Working Group on Ideal State of Safe and Secure User Environment in Smartphone Era—Final Report

# SUMMARY OF SMARTPHONE PRIVACY INITIATIVE Ⅱ

## －Ideal Third-party Verification of Applications －

September 2013

Study Group on Consumer Issues with ICT Services

- The Study Group for Various Problems released a report Smartphone Privacy Initiative in August 2012, indicating Guideline for Handling Smartphone User Information as an ideal state of handling smartphone user information, and suggesting the efforts that can be made for each business entity towards the maintenance of a safe and secure user environment.
- It also suggests creating industry-specific guidelines, creating the mechanism for verifying apps through a third-party institution, information sharing about app developers through the websites operated by app distributors, and considering better displays depending on the size of smartphone screens in order to meet the effect of the guideline.
- Industry organizations have been making progress in preparing voluntary guidelines.

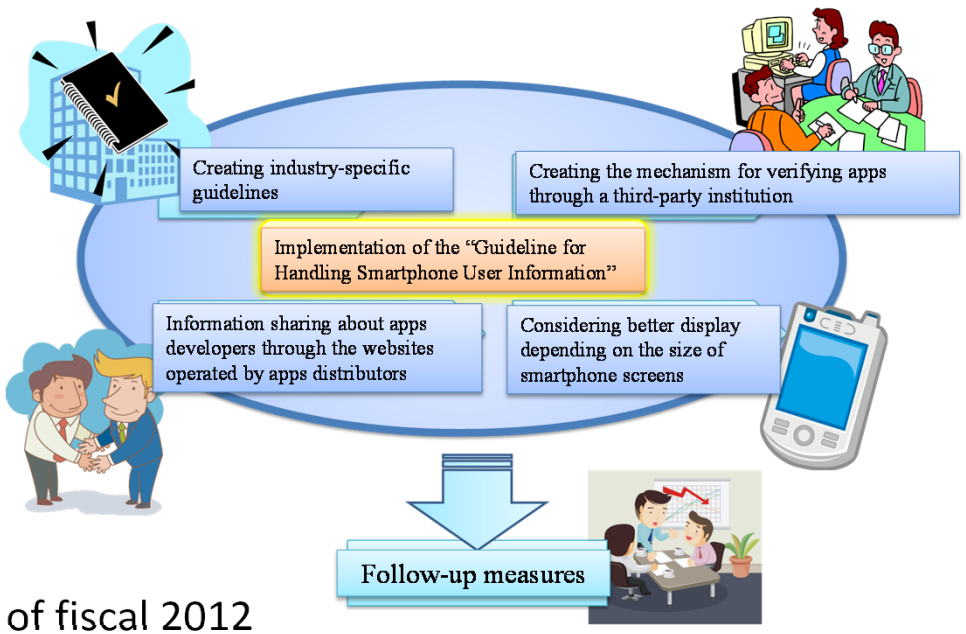
## ✓ Preparation for voluntary guidelines by industry organizations

- Tao software : Security guideline for Android（October 2012）
- Mobile Content Forum(MCF): Guideline for privacy policy of smartphone application(November 2012)
- Telecommunication Carriers Association(TCA)(March 2013)
- Japan Online Game Association (JOGA)(April 2013）
- Japan Internet Advertising Association (JIAA)(Under examination)
- Kyoto city： Kyoto city smartphone application utilization guideline（January 2013）

## ✓ Smartphone Privacy and Security Council (SPSC)

- Established in October 2012, with the aim of promoting the preparation of industry guidelines.
  More than 35 industry associations, companies, and organizations participated.

(1) Information exchange over industry guidelines and model privacy policies.
(2) Information exchange over display methods of privacy policies.
(3) Study and sharing of recommended cases and problem cases.
(4) Information exchange over international trends.
(5) Implementation of information dissemination.




