requires that those businesses designated pursuant to an MIC public notice (selected by the MIC from among registered/notified businesses¹ that provide particularly large-scale services (ten million users for free services and five million users for fee-based services)), when the designated businesses are handling specified user information², to *inter alia*: (i) prepare and notify to the MIC of their “*Information Handling Rule*”, (ii) to prepare and publicly announce their “*Information Handling Policy*”, (iii) to evaluate their way of handling Specified User Information (each

¹ That is to say, businesses registered and notified for the operation of a telecommunications business.

² Here specific user information is information that falls under (a) confidential communications, and (b) information on persons who have entered into a contract with the business or made an account by user registration (being itself information constituting a database).

TECH, IP AND TELECOMS LAW UPDATES

fiscal year), and (iv) to appoint and notify the MIC of a Specified User Information Supervisory Manager.

In addition, although notification was not required until now for (a) telecommunications services for searching for information and (b) telecommunications services equivalent to mediating communications, such service providers will also now be required to notify the MIC if (i) their users reach or exceed ten million and (ii) they are individually designated pursuant to an MIC public notice. Therefore, businesses providing such specified services are expected to be designated as subject to the Rule on the Proper Handling of Specified User Information. In the revised Manual Supplement and Supplement Guidebook, explanations were added regarding such (a) telecommunications services for searching for information and (b) telecommunications services equivalent to mediating communications, citing examples such as online search services, social media services, electronic bulletin boards, video sharing platforms, and blogging platforms. The Manual Supplement and Supplement Guidebook clarify that site searches and word-of-mouth bulletin boards provided along with other services are not required to be notified to the MIC. As a consequence, such services are not subject to the Rule on the Proper Handling of Specified User Information.

4. The Supreme Court Accepts a Request for the Disclosure of the Phone Number of a Perpetrator of Online Defamation Committed before MIC Ordinance Revision

Online defamation is, unfortunately, an everyday occurrence in the modern world; increasingly it is being litigated. In this case, the appellant claims that his or her rights were infringed by an article posted on an electronic bulletin board on the Internet. The appellant demanded the respondent, an access provider (mobile carrier operator) who provided internet connection services to the person who posted the article, disclose the telephone number and other information of the sender, under the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (the so-called Provider Liability Limitation Act).

The types of information which can be disclosed are specified by the related ordinance of the Ministry of Internal Affairs and Communications (“MIC”), and at the time of the filing of this lawsuit (in June 2019), the name, address, and other information of the sender were specified by MIC ordinance as information which may be disclosed. Following 21 August 2020 amendments of the MIC ordinance, the sender’s telephone number was added to information of the sender which may be disclosed. Unfortunately, when making this amendment, no transitional provision was established expressly to exclude (or allow)

TECH, IP AND TELECOMS LAW UPDATES

the amended MIC ordinance to apply to a request for disclosure of a sender's information arising from alleged infringement of rights occurring *prior* to the amendments. After the amended MIC ordinance came into effect, the appellant added – at the appeal level – a request for disclosure of telephone numbers.

The appellate court (the Tokyo High Court on 24 September 2021) dismissed the request for disclosure of the telephone number without applying the amended MIC ordinance retroactively, on the grounds that allowing a request for disclosure of the telephone number, in cases like this, where the right was alleged to have been violated before the amended MIC ordinance came into effect, would infringe on the sender's important rights and interests, such as the confidentiality of communications and the sender's freedom of speech. The appellant appealed this decision.

The Supreme Court overruled the Tokyo High Court and held that the amended MIC ordinance should apply to the appellant's information disclosure request submitted after the amended MIC ordinance came into effect, regardless of when the allegedly infringing act occurred, because no transitional provisions existed. Proponents of the court's ruling support it on the basis that the Supreme Court's decision follows the principle that, in the absence of a transitional provision, the content of the MIC ordinance in effect at the time of the conclusion of oral argument should be applied to in giving judgment.

5. Japan Fair Trade Commission Releases its Investigation Report on Mobile OS

On 9 February 2023, the Japan Fair Trade Commission (“JFTC”) released its [“Investigation Report on Mobile OS, etc.”](#). Focusing on mobile OS and apps, which are essential to the use of smartphones, the JFTC conducted a survey on the competitive environment of the mobile OS market and app distribution services market (e.g. app stores), and found that Google and Apple are in a “*dual position*” of providing a mobile OS and operating app stores, while also competing with other businesses in the app market and other peripherals markets. In the JFTC's view there is not enough competitive pressure on the mobile OS and app stores provided by these two companies.

In light of this situation, the report states that, in order to compliment the (*ex post facto*) response of enforcing the Antimonopoly Law, Google and Apple should *inter alia* (i) prevent their own preferential treatment, such as allowing the use of in-app billing systems other than their own, (ii) ensure fairness in rulemaking by notifying the businesses concerned in advance of changes in the rules within the mobile ecosystem, (iii) ensure a healthy competitive environment in both markets by, for example, allowing apps to be downloaded from sources other than the company's own app store if there

TECH, IP AND TELECOMS LAW UPDATES

are no problems with security or privacy protection. In addition, to ensure the effectiveness of these measures, it was suggested that *ex-ante* regulations be introduced to the extent necessary through institutional development by law.

The competitive environment in the mobile ecosystem, including the mobile OS and app store markets, has been discussed since 2021 by [a working group of the Digital Market Competition Council](#) in [the Digital Market Competition Headquarters](#) of the Cabinet Secretariat, and at the 46th meeting of the working group (14 February 2023) held at the Fair Trade Commission of Japan. At [this 46th meeting of the working group](#), the JFTC also reported on its investigation report. It is expected that these ministries and agencies will continue to collaborate and cooperate to study regulations for mobile ecosystems.

6. Metaverse Government Policy Discussion Update

As mentioned in the [first volume of this newsletter](#), discussions on the use of the Metaverse are active across various government research groups. For example, on 10 February 2023, the Ministry of Internal Affairs and Communications' ("MIC") Study Group on the Use of the Metaverse for the Web3 Era published [an interim summary](#). The summary outlines some points for further discussion on practical issues related to the metaverse, including some legal issues, such as whether identities in the metaverse should be legally protected and whether the legal liability of platform companies for wrongful acts committed in the metaverse required clarifying in relevant laws.

These discussions and developments continue. In addition to the abovementioned MIC Study Group, [the Second Subcommittee of the Public-Private Partnership Conference on Addressing New Legal Issues Concerning Content in the Metaverse](#) is currently discussing how existing laws, such as those governing the right of publicity, portrait rights and copyright, could be applied to avatars in the metaverse. For example, it discusses some cases where the portrait of a real person or an avatar that imitates the portrait of another person is used without permission, and suggests creating guidelines and policies to make platform operators and users aware of relevant issues.

In the 211th Ordinary Session of the Diet, which is currently in session, [a bill has been submitted to partially amend the Unfair Competition Prevention Act, etc.](#) The amendment includes making the act of offering products that imitate the product forms of others in the digital space an act of unfair competition and allowing the exercise of injunctive and other rights. In this way, the protection of brands and designs in the metaverse is

TECH, IP AND TELECOMS LAW UPDATES

anticipated to be strengthened. As discussions on metaverses continue in government bodies, legislation is being speedily enacted, and industry participants will need to continue to monitor the state of discussions within the government.

Public Relations
mhm_info@mhm-global.com
+81-3-6212-8330
www.mhmjapan.com