



Communications News

Vol. 19 No. 12
September 26, 2008

Biweekly Newsletter of the Ministry of Internal Affairs and Communications (MIC), Japan

ISSN 1349-7987

Please feel free to use the articles in this publication, with proper credits.

TOPICS

The Revision of the Specified Electronic Mail Law

The Law on the Regulation of Transmission of Specified Electronic Mail (Law No. 26, 2002) (referred to below as the Specified Electronic Mail Law) which was passed as a countermeasure to SPAM required that advertising sent out without the recipients' approval should clearly state "unsolicited advertising" and made it illegal to disguise information on the sender. A revision of this law

was announced on June 6, 2008 as law No. 54, 2008 and will come into force by December 5, on the day determined by the government. This document introduces the changes in the revision of this law.

(1) The introduction of the opt-in format (post-revision article 3 and article 4) (please refer to Figure 1)

CONTENTS

TOPICS

The Revision of the Specified Electronic Mail Law

..... 1

**International Policy Division,
International Affairs Department,
Telecommunications Bureau,
Ministry of Internal Affairs and
Communications (MIC)**

1-2, Kasumigaseki 2-chome, Chiyoda-ku, Tokyo 100-8926, Japan
Fax: +81-3-5253-5924
Tel: +81-3-5253-5920

We welcome your comments via:

http://www.soumu.go.jp/joho_tsusin/eng/contact.html

MIC Communications News is available at:

http://www.soumu.go.jp/joho_tsusin/eng/newsletter.html

Presentation materials of MIC are available at:

http://www.soumu.go.jp/joho_tsusin/eng/presentation.html

E-mail distribution of this newsletter is possible if desired.