## ✓ The progress of the penetration of smartphones and issues surrounding smartphone user information

- Penetration of smartphones: Approximately 38% as of the end of fiscal 2012
- Increase in malware aimed to acquire user information

■ **With consideration to the Guideline for Handling Smartphone User Information, it is desirable that application providers prepare and announce privacy policies for the applications in advance, and post the privacy policies in easy-to-see places or specify hyperlinks to the privacy policies in order to ensure the handling transparency of user information.**

■ **It is also desirable that application providers prepare a summary version of privacy policies and post it in easy-to-see places**

✓ **Creation and posting status of privacy policies for applications**

・It cannot be said that the penetration of privacy policies of all applications is high. It is necessary to effectively promote the preparation of privacy policies in the future.
(Example: The average posting rate on application providing sites is about 20%.(KDDI R&D Labs, The National Institute of Advanced Industrial Science and Technology))

・Case examples of privacy policies for applications prepared and announced in advance.
①Displayed within applications: **A little less than 50% in the United States, and a little less than 40% in Japan**
②Posted on application providing sites: **As high as just over 50% in the United States, while approximately 25% in Japan**
In both cases, the ratios in the United States are higher than the ratios in Japan.

✓ **Contents**

・If privacy policies are prepared for applications, many of the privacy policies provide information about the eight items of the Guideline for Handling Smartphone User Information. However, there are not many privacy policies describing methods of user involvement or providing information on the existence or absence of information collection modules.

✓ **Summary version**

・The promotion of preparing a summary version modeled after existing industry guidelines and precedents. Trends in international discussions are taken into consideration as well.

| The place where a privacy policy was displayed | Japan(40 applications) | | U.S.(36 applications) | |
|---|---|---|---|---|
| | Numbers | Ratio | Numbers | Ratio |
| In the application | 14 | 35.0% | 17 | 47.2% |
| In the introduction page of Google Play | 10 | 25.0% | 19 | 52.8% |
| In the Web page of the developer | 32 | 80.0% | 25 | 69.4% |

(The National Institute of Advanced Industrial Science and Technology (January 2013))

## ■ Challenges and response to privacy policies for applications

It is necessary to promote the preparation of privacy policies for applications so that users can see them with ease.

**① Promoting the preparation of privacy policies for applications**

・Promoting the preparation and publication of privacy policies for applications

⇒If necessary arrangements have not been made for existing applications, **plans should be considered promptly** to promote necessary arrangements.

⇒**Preparing privacy policies in advance** for applications that may be prepared in the future.

**② Display methods**

・**Where to put privacy policies for applications :** Posted on application providing sites E.g., hyperlinks
**Displayed at the first startup of applications** if privacy policies are specified in the applications.

・A mechanism is required to use **a pop-up, for example, to display important information so that readers will never fail to read the information**.

**③ Standard format or style**

・Providing information users want to know in a simple and understandable manner

・The **eight items and other desirable matters are described** according to the Guideline for Handling Smartphone User Information, industry guidelines, etc.
（Preparing privacy policies maintaining their consistency with the privacy policy of the entire enterprise.）

**④ Creating a summary version** ：**Creating a summary version briefly described** so that the entire contents can be viewed on the smartphone screen.

**⑤ Sharing information and raising awareness for users**

・The handling of user information must be explained in the privacy policies for the application, and information needing a high level of privacy, such as phonebook information, must be displayed as a pop-up to get the user's consent and keep the user informed of the importance of said information.

・Revising and publishing "Smartphone Privacy Guidelines."

**⑥Handling of information on youth:** deepening **the study with consideration of the characteristics of youth and international trends.**

**⑦Implementing periodical application surveys and follow-up**

## ■ It is also desirable that information collection module providers prepare and announce privacy policies and notify app providers regarding the items, purposes, and presence or absence of transmission externally, of the personal information to be acquired.

・Any information collection modules dispatch subscriber or terminal-specific IDs and other information, such as position information.

