弁護士法人中央総合法律事務所
CHUO SOGO LAW OFFICE, P. C.

STAND YOUR GROUND AGAINST ANONYMOUS ONLINE HARASSERS WITH *AMENDED PROVIDER LIABILITY LIMITATION ACT*

November 17, 2022
Yugo Kobayashi, Attorney
E-mail/kobayashi_y@clo.gr.jp

I. Introduction

The incidents of harmful and defamatory posts on the Internet and social media or illegal use of copyrighted materials (hereinafter, ***violating post(s)***) have become a social issue these past years. To address this issue, the law known as the ***Provider Liability Limitation Act***[1] (hereinafter, the ***Act***) was revised in 2021 with the revision coming into effect on October 1, 2022. The amendment is referred to below as the ***Amendment***, and so amended *Provider Liability Limitation Act* as the ***Amended Act.***

As a result of the revision, (1) the scope of authorized disclosures has been amended to allow to identify, when necessary, the sender of a *violating post*, by disclosure of the presumed sender's information, such as the IP address(es)[2] associated with the login event concerning the sender's social media account, and (2) a new court procedure by the name of the *Court Proceedings Concerning a Case Involving Order to Disclose Identification Information of the Sender* (hereinafter, ***Court Proceedings Concerning Order to Disclose Sender Information***) has been established to ensure faster and more appropriate disclosures of sender information.

This article explains the amendments (1) and (2) above.

II. Right to Demand Disclosure of Sender Information

The "right to demand disclosure of sender information" refers to the right to demand disclosure of identification information, such as the name and address, of the sender who

[1] *Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Sender* (Law No. 137 of November 30, 2001).

[2] An identification number assigned to each computer or communication device connected to an IP network such as the Internet. It is known as a "network address" and can often serve as the first clue to the sender's identification.

placed a post on the Internet.

A victim of a *violating post* on the Internet may, by way of a legal action, demand the removal of such post, or alternatively, make claims for damages against the sender of such a post. To claim damages, however, the victim needs to know the sender's name and address. In general, as *violating posts* are made anonymously, it is not easy for the victims to identify the senders' names and addresses. On the other hand, as information can spread quickly on the Internet and damages can quickly ramp up, it is important to have a clear way to seek recovery of damages. In light of these circumstances, the right to demand disclosure of sender information has now been legislated in the *Amended Act*.

Based on this right, victims are entitled to demand that social media providers and telecommunications carriers that hold information about the sender disclose the name and address of the sender, and to claim damages from the sender.

The right to demand disclosure of sender information can be exercised either in or out of court as it is provided under substantive law. In practice, however, sender information is rarely disclosed out of court by the providers (voluntarily) not only in cases where it is difficult to determine the applicability of violation of rights, but also even in cases where violation of the rights seems obvious[3].

III. Right to Demand Disclosure of "Specified Sender Information"

1 Background to the Amendment

Some social media providers never keep track of the IP address(es) and other related information associated with posting events. However, they keep track of IP address(es) and other related information associated with the login events of the users of the service (hereinafter "*login event information*"). Twitter, for example, records the *login event information* of each user without recording the IP address(es) and other related information associated with each tweet. This means that in such situations, even when the violation of rights is attributable to a *violating post*, there is no way to know the IP address(es) and other related information directly associated with such post. This type of service which records the *login event information* only, is called a login-based service and is utilized not

[3] "Final Report of the Study Group on Disclosure of Sender Information" p. 4 (December 2020)

only by Twitter but also Facebook and Instagram. *Violating posts* are often made on login-based social media.

On the other hand, as for IP address(es) and other related information not directly associated with *violating posts*, disclosure was never explicitly stipulated in the *Act* because at the time of its enactment, the *Act* was targeting bulletin board network services (such as 4chan) where they kept track of IP address(es) and other related information associated with each posting event. *Login event information* itself is not violating any rights. Hence there is much discussion as to whether such information should be disclosed, and even the court decisions varied case by case in this regard.[4]

2 Description of the Amendment

The *Amendment* was enacted to protect the victims of *violating posts* made on login-based social media as described above. Specifically, the scope of authorized disclosures was expanded to allow, when necessary, to identify the sender of a *violating post* by disclosure of the IP address(es) and other related information associated with the login event and not directly associated with the *violating post* itself. (*Amended Act*, Art. 5) IP address(es) and other related information associated with a login event (or *login event information*) are defined as "*specified sender information*" and available for disclosure subject to certain requirements. It should be noted, however, that the requirements for disclosure of *specified sender information* are stricter than those for disclosure of other information, because as mentioned above, *login event information* itself is not directly associated with *violating posts*. Specifically, the requirements for disclosure of *specified sender information* are intended for limited cases, for example where the communication logs related to individual posts made are not stored in the information systems of the social media provider concerned.

IV. Court Proceedings Concerning Order to Disclose Sender Information

1 Background to the Amendment

[4] Judicial precedents of cases where disclosure was granted include Tokyo High Court Precedent May 28, 2014 (p. 113 of *Hanrei-Jiho* No. 2233). Those of cases where disclosure was not granted include Tokyo High Court Precedent September 9, 2014 (p. 170 of *Hanrei-Times* No. 1411).

Prior to the *Amendment*, victims were not able to identify the access provider[5] (e.g., a telecommunications carrier) that holds the name and address of a given sender unless they had received from the relevant contents provider[6] (e.g., social media provider) disclosure of the IP address(es) and other related information necessary for identification. Therefore, to obtain identification information of the sender, as a general rule, as shown under "Conventional Proceedings (Provisional Disposition + Litigation)" in Figure 1 below, victims had to (1) obtain a court decision on provisional disposition against the contents provider for disclosure of sender information; (2) identify the access provider by using thus disclosed IP address(es) and other related information; and (3) commence separate litigation against thus identified access provider for disclosure of the sender information. Furthermore, victims needed to apply for another provisional disposition to prohibit deletion of IP address(es) and other related information because, as a general rule, each provider sets its own record retention period for IP address(es) and other related information and it was highly likely that the target IP address(es) and other related information for disclosure would have been deleted while the above-mentioned provisional disposition or litigation was in progress. Such court proceedings were time-consuming, costly, and hence imposed significant burdens on the victims seeking to redress the wrongs inflicted on them by the senders.

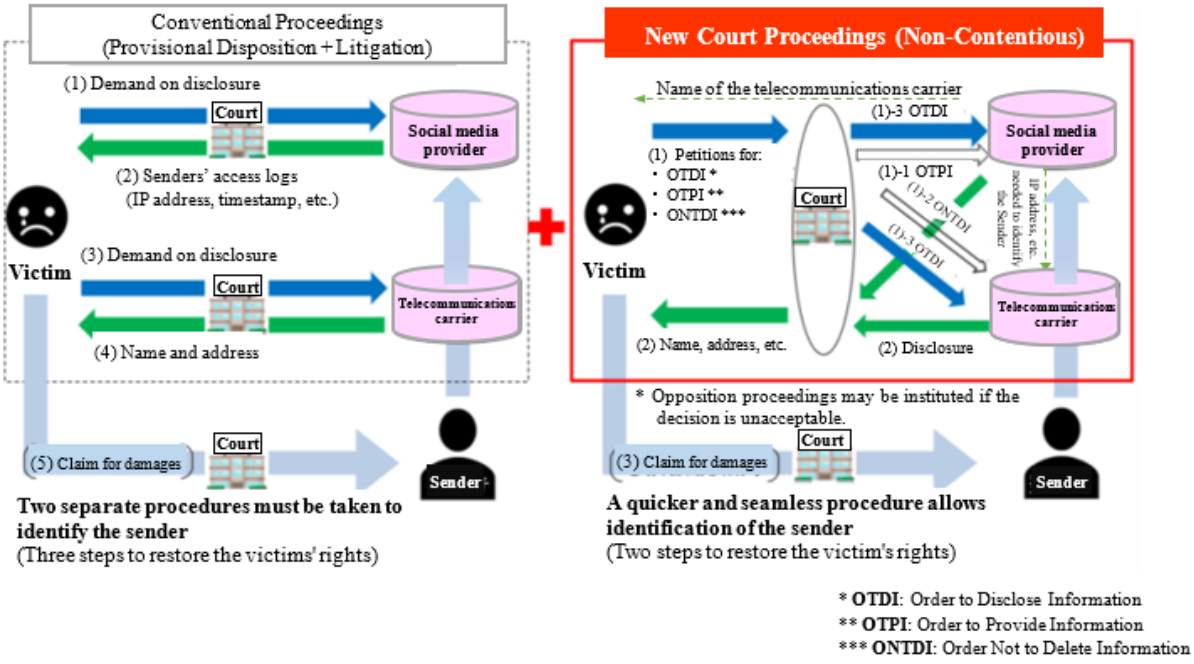
To address such a situation, a new court proceeding has been established as the *Court Proceedings Concerning Order to Disclose Sender Information.* (*Amended Act*, Art. 8 *et seq*.) It does not mean that after the *Amendment* one may no longer take the conventional procedures such as filing a petition for provisional disposition for the disclosure of sender information, a provisional disposition for prohibiting the deletion of the same, or a litigation for demanding disclosure of the same. In addition, since the *Court Proceedings Concerning Order to Disclose Sender Information* is no more than a procedure for exercising the right to demand disclosure of the sender information, it is still necessary to file a petition for provisional disposition or pursue litigation as before to seek deletion of *violating posts*.[7]

[5] A company that provides Internet access services to subscribers. Examples include NTT Communications Inc., NTT DoCoMo Inc., KDDI Inc., and SoftBank Corp.

[6] A provider of digital content on the Internet.

[7] Kuniko Ogawa et al. "Q&A on 2021 Amended Provider Liability Limitation Act" Q10, Q35 (published by SHOJIHOMU, 2022)

[Figure 1] Conventional Procedures versus New Court Procedure



(Source: Page 2 of *"How to Address Cases Involving Order to Disclose Identification Information of the Sender"* annexed to the *"Guidelines Relating to Sender Information Disclosure"* issued by the Provider Liability Limitation Act Guidelines Review Council)

2 Description of the Amendment

The *Court Proceedings Concerning Order to Disclose Sender Information* allow for two separate trials - one against the contents provider (e.g., the social media provider) and another against the access provider (e.g., the telecommunications carrier) – to be conducted seamlessly in an integrated manner. The process flow is outlined below, in the context of a case of a *violating post* made on a social media as an example.[8]

(1) The victim files a petition for an *Order to Disclose Identification Information (such as the IP address) of the Sender* (hereinafter often referred to as ***"Order to Disclose Information"*** *or* ***"Order to Disclose"***) against the target social media provider, and at the same time, files a petition for an ***Order to Provide Information*** as an incidental procedure.
An *Order to Disclose* and an *Order to Provide Information* are two different orders with similar names. An *Order to Disclose* in this context means an order against the social media provider to disclose information about the sender. An *Order to Provide Information*, on the

[8] Keiji Mukai et al. *"Operation of Court Proceedings Concerning a Case Involving Order to Disclose Identification Information of the Sender"* (NBL #1226, 2022, pp.79-92)

other hand, is described in Step (2) below.

(2) The court considers whether to issue an *Order to Provide Information* prior to an *Order to Disclose*, and issues the order if the requirements for issuance are satisfied, for example, if without the order it would be "impossible to identify the sender of *violating posts* pertaining to a petition for an *Order to Disclose* regarding the sender information." (*Amended Act*, main text of Art. 15, para. 1) Specifically, the social media provider is given an *Order to Provide Information* comprising the following obligations: (a) identifying the name and address of the target telecommunications carrier based on the sender information (IP address(es) and other related information) in its own possession and providing thus obtained information to the victim, and (b) providing the target (sender's) IP address(es) and other related information in its possession to the above-identified telecommunications carrier following the victim's filing of a petition for an *Order to Disclose* against the telecommunications carrier.

The social media provider's fulfillment of the obligations set forth in (a) above allows the victim to identify and to file a petition against the target telecommunications carrier for an *Order to Disclose* as in Step (4) below before the target IP address(es) and other related information held by the telecommunications carrier is deleted on the grounds of expiry of the retention period. The social media provider's fulfillment of the obligations set forth in (b) above allows the target telecommunications carrier to identify the sender information subject to disclosure promptly in response to the victim's filing of a petition for an *Order to Disclose* in Step (4) below, and to respond to the ***Order Not to Delete*** described in Steps (4) and (6) below.

(3) To comply with the *Order to Provide Information*, the social media provider first fulfills the obligations set forth in (a) in Step (2) above by identifying the name and address of the target telecommunications carrier based on the sender information (IP address(es) and other related information) in its own possession and providing the information to the victim.

(4) Having received the name and address of the telecommunications carrier, the victim then files a petition for an *Order to Disclose* regarding sender's information such as his/her name against the telecommunications carrier, and at the same time, files an ***Order Not to Delete Information*** *(or* ***"Order Not to Delete")*** as an incidental procedure.

The *Order Not to Delete* is an order which the court issues to prevent deletion of IP address(es) and other related information of the sender prior to the conclusion of the case of the *Order to Disclose* and relevant opposition proceedings, by prohibiting the

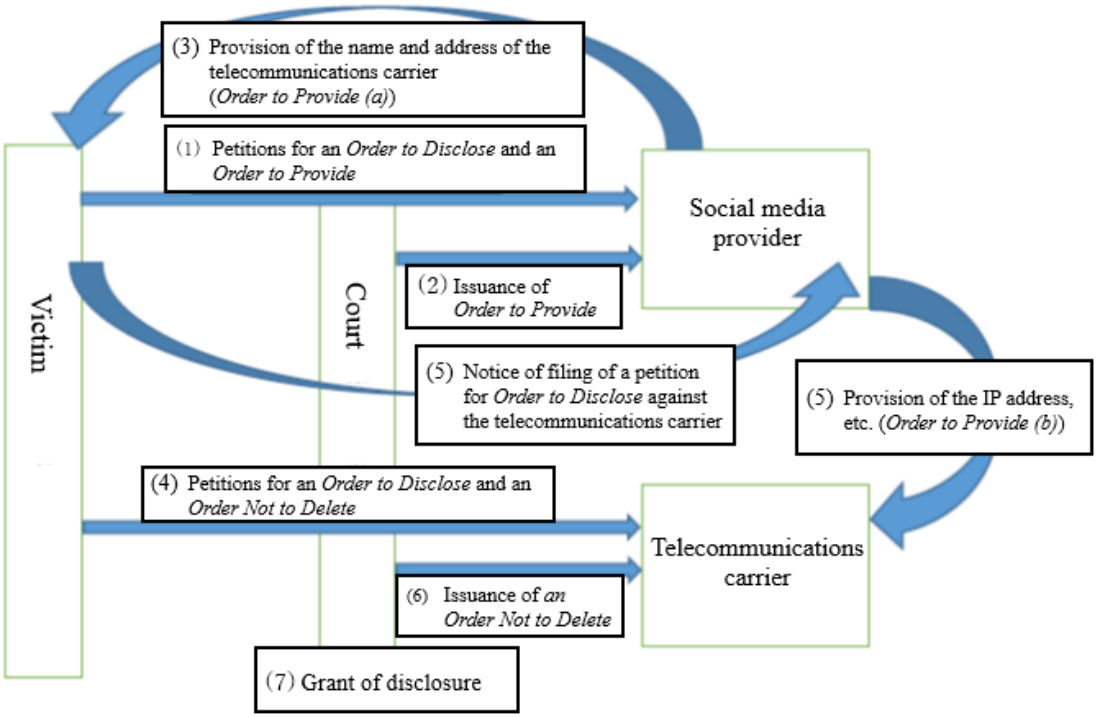
telecommunications carrier from deleting the sender information on the grounds of expiration of their internal retention period while the trial of the *Order to Disclose* is pending. As described above, proceedings for *Order to Disclose*, *Order to Provide Information*, and *Order Not to Delete* are undertaken separately, in view of the following contradictory consideration: (1) that considering the retention period of IP address(es) and other related information, the sender information must be secured in order to protect the victim(s); and (2) that disclosure must be carefully deliberated on beforehand because once disclosed, no sender information can be recovered. The separate issuance of an *Order to Disclose*, an *Order to Provide Information*, and an *Order Not to Delete* secures not only the sender information subject to disclosure but also sufficient time to determine the grant of disclosure to the victim.

(5) Once the victim notifies the social media provider that it has filed a petition for an *Order to Disclose* against the telecommunications carrier, the social media provider that has received such notice then provides the target telecommunications carrier with the sender information (IP address(es) and other related information) in its own possession, thereby fulfilling the obligations set forth in (b) in Step (2) above.
Incidentally, the victim must make the above-mentioned notification to the social media provider within two months after the receipt of the name and address of the telecommunications carrier in Step (3) above. At this stage, no IP address nor other related information can be disclosed to the victim yet.

(6) The court considers whether to issue an *Order Not to Delete* prior to an *Order to Disclose*, and issues the order if the requirements for issuance are satisfied, for example, if the telecommunications carrier possesses the sender information, or if, without the order, it would be “impossible to identify the sender of the *violating post* pertaining to a petition for an *Order to Disclose* regarding the sender information." *(Amended Act*, Art. 16, para 1.)

(7) The court conducts the trial in an integrated manner after consolidating the petition for *an Order to Disclose* against the social media provider filed in Step (1) above and the petition for *an Order to Disclose* against the telecommunications carrier filed in Step (4) above. A decision to grant disclosure of the sender information is then made provided that the relevant requirements are satisfied, for instance when it is determined that the posts in question obviously violate the rights of the victim and thus constitute reasonable grounds for disclosure.

[Figure 2] An example of the process flow of the *Court Proceedings Concerning Order to Disclose Identification Information of the Sender*



As can be seen from the above, the *Court Proceedings Concerning Order to Disclose Sender Information* addresses the problem persisting before the enforcement of the *Amended Act* and hence is expected to enable victims to recover damages resulting from a *violating post* faster and with certainty.

V. Conclusion

The *Amended Act* came into effect on October 1, 2022. On the other hand, the *Court Proceedings Concerning Order to Disclose Sender Information* can be retrospectively applied to posts published on or before October 1, 2022[9]. As it is only a month since the implementation of the *Amended Act,* the reader is encouraged to keep a close eye on the future impact the *Amended Act* will have on both the directions of court practices and on the responses of social media providers and telecommunications carriers.

[9] Statement by the Director-General of the Telecommunications Bureau of the Ministry of Internal Affairs and Communications at the Committee of the House of Councillors on Internal Affairs and Communications on April 20, 2021

The *Amendment*, however, does not eliminate the necessity of taking a legal action (e.g., petitions) as quickly as possible in view of the retention period of communication logs including IP addresses. Indeed, the victims of *violating posts* on social media, etc. who are considering making claims for damages, need to take a prompt action as before. In light of the new court proceedings, they should also consider which procedure will serve them toward recovery of damages.

End