2021 Commissioned Research Report
PG11004-0171

Research on the Governance Model of Data-Based Innovative Application Services of Telecommunications Enterprises in 2021 Final Report
(English Abridged Version)

Commissioned by National Communications Commission

January 2022

Chapter 1 Origin of the research

In the face of the wave of digital transformation sweeping the globe, governments of all countries are attaching high importance to the digital economy, and technologies such as 5G, the Internet of Things (IoT), blockchain, big data, and artificial intelligence (AI) are booming. The telecommunications industry is no longer limited to providing basic telecommunications and network services, but has become the core of technological development in the era of "Omni-" Internet of Things. Meanwhile, in face of the ever-changing consumer behaviors and demands, as well as the declining revenues from the core business, the telecommunications industry has, based on a large amount of data accumulated previously, conducted analyses with customer personal data, services usage situations ,or the huge data/information derived from the telecommunications services, business behavior data, and machine-generated data, so as to provide higher quality services and better customer experience, which also makes the key to the applications of digital transformation. The processing and analysis of big data through AI can lay a foundation for new products and services, while improving operations and increasing revenues of the business.

According to the latest "State of Digital Communications (SDC)" [1] released by the European Telecommunications Network Operators Association (ETNO) in January 2021, Europe lagged behind in key digital indicators. For example, in terms of the indicators of key network deployment and digital investment (including investments in 5G, AI, and networking), Europe seriously lagged behind the US and Asia, despite the expansion of investments by large European telecommunications operators. In terms of the population coverage by 5G, Europe witnessed growth from 12.9% in 2019 to 24.4 % in Q3 of 2020, which, however, still lagged far behind the coverage of 76% in the United States and 95% in South Korea, during the same period. In face of the fierce competition in the global arena, European telecommunications companies are expanding their business areas through AI technology applications, such as data applications, cloud services, and information security, so as to bridge the gap in

[1] New Report: Europe behind on key digital metrics, telcos essential to achieve leadership, ETNO, https://etno.eu/news/all-news/8-news/694-state-of-digi-2021-pr.html (last visited Aug. 13, 2021).

innovation. The latest SDC report also found that telecommunications revenues in Europe obtained from digital services (such as enterprise solution proposals, security, etc.), was expected to grow from EUR 65 billion (about TWD 2 trillion) in 2017 to EUR 100.4 billion (about TWD 3.2 trillion) in 2021. However, the pressure of competition with other large technology companies has been considerably high. Moreover, the drafts such as the Digital Services Act (DSA) and the Digital Markets Act (DMA) were introduced by the EU in December 2020 to protect users of digital services, and to regulate the competition in the digital market. Accordingly, telecommunications operators would need to ponder on the relevant strategies for the future, in response to the aforementioned pressure and Acts.

In addition, according to the "2021 Outlook for US Telecommunications, Media, and Entertainment Industry"[2], released by Deloitte US for 2021, it was indicated that the telecommunications industry had been facing structural challenges for a long time. In response to the new corona pneumonia (COVID-19) pandemic, the telecommunications industry would need to ponder on recovery strategies, such as refocusing on customer needs, integrating entertainment experience, and exploring new products and services of direct-to-consumer. Meanwhile, the application of the 5G technology to develop new products, services, and business models could reposition telecommunications services. This 2021 Outlook report also estimated that 5G would reach an economic value of USD 700 billion (about TWD 19 trillion), and 68 % of the market would be directed by applications in retail, government, and finance.