・Preparing and sharing a list of information collection modules is useful as common infrastructure.

## ■ Measures undertaken by other relevant businesses

✓ **Mobile telecommunications carriers・mobile terminal providers**

**①Activities of operators of application providing sites: Support to application providers**

・Preparing and presenting posting guidelines to application providers in accordance with the smartphone privacy initiative. Making inspections in response to prior applications from application providers (delivery type).

・Establishing a hyperlink to privacy policies created by application providers.

・Raising awareness about privacy protection among application providers.

**② Sharing information and raising awareness for users**

・Keeping users informed at the time of entering contracts or at any other suitable time.

・Responding to consumers varying widely in literacy.

✓ **Website operators for app distribution and OS providers**

・Establishing a hyperlink to privacy policies created by application providers.

・A certain explanation about posting standards is given to application providers in advance.

✓ **Other relevant business actors**

・An application introduction site is available, where applications are recommended according to the unique standards of the site.

（Providing users with information on the validity of permission and verification results of virus scanning.）

## ■ Contact for user queries on application provision sites

✓ **Application provision sites of mobile telecommunications carriers**

✓ **Application provision sites of OS providers**

} **Set up a contact for user queries**

**①Clarification of posting standards for the handling of user information**

⇒The promotion of appropriate applications with enhanced transparency is desired.

**②Promotion of the cooperation between contact windows**

⇒Promoting the cooperation between these windows along with information sharing for problematic applications.

# Ideal Third-party Verification of Applications



- From the viewpoint of enhancing the effectiveness of the Guideline for Handling Smartphone User Information, it is desirable that a mechanism be introduced by the private sector to enable third parties to verify the proper handling of user information related to individual applications in terms of operational and technical aspects.
- Allowing a number of entities to maintain or provide functions in a dispersive manner to enable third parties to verify applications. Each application is verified according to the functions and capabilities of each entity. Necessary common verification standards are prepared and applied.

## Verification of each application

Consideration of describing **privacy policies** for each application

- ① Presence or absence of the creation and publication of privacy policies for the application
- ② Contents of the privacy policies for the application

**Technical validation** on user information

- ① Presence or absence of user information to be transmitted externally
- ② Consistency with privacy policies for applications

## Self-verification of application providers

Application providers' **compliance with privacy policies**

→ Post-confirmation of **in-house and management systems**

→ Building confidence in applications

→ Providing criteria objectives to users

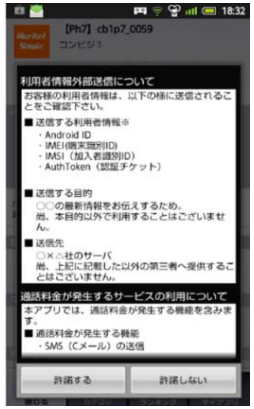
■Case examples of efforts to strengthen reliability through the verification and transparency improvement of applications
① Operators of application providing sites（OS providers, mobile telecommunications carriers, etc.）
② OS providers, mobile terminal providers
③ Security-related businesses, review site operators
④ Certification bodies
A variety of entities will implement various verification efforts and transparency improvements for the handling of user information.

## OS providers

①**Consent of information acquisition**: Acquiring the consent of each individual for applications acquiring a high level of privacy
②**Dashboard**: One-stop viewing of the status of permission for access to user information
③**Notification at the time of information access**
④Access authorization to applications that received **market screening**

## Mobile telecommunications carriers

①**Application screening**: Conducting the technical verification of applications at the request of the application providers
②**Users' help panel**: Provides a simple help panel regarding user information to be transmitted externally




## Mobile terminal providers

・Phonebook access monitor: Visualizing the access timing of application to phonebook information at any time

## Review site operators

・Providing only screened applications to sites
・Providing information to companies

## Security-related businesses

・**Display through security software**
Making a database of privacy risks, and display the results of verification on users' terminals through security software.
・**Published to the site of the analysis results**
・**Providing in-depth analysis to business operators**

## Certification bodies

・Indicating the level to be satisfied from the viewpoint of transparency
・Management check on an organization-by-organization basis

## ■Ideal Third-party Verification of Applications

- **Verification of each application**：verification of the proper handling of user information
  - **①Verification of the description of privacy policies for applications**
  - **②Technical validation on user information**
  - ⇒Verification and certification experts or agencies to objectively verify and screen the above ① and/or ②.
- **Verification of the application provider**
  - **③Confirmation of the application providing system**：e.g., confirmation of the location and the positioning of the Guideline in the management system.

### Standards of the verification of the description of privacy policies for applications

**①Presence or absence of the creation, and publication of the privacy policy for the application（APP）**

- ●An APP is created.
- ●Posting the APP in easy-to-see places or specifying hyperlinks to the privacy policies
- ・The summary version must be consistent with the APP.

**② The items described in the APP**

- ●The APP must provide information about the eight items of the Guideline for Handling Smartphone User Information.
- ●The relationship between user information acquired and the contents, service, etc. of the service
- ●The names of the information collection modules, providers, etc.

**③Acquiring users' consent**

- ●Acquiring the consent of each individual for applications acquiring a high level of privacy
- ●Acquire the consent of each individual in the case of providing applications to third parties

### Standards of the technical validation on user information

**①Presence or absence of user information transmitted externally**

- ●Presence or absence of user information transmitted externally by the application
- ●The items of user information transmitted externally
  - ※Applications must be verified with sufficient consideration of the fact that a wide range of user information can be pointed out in the case of making only a static analysis of the applications.
- ● The destination of user information transmitted externally

**②Consistency with privacy policies for applications**

- ●The items of user information described in the APP must coincide with the items on user information transmitted externally.
- ●The usage purpose of user information transmitted externally is clear.
- ●There is certain consistency between the contents of applications and the purpose of the service provided.
- ●The names of the information collection modules, providers, information transmitted, etc. coincide

### Standards of the confirmation of the application providing system

**①Check and credit check of the application provider**

- ・Contact information on application providers must be grasped along with information on the achievement results of the application providers.

**②The handling system of user information considering of the Guideline.**

- ・A system must exist to create and observe APP.
- ・ The above ② must be confirmed by other verification or authentication means.
  （If other certification bodies (e.g., EMA) have confirmed, their results will apply mutatis mutandis.）

## ■Concrete Measures for the Future

○ Promoting the preparation of application privacy policies ：a system that will allow the efficient implementation of verification in a standardized format.

○Considering the following common items: the announcement and listing of third-party institutions implementing the verification of applications, display method of third-party institutions' verification results of applications, cooperation of businesses managing provision sites of each application, and listing of information collection modules.

○Maintaining a system of implementing applications for user support and verification support, periodical application surveys, and common items.

⇒For the time being, the preparation of a follow-up report about once every six months.

①Promoting the preparation of application privacy policies

・Standardizing a format
・A system that will allow the efficient implementation of verification

Common considerations

②The announcement and listing of third-party institutions implementing the verification of applications

③ Considering the display method of third-party institutions' verification results of applications

④ Cooperation of businesses managing provision sites of each application

・Promoting the sharing of information and response methods.
・Making a database of risky applications etc.

⑤ listing and sharing of information collection modules

⑧Maintenance of a system to implement common considerations.

・Grasping, considering, and reviewing the method and details of third-party institutions' verification of applications.
・A system of effectively promoting items ① to ⑦ as common considerations.

Further responses

⑥ Considering applications and websites for user support and verification support

⑦ Implementing periodical application surveys（APP and Technical validation）

○ Smartphones should be devices that **a variety of people, ranging from youth to elderly people, can use with ease**.
- It is Important for other relevant businesses to share information and raising public awareness in order to improve user literacy.
- Necessary to improve the understanding and awareness of third-party institutions' verification of applications by giving easy-to-understand explanations, including **the display of information (the summary version)** with consideration of the smartphone screen size and the confirmation of users' consent with a **pop-up** at the time of acquiring information at a high level of privacy.

○ **Transmitting information to smartphone application providers and keeping them well informed of the above.**
（Website operators for apps distribution , OS providers, industry organizations , research institution ）

## Information Sharing and Awareness Raising for Users

**1 Contents of information dissemination and common knowledge education**
（1）Difference between smartphones and traditional mobile phones
（2）Notes on the handling of user information
（3）Information security measures
（4）Information necessary to youth and elderly people

**2 Implementing initiatives in response to the literacy of users**
（1）Initiatives at the time of terminal and service development
（Example: Providing youth and elderly people with smartphones）
（2）Initiatives at the time of using services
（Example: Holding voluntary seminars）

**3 Information dissemination and common knowledge education based on this proposal**
（1）Smartphone Privacy Guidelines
（2）Consent of information acquisition, Creating a summary version, Keeping general users informed about use of third-party institutions' verification of applications etc.

## Awareness Raising for application providers

**1 Sharing information by website operators for app distribution and OS providers**
（1）Guidelines posted on application providing sites
（2）Making and publicize Proper privacy policies
（3）Raising awareness about privacy protection among application providers.

**2 Information dissemination by industry organizations**
（1）Preparing guidelines and transmitting information for application providers
（2）Transmitting information through cross-industrial fields E.g., SPSC
Providing information, including voluntary guidelines by industry organizations and guidelines posted on application providing sites, clearly and by one stop

## ■U.S.

（1）**U.S.- Japan Business Dialogue on the Internet Economy** (Washington, D.C. : October 2013)

・Japan provides information about “Smartphone Privacy Initiative”. The NTIA provides information including that on a multi-stakeholder meeting concerning the code of conduct for improvements in the transparency of mobile applications with consideration of the policy outline of the White House.

・Agreed to share best practices and updates for the protection of consumers’ data as a result of a discussion over the transparency and importance of smartphone applications concerning the privacy of smartphone users and literacy improvements in smartphone users.

（2）**Movement of study within the U.S.**

**①Multi-stakeholders’ meeting organized by the NTIA.**

・Meeting 15 times by June 2013 to discuss a draft of the code of conduct on the transparency of mobile applications and brief notices.

**②FTC Staff Report “Mobile Privacy Disclosures : Building Trust Through Transparency” (February 2013)**

**・Provided recommendations on the role of Mobile App Market Companies, App developers, industry organizations etc.**

**③Attorney General California Department of Justice ”PRIVACY ON THE GO : RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM”(January 2013）**

**④FTC ” Children's Online Privacy Protection Act (COPPA)” Amendment（December 2012）**

## ■EU

（1）**Japan-EU ICT Policy Dialogue** (Tokyo: **November 2012**), **Japan-France ICT Policy Dialogue** (Paris: **February 2013**), **Japan-Finland ICT Policy Dialogue** (Tokyo: **June 2013**)

・The MIC provides information about “Smartphone Privacy Initiative”. EU provides information including e-privacy directive data protection directive. Implementing exchanges of information and opinions in the future as well.

（2）**Movement of study within the EU**

・The GSMA (GSM Association) announced privacy principles and guidelines for mobile devices (January 2012).

## ■Movement of study in Korea

・Korea Internet & Security Agency(KISA) announces “Privacy Guideline for application developers”(March 2012),staying informed of the same guideline through domestic telecommunications carriers. KISA develops and releases an application (SS Checker), which plays a monitor function role in smartphones.

・Laws and regulations relating to privacy protection vary with each country and region. Major developed countries have been making progress in the study and initiatives of improvements in the transparency of privacy policies almost in the same direction.

・Proactively explaining Japan’s efforts in multilateral and bilateral framework (e.g., international organizations, such as the OECD,