Figure 1: The shift to the opt-in format

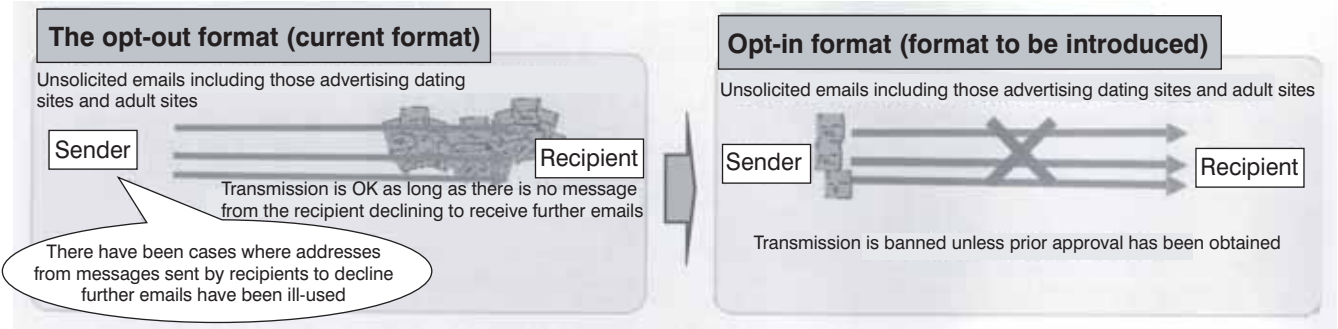
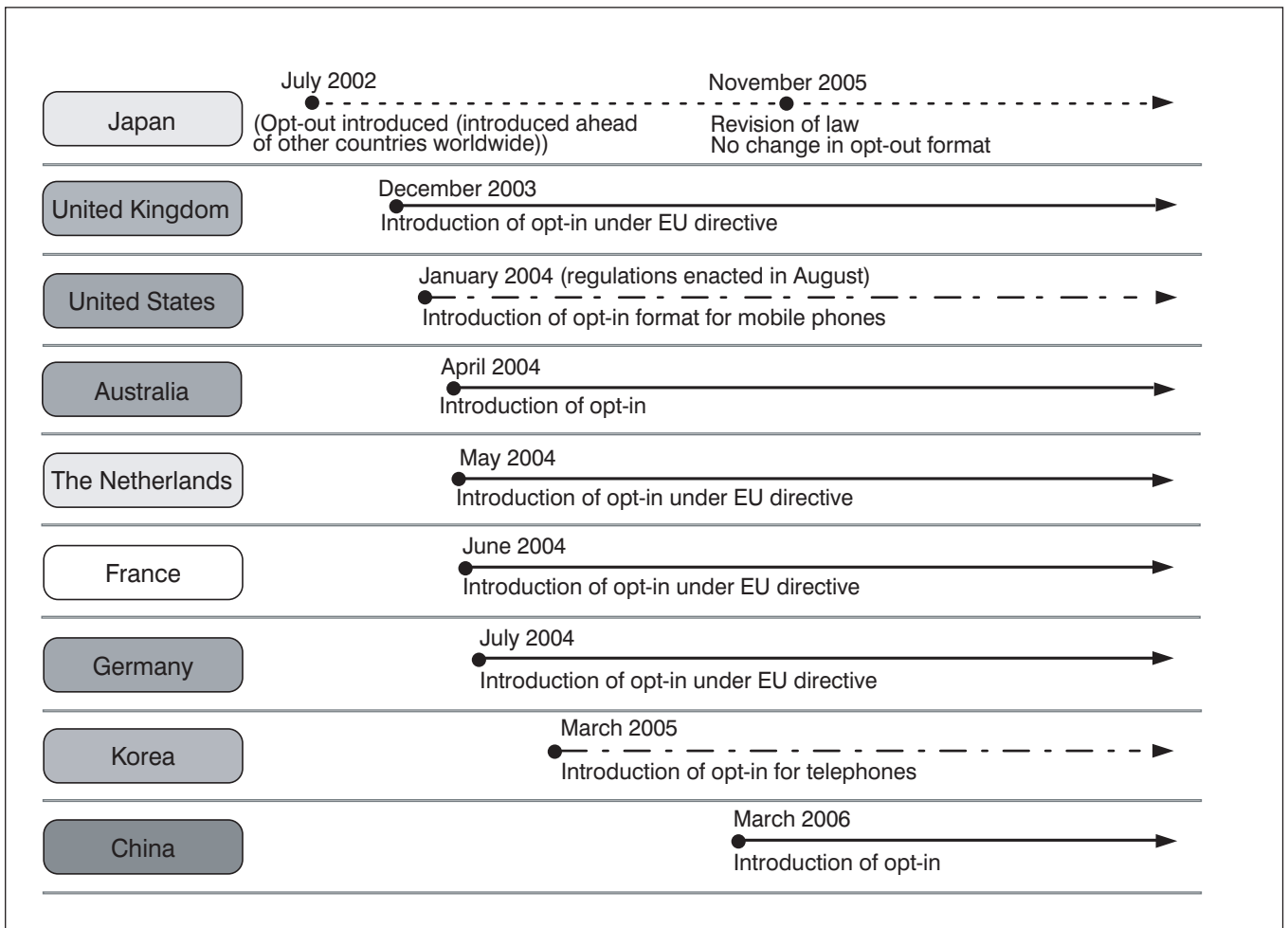


Figure 2: The state of introduction of the opt-in format in various countries



The existing Specified Electronic Mail Law uses the opt-out format which enables the sending of emails as long as there is no message declining reception from the recipient but (1) there have been problems with malicious senders using the messages declining reception to send even more SPAM, (2) opt-in is in standard use for advertising that is sent out by legitimate businesses, and (3) there has been an increase in SPAM originating overseas, and with the need for greater coordination between countries, opt-in has become the mainstream (see figure 2). Therefore, the current revision has introduced the opt-in format which basically forbids the sending out of mass emails without prior approval, to replace the opt-out format.

In concrete terms, with the exception of specified cases such as where there is a business relationship, the sending of advertising emails is forbidden without getting proper approval from the recipient, as well as sending any subsequent emails following reception of a message declining reception. It is also compulsory to display the name and appellation of the person(s) responsible for transmission as well as the email address and URL of those declining reception, and to store records that attest agreement.

Furthermore, with regard to methods for operating the opt-in format such as details of exceptions where one can send is laying down a set of guidelines

for which the basis approach is shown in the final draft report from the Study Group on Countermeasures against Unwanted Junk Mail that was set up by MIC.

(2) Consolidating the enforcement of the law

With the overall amount of SPAM increasing, and the means for transmissions becoming more malicious and sophisticated, the following revisions in the contents aim at consolidating the enforcement of the law.

(a) Clarification of the fact that telecommunications operators can refuse to provide services to those sending of email that uses disguised sender information (post-revision article 11)

With regard to transmissions that uses botnets that have recently been gaining in popularity, the sending out of phishing emails, and the sending of emails with disguised sender information, which is particularly widespread overseas, examples are stipulated in the text of cases where telecommunications operators can refuse transmission, and measures put in place to enable the operators to take independent countermeasures.

(b) Setting up regulations that will make it possible to request information from providers concerning information on subscribers they have on file, such as email addresses (post-revision article 29)

In order to facilitate identification of those breaking the law, regulations have been put in place enabling the MIC minister to request from telecommunications business operators to provide the necessary information specific to the users of emails that are suspected of breaking the law as well as the email addresses, IP addresses and domain names displayed on the websites to which the emails redirect recipients. However, this does not involve requests for information on communications records for individual communications which are bound by communications privacy.

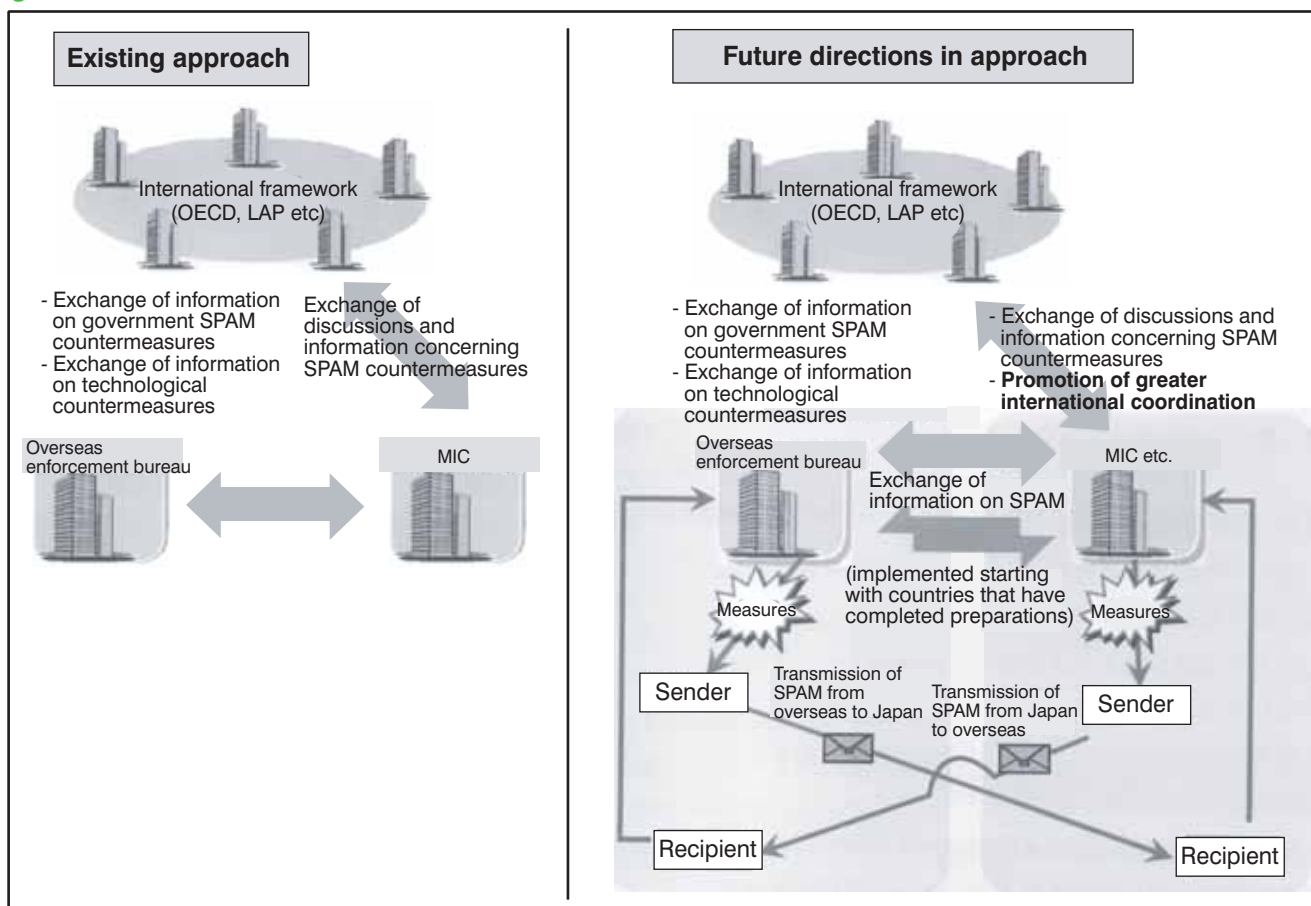
(c) Expanding the range of measures directives, collection of reports and spot inspections (post-revision article 7 and article 28)

Adding those who have entrusted the sending of emails (transmission consigners) as recipients of administrative measures such as measures directives, collection of reports and spot inspections, to simplify the legal handling of pursuits even when the sender is not clear.

(d) The maximum fine for corporations to be increased 30-fold (post-revision article 37)

Some corporations with fairly high sales figures have been among the law-breakers to date, and the fine for corporations has been increased from a maximum of 1 million yen to a maximum of 30 million yen, making it more of a deterrent.

Figure 3: Framework for future international coordination



(3) Strengthening of international coordination (please refer to figure 3)

There has been a sharp increase in the number of SPAM emails coming in from overseas, with 90% of SPAM received in Japan originating overseas. The following revisions have therefore been made as countermeasures against cross-border SPAM emails.

(a) Clarification that any emails originating overseas and received in Japan come under the law (post-revision article 2-2)

It has been clarified that it is not only email that is sent and received domestically, but also email which is sent from overseas to Japan, and email that is sent from Japan to overseas that comes under the Specified Electronic Mail Law, and a flexible operation of the law is planned so that some legal measures can be taken even against SPAM originating overseas.

(b) Putting in place regulations for

providing information to the overseas enforcement bureau (post-revision article 30)

Since the basic approach in terms of measures taken against senders of SPAM is that the bureau, which is in charge of SPAM countermeasure for the sending country will base itself on local laws, MIC is putting in place regulations for providing the necessary information for the enforcement of legislation aimed at SPAM in the country from where the SPAM is originating, and facilitating the exchange of detailed information between MIC and the bureaus overseas.

(c) Expanding the applications of measures directives and report investigations (post-revision article 7 and article 28)

By adding transmission consigners that are covered by collection of reports and spot inspections, it will be possible, in cases where even though the actual sender is overseas, the

consigner is actually in Japan, to target the sender through report collections and spot investigations of the consigner. In addition, by adding the transmission consigner targeted by the measures directives, even if the actual sender is residing overseas, the fact that the consigner who is in Japan receives measures directives is significant as a countermeasure against SPAM that is generated overseas.

(d) Refusal to provide services by telecommunications business operators (post-revision article 11)

In the case of SPAM transmission from overseas, messages are often sent using botnets and with disguised sender information. The current revision clarifies that the provision of services can be refused to those who disguise their information when sending emails, and this is expected to stimulate measures by telecommunications business operators.