In Taiwan, the cross-field applications by telecommunications enterprises are trending upwards. Joint enterprise partnerships and cross-field cooperation are prevalent in smart finance, smart medicine, smart retail, smart manufacturing, smart warehousing, smart exhibition, and entertainment, etc. Innovative applications, and scenarios with virtual reality are being developed. All these situations contribute to the gradual transformation of the telecommunications ecosystem into a new era of 5G. As an important driver of future digital transformation, the telecommunications industry has begun to ponder on and undertake the development of cross-field integrated

[2] 2021 telecommunications industry outlook, Deloitte US, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html (last visited Aug. 13, 2021).

applications. However, telecommunications enterprises are highly regulated by governments across the world. When it comes to the innovative applications of the data held by the telecommunications enterprises, not only the norms and specifications for the telecommunications enterprises must be observed, but also the related laws and regulations for data protection shall be upheld by the telecommunications enterprises as well. At present, on the one hand, with regards to the applications of telecommunications data, and even that of consumer data, the practices international-wise require the consideration of issues such as data circulation, privacy protection, information security, and market competition, under circumstances involving the trade-off between privacy infringement and reasonable data usage, or the sophisticated cross-field innovative applications, in the aspect of the legal system. On the other hand, with regards to the existing regulatory sandbox mechanism, the practices domestic-wise in Taiwan still aim at the financial sector. In order to safeguard the national security or public interests during the data applications by the telecommunications operators, this Project is undertaken with the aim to put forward recommendations to the competent authorities of the telecommunications enterprises and the government authorities in charge of the industry concerned in decision-making processes related to innovative applications and services, data use and governance, through the study and analysis of the related international policies and cases, as well as through the collection, and compilation of opinions through public opinion consultations, seminars, etc. Such recommendations put forward can be served as a reference for the government authorities in charge of the industry concerned in formulating relevant policies.

Chapter 2　Demand Work Items

Entrusted by National Communications Commission (“NCC”), this Project Team at the Institute for Information Industry (“III”) undertakes the “Project of 2021 Annual Study on the Governance Model of Data-/Information-Based Innovative Application Services of the Telecommunications Enterprises” (“the Project”). According to the required guidelines, the Project has delivered study results in six itemized works, detailed as follows:

1. Collection of the data about the telecommunications enterprises in the target

countries (e.g. Estonia, the United States, the United Kingdom, Japan, South Korea, etc.) was completed, including their collection, processing, and use of telecommunications data, how the applicability of the related laws was evaluated in case the privacy protection was involved, what guidelines were referred to, and how the decision-making processes were conducted, to safeguard their national security or public interests in cooperation with the related authorities. Based on the data collected, a study and analysis report were also completed.

2. Collection of data generated by telecommunications service operators during the telecommunications services they provided in the target countries or regions (e.g. Estonia, Germany, the United States, the United Kingdom, Japan, South Korea, etc.) was completed, including twelve case studies of practical innovative applications in various types of cross-industry cooperation models. Based on the data collected, studies and analyses were conducted on the governance situations in the telecommunications industry in activating the use of data or applying the data to business models, as well as on the acts of the local governments in using the data for the development of economic policies, under the relevant legal system and the current regulatory status, in the negotiation and decision-making processes or guidelines, etc.
3. Based on the data studied and analyzed for the practical case studies mentioned in the preceding paragraphs, the following work items were completed:
   (1) From July 19 to August 1, 2021, the online public opinion consultations were completed, and the opinions therein were collected and compiled.
   (2) On August 2 and 4, 2021, two sessions of forums were held.
   (3) The resulting data was compiled and preliminary recommendations were put forward.
4. Based on the aforementioned data collected from the development trends, the public opinion consultations, and the seminars held, the following work items were handled:
   (1) Results in report was completed, and specific opinions and recommendations on the decision-making processes were put forward, including the types of relevant data/information, forms of the applications, problems possibly

encountered during the applications, and recommendations on the solution processes.

(2) On October 13, 2021, one session of the forum was held for the discussion of the feasibility of the solution proposals (in the drafts) and the collection of specific comments, which were provided to the government authorities in charge of the industry concerned for reference.

5. Consultations services on five topics were completed, including 1) the study and analysis of the applicability of laws to the use of the statistical data from the telecommunications enterprises' collection of customers' viewing behaviors; 2) the study and analysis of the terms and conditions of the standard service contract of the telecommunications enterprises; 3) the cross-field sharing of personal data under reasonable use by the governments based on the data provided by the telecommunications enterprises; 4) the promotion of the independent use of the data subjects' data in the cross-industry cooperation involving cross-field applications of business information; and 5) the study and analysis of the latest international trends in personal data law, etc.

6. With the review of the current laws and regulations in Taiwan, recommendations were put forward on the feasible practices in data use, data value addition, data protection, and innovative application services in the telecommunications field, on the restrictions and challenges to the related laws and regulations, and the standardization of decision-making processes related to amendments of laws and regulations in the future. Such recommendations put forward can be served as a reference for the government authorities in charge of the industry concerned in formulating policies in the future.

Chapter 3 Implementation and Research Findings

Section 1 Study and analysis on the application of telecommunications data by the telecommunications enterprises in cooperation with the implementation of safeguarding the national security and public interests

As the policy for data sharing is changing in the future, one of the most significant

challenges will lie in the societal demands for and ethical handling of data privacy. In terms of tracking people's digital devices, the world sees different policies in different regions, societies, and governments. Among the countries under study and analysis in this Project, Estonia, as a model country for e-government, believes that during the development of e-governance, it is not necessary to establish a comprehensive legislative system in specific fields. Rather, the only measures to take are, for important topics such as data sensitivity, under the situation of maintaining the neutrality of the technology, to analyze the existing laws and identify differences among them; as well as for areas where laws may hinder the development of e-governance, to gradually review and adjust the laws. It is suggested that legal experts should be consulted in the planning process, and legal risk analysis should be carried out as early as possible, so as to avoid excessive regulation or cause regulatory obstacles.

In the United Kingdom, with a different approach, an overall strategy was formulated for the national data from the top down. In face with the challenges brought about by the impact of the pandemic, the UK also believes that not only the flexibility in legislation and policy aspects is necessary, but also the privacy and information security issues that people are concerned about cannot be ignored. In order to win public trust, data storage and use should be fully transparent, and data risk assessments should be conducted. As for the government's using the data of anonymous people-gathering locations provided by telecommunications companies to evaluate resource allocation, and the social distancing measures, there may still be a risk of re-identification of individuals. Moreover, the current de-identification technology is not sufficient to provide complete privacy protection for individuals, and the issue of the digital gap should also be considered. Therefore, the development of digital technology not only accelerates the government's contingency abilities, but also requires the consideration of the ethical and technical challenges therein.

In Japan, the *Act on the Protection of Personal Information (APPI)* has been enacted as a common norm for personal data protection that the state, local autonomous groups, and business operators must follow. In order to assist business operators in the proper use of data, the Personal Information Protection Commission (PPC) has

formulated the General Guidelines for the *APPI*, where the General Guidelines consists of three parts to address different situations, namely: Confirmation and Recording Obligations, Transfers to Third Parties in Foreign Countries, and Anonymized Information handling. In addition, for telecommunications and communications operators, the Ministry of Internal Affairs and Communications (MIC) has formulated the Guidelines for Protection of Personal Information in Telecommunications Business, to take into account the convenience of telecommunications services and the protection of personal data.

In South Korea, in the aspect of applications of telecommunications data by the telecommunications enterprises in cooperation with the national security and public interest, the general practices include the submission of data, such as specific locations, and communication records, to cooperate with the criminal investigation of the prosecutorial and police offices. Especially, while building smart cities, the South Korean government has taken advantage of the data, such as network interconnections and users' locations, from various bases of the telecommunications enterprises, so that the complete tracking center could be built, where the center can facilitate the search for wanted vehicles and the arrest of suspects. Due to the global COVID-19 pandemic, in order to fully control the spread of infectious disease in South Korea, applications of telecommunications data have gradually extended on issues from simple social security to health care. In cooperation with government policies, the Korean National Assembly has amended the *Infectious Disease Control And Prevention Act,* so that the relevant competent authorities can directly authorize the acquisition of telecommunications data in accordance with the law, and can, based on such data, cooperate with telecommunications operators in developing smart quarantine systems, so as to realize the control of the source of infectious diseases. With the operation of K-MyData, it is expected that in the future, the data subjects will be able to dictate their own personal data including telecommunications data, and authorize the transmission and application of their own personal data, so that the applications of personal data will become more effective.

In the United States, in comparison with the afore-mentioned countries, at present,

it lacks universally applicable special laws on personal data protection. However, relevant personal data protection norms have been formulated in the US according to various fields and categories. With strong waves of the COVID-19 pandemic, the US government is reconsidering the benefits of using telecommunications data to assess crowd mobility while making trade-offs between public interest and privacy.

In the observations of the case studies in safeguarding national security and public interests through the transmission of data via information and communications technologies (ICT), it is seen that various countries have developed various applications in tracking contacts in response to the pandemic. It should be explained first that, some of such applications involve the collection, processing, or use of location information; whereas others only use Bluetooth transmission and anonymous exchange of ID without involving the user's telecommunications data. As for other applications, most of them apply the location information to the analysis of population mobility, where the analysis is conducted anonymously on statistical data, or the data subjects are notified for their consent for the purpose of disaster prevention and relief.

Section 2 Study and analysis on the situations of innovative applications of the telecommunications service providers, on the case studies of the practical applications, and on the policies and legal system

Depending on the social and economic requirements for data application, with the prevalent applications and analysis of big data, the application of data by the telecommunications enterprises are often not limited to specific projects or application fields, but rather, diverse cooperation with various industries has been undertaken to discover the new development direction of the telecommunications industry in the future. In the observations of the cross-industry cooperation of the telecommunications industry on data applications in various countries, more diversified business models and more convenient services have also emerged. However, when telecommunications operators provide data to third parties for data analysis as the basis for service applications, the protection of privacy of the data subjects' personal data cannot be ignored.

Countries under the study and analysis are also facing challenges. For example,

Estonia has a large amount of personal data in its national database. As long as the consent of data subjects, it is possible to open such data for the development of innovative services. However, the controversies of this approach lie in that it is impossible to know whether such services transmit such data to third-party service providers, and it is also impossible to obtain consent from the data subjects to use their personal data.

In Germany, two telecommunications-related regulations were amended in 2021. One of the two amendments was made on the *Telecommunications Modernization Act* (*Telekommunikationsmodernisierungsgesetz*, *TKMoG*) which aimed to transpose the European Electronic Communications Code (EECC) in the existing regulatory framework of electronic communications, and to comprehensively revise the regulatory framework of telecommunications, while hoping not only to maintain the accessibility and security of the networks and services, but also to increase the willingness to cooperate and invest, and increase the interests of end-users. The other amendment was made on the *Telecommunications-Telemedia Data Protection Act* (*Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien – "TTDSG"*), which aimed to protect data and privacy in the digital world, and to balance the interests of the digital service users with the economic interests of the companies, while solving the dilemma for consumers, telecommunications service providers, and regulators in choosing the application of the concurrent *Telecommunications Act, Telemedia Act (Telemediengesetz* – "*TMG*"), and *General Data Protection Regulation* (*GDPR)*.

In Japan, several major amendments to the *APPI* was made in 2020 and 2021. The amendment in 2020 aimed to balance the data-based innovative applications with the protection of personal data, whereas the amendment to the *APPI* in 2021 aimed to unify the norms for personal data protection among the state, local governments, and the private sector, in response to the formulation of the Basic Act on the Formation of a Digital Society. The above amendments are to facilitate the promotion of data circulation and help telecommunications operators in carrying out data-based innovative application services in a more diverse way.

In the United States, the telecommunications network is rapidly adapting to changes in the way people live, work, learn, and play. Through a more flexible regulatory approach, competitions are promoted regulations are reduced, and the rapid deployment of new telecommunications technology is encouraged. In the United Kingdom, the national data strategy is taken as the overall driving direction, supplemented by the Smart Data program as the framework for sharing consumer data, allowing consumers to stay in control of their data, in response to future cross-field data applications, while benefiting third-party business operators in developing data-based innovations business models and services. In addition, the UK government also considers the impact of data on the competition in the digital market, as well as the impact of the government's opening up data on the private sector, while developing a sharing model for obtaining values from public and private data.

In South Korea, with the advent of the fourth industrial revolution, telecommunications operators have all invested in the development of data analyses and applications with big data, and other related industries. The three major telecommunications operators respectively launched their "Mega Information Service Platforms" based on their respective telecommunications data, for the analyses and applications in different fields. As a result, telecommunications data is no longer limited to specific individuals, but is extended to include applications in business, real estate, financial, and other services, which has promoted cross-industry integration. Especially, during the COVID-19 pandemic, when the local economy is affected, telecommunications operators have used the telecommunications data in deriving and extending data analyses and results with big data which have been provided at considerable discounts to different industries for the planning of suitable marketing services and business promotion. This has moderately mitigated the impact of serious infectious diseases on society. In 2020, the *Personal Information Protection Act* of South Korea introduced the concept of pseudonymous intelligence, which clearly stipulates that pseudonymous intelligence can be used in fields such as statistical compilation, scientific research, or preservation of public welfare records. The implementation of the new act has alleviated the obstacles possibly encountered by the

telecommunications operators in the statistical compilation or scientific research, including obstacles related to what kind of telecommunications data can or cannot be used, thus facilitating the development of analytical services with big data by telecommunications operators using telecommunications data.

Section 3 Study and analysis on the governance model of data-based innovative application services of the telecommunications enterprises (based on the online public opinion consultations and two sessions of case-sharing forums)

After collecting the case studies and governance models of data-based innovative application services of the telecommunications enterprises in the abovementioned countries, the Project Team further compiles, and analyses opinions from various parties through online public opinion consultations and invitation of experts and scholars to participate in forums, hereby proposing recommendations on the governance models of data-based innovative application services of the telecommunications enterprises, as follows:

1. Amending the Measures for Safeguarding Personal Data Security by Non-Government Agencies Designated by the National Communications Commission (short-term recommendation)

It is recommended that with reference to the Guidelines on Consent under Regulation 2016/679, Guidelines on Transparency under Regulation 2016/679, and the Guideline for Big Data Personal Information Protection released by Korea Communications Commission (KCC), and other relevant norms, NCC can supplement norms related to value-added applications with telecommunications data in the *Measures for Safeguarding Personal Data Security by Non-Government Agencies Designated by the National Communications Commission.* The contents recommended are as follows:

(1) effective obtaining of consents and transparency requirements;
(2) standards or guidelines for de-identification of telecommunications data;
(3) privacy impact assessment; and
(4) strengthening of the rights of the data subjects.

For details, please refer to the revised draft of the *Measures for Safeguarding Personal Data Security by Non-Government Agencies Designated by the National Communications Commission* proposed in this research.

2. Establishing an online public opinion consultation platform (short-term recommendation)

It is recommended that with regarding to the experience through this research, NCC can establish an online public opinion consultation platform to enable the transparency of the policy formulation process, make relevant laws and policies more in line with practical needs, and enhance the effectiveness of governance.

In addition, when conducting regulatory sandbox experiments, telecommunications enterprises can also use the platform to enable their communication and dialogue with the online public, to promote the public's trust in NCC and telecommunications enterprises.

3. **Formulating norms for telecommunications regulatory sandbox, while encouraging telecommunications operators to conduct innovative experiments with the regulatory sandbox mode (mid-term recommendation)**

It is recommended that concerning to the *Financial Technology Development and Innovative Experimentation Act* issued by the Financial Supervisory Commission (FSC), NCC can formulate the *Telecommunications Value-added Development and Innovation Experiment Act* to conduct the regulatory sandbox mode. Telecommunications operators *are* also encouraged to experiment with the innovative services of identity recognition and transportation, so that such services later can be implemented through the integration with the laws and regulations.

4. **Establishing a data bank system (long-term recommendation)**

In order to encourage telecommunications operators to carry out innovative value-added applications and avoid being limited by laws and regulations, NCC can evaluate the establishment of a data bank system as implemented in Japan, deploy a trustworthy third-party organization as the basis for data circulation, and encourage and promote the value addition and re-use of telecommunications data.

Section 4 Study and analysis on the governance model of data-based innovative

application services of the telecommunications enterprises

1. Types and forms of data applications

Regarding the types of data collected by telecommunications operators, in principle, the data provided by the public when applying for telecommunications services and the data generated when using telecommunications services are both collected, processed, and used to provide services following the *Personal Data Protection Act*. Regarding telecommunications operators' making use of value-added telecommunications data, in principle, the value addition to telecommunications data shall be subject to the consent of the data subjects in accordance with the provisions of Article 20 of the *Personal Data Protection Act*, unless otherwise for the considerations of public interests or under the data de-identification. Besides, attention should also be paid to the legal provisions on the data retention period for telecommunications enterprises.

In the context of safeguarding public interests and promoting national development, to ensure the legitimacy of government agencies' use of the telecommunications data, it is recommended that clear norms, and transparent review and regulatory organizations or systems, shall be in place. As for risks, it is recommended to distinguish data by risk level, to regularly review the situation, and adjust the risk level accordingly. In addition, issues such as data standardization and formatting need to be addressed, and data de-identification should be ensured.

2. Issues of data applications encountered by telecommunications operators

Regarding the data application problems currently encountered by the telecommunications operators, based on the compilation of opinions from the online public opinion consultations and the two sessions of case-sharing forums, attention should be paid to the data de-identification, notification of consent, consumer protection, the establishment of a special authority for personal data, etc. Through consumers' awareness of the applications and values of their data, the consumers should be given options to opt-out of such applications or value additions, and to determine the scope of the de-identification of their data. At present, there is no competent authority in charge of personal data in Taiwan, experts suggest that an

explicit competent authority should be established along with relevant guidelines and the strengthening of the transparency in data applications. In addition, attention should also be paid to ID identification and the establishment of public trust in the government. As well, the data subjects' rights to data portability, and value-added data applications in promoting commercial purposes, should be strengthened.

3. **Recommendations for solutions**

Regarding short-, medium- and long-term planning, in the aspect of norms, the exercise of the data subjects' rights should be strengthened. The data subjects should be aware of, and be able to adjust, their consent to data applications. Another point that is worth discussing is the sandbox mechanism for telecommunications data applications, which can refer to the experience of open banking for comparison. Moreover, incentives should be provided to telecommunications operators, and user-friendliness should be offered to small and medium-sized enterprises. In order to encourage telecommunications operators, appropriate supporting measures need to be formulated, along with the classification of personal data, enhancement of risk tolerance, and continuity in the policy aspect.

Section 5 Consultation services

1. **Topic 1: Study and analysis on the applicability of laws to the use of the statistical data from the telecommunications enterprises' collection of customers' viewing behaviors**

For mediation, NCC intends to collect the related statistical data on the viewing behaviors of the viewing users from the business operators of MOD platform or cable TV system, and the channel supply enterprises (hereinafter referred to as the "target enterprises"). After studying the related procedures and opinions of the applicable laws, the Project Team put forward specific feasible recommendations as follows:

(1) Analysis of the applicability of laws

a. In the context necessary for the execution of the statutory duties of mediation, NCC may collect, from the target enterprises, the data on viewing behaviors of identifiable viewing users. However, the determination of the "necessary context" requires prudence.

b. It should be explained that, even for the execution of the statutory duties of mediation, NCC may collect, from the target enterprises, the data on viewing behaviors of identifiable viewing users; however, under the current law, the target enterprises do not seem to be clearly obligated to provide such data for the mediation purposes.

(2) Specific feasible measures

a. It is recommended that NCC evaluates the subject mediation in advance to see whether it is necessary to "obtain the data on viewing behaviors of identifiable viewing users". If there is any doubt, it is recommended to obtain, from the target enterprises, the data on viewing behaviors with de-identification of viewing users, as it could better avoid risks. In another word, it is also recommended to reduce the use of data with identities of identifiable users, to reduce the risk of infringing personality rights.

b. During the mediation process, when obtaining the data on viewing behaviors with personal data, in principle, NCC may only use such data for the purpose of mediation. When intentionally using the data on viewing behaviors for other purposes, NCC should evaluate the conformity to the norms of the *Personal Data Protection Act.*

2. Topic 2: Study and analysis of the terms and conditions of the standard service contract of the telecommunications enterprises

Regarding how NCC inspects and reviews the contents of terms and conditions of the standard service contract of the telecommunications enterprises, how to avoid the infringement of personality rights, and the promotion of the reasonable use of the users' personal data by telecommunications enterprises, after studying the related procedures and opinions of the applicable laws, the Project Team put forward specific feasible recommendations as follows:

(1) This research believes that although telecommunications operators do not need to submit the personal data notification statements to NCC for approval, NCC can still require telecommunications operators to submit personal data notification statements for inspection through administrative inspection or administrative guidance.

(2) In order to assist NCC in reviewing the contents of terms and conditions of the standard service contract of the telecommunications enterprises, this research organizes the substantive notification items, along with the required formats and matters for attention, as required in Article 8 of *the Personal Data Protection Act*, into a table and a checklist for NCC to do tick marks during its administrative inspections to check whether the privacy policy or the personal data notification statement of the telecommunications operators complies with the norms of the Personal Data Protection Act.

(3) In addition, NCC also needs to verify whether the "consent" provided by the user conforms to the norms of the Personal Data Protection Act. Therefore, focusing on "Taking the consent as the basis for non-purpose use" and "Taking consent as the basis for collecting and processing users' personal data", this research organizes the form "Key Requirements for Valid Consents" for NCC's reference and consideration. Accordingly, NCC can use the form during its administrative inspections and administrative guidance to check whether the consent is valid according to the specific circumstances.

3. Topic 3: Cross-field sharing of personal data under reasonable use by the governments based on the data provided by the telecommunications enterprises

In this Project, the German Corona-Warn-APP, along with its privacy statement and related legal basis, is analyzed as a reference for Taiwan's related measures in response to the pandemic. First of all, both the German Corona-Warn-APP and Taiwan's social distancing APP use Bluetooth technology to exchange IDs, without collecting personal or location information. Next, download and use of either one of the APPs is at the discretion of the people; whereas upload of contact data after contacting those with confirmed COVID is also at the discretion of the people. Therefore, there is still room for people to decide whether to provide data for pandemic prevention. However, these measures are still relatively passive in pandemic prevention. If the number of people using the APP is insufficient, the benefits of contact tracing cannot be manifested. In addition, Taiwan's social distancing APP has not

involved Taiwan's telecommunications operators; therefore, no such problem as having telecommunications operators provide telecommunications data. Accordingly, the main focuses of the discussions to follow are on the study and analysis of the data application of the 1922 SMS Contact Tracing System in Taiwan:

(1) **The privacy right announcement about the 1922 SMS Contact Tracing System should state in detail the relationship between Taiwan Centers for Disease Control (CDC) and telecommunications operators, as well as about the collection and retention period of the data by the telecommunications operators**

The 1922 SMS Contact Tracing System is implemented by users sending text messages via their telecommunications companies. However, the privacy right announcement only states that the 1922 SMS Contact Tracing System is produced and maintained by TRADE-VAN INFORMATION SERVICES CO. entrusted by CDC. With reference to the privacy statement and Q&A online about the German Corona-Warn-APP, detailed explanations are available concerning the data controller and processor of the APP and a clear legal basis for data processing. In addition, with reference to the privacy right policy about the German Luca-Contact-Management-Tracing-APP which is similar to Taiwan's 1922 SMS Contact Tracing System-APP, detailed explanations are available concerning the data collected by Deutsche Telekom AG the location of the server, and the phone numbers involved are processed by Deutsche Telekom AG for verification and retention in the specified number of days. In Taiwan, the privacy announcement about the 1922 SMS Contact Tracing System does not clearly state what data the telecommunications operators handle and how long the data retention period is. Such data even appears in the news release. Therefore, it is recommended that such privacy announcement should state in detail the relationship with the telecommunications operators, as well as the data collected by the telecommunications operators and the data retention period, so as to balance the reasonable use of data with the transparency of data application, and to win the people's trust.

(2) **The authorization to telecommunications operators in collecting personal data should be subject to a clear legal basis**

Under the 1922 SMS Contact Tracing System, the data collected by the telecommunications companies consists of three items, namely the phone number, the text sent, and the time and location code at the moment of sending the text, without ID verification data. Therefore, for the telecommunications enterprises to provide users' personal data, cooperate with the government's reasonable use of the users' personal data, and share the users' personal data for cross-field business purposes, it is necessary to resort to Articles 4, 15 ,and 16 of the *Personal Data Protection Act* under the currently available laws, where the provisions therein state the government agency's collecting and processing personal data in the necessary context for performing statutory duties.

For the government to require the telecommunications enterprises to provide users' personal data and cooperate with the government's reasonable use of the users' personal data, it is necessary not only to base on the aforementioned norms of the *Personal Data Protection Act,* but also to explain the statutory duties and powers based on explicit legal provisions for the reasonable use of the users' personal data. Besides, it is necessary to incorporate the concept of data governance, conduct a prior privacy risk assessment, and even cover the related descriptions in detail in the content of the privacy policy. In the face of the subsequent data sharing, it is recommended to formulate contract guidelines related to data sharing, and even to clarify Taiwan's de-identification technology, and promote the establishment of a dedicated authority for personal data, so as to facilitate the overall control of the reasonable use, and the privacy protection, of the personal data.

(3) **Digital certificate issuance platform in Taiwan is still in the research stage, where the experience of the EU's digital COVID certificate rules can be learned from**

As for digital COVID-19 certificates, the digital certificate issuance platform in Taiwan is still in the research stage, and the digital COVID-19 certificate has not been promoted as a passport at this stage. The EU has gradually lifted the lockdown in the face of the pandemic, and has adopted the digital COVID-19 certificate to facilitate the free movement of people in the EU, where the personal data involved is regulated by

clear legal bases, i.e. by the rules for EU digital COVID-19 certificate and related GDPR provisions. Later, when Taiwan is to promote the digital COVID-19 certificate, a thorough assessment and clear legal bases shall be in place.

4. **Topic 4: Promotion of the independent use of the data subjects' data in the cross-industry cooperation involving cross-field applications of business information**

Unlike the EU's e-wallets offering digital identity certification, at present, most of Taiwan's e-wallets are still limited to the electronic payment function. Meanwhile, although Taiwan intends to implement the digital identity card (new eID) policy allowing the people's proof of their ID identification online, and the connection to the government backbone network (T-Road) for various e-government services. However, concerns about safety, legal basis, etc. have subsequently postponed the implementation of the new eID policy. As for EU's e-wallets, the main purpose is to integrate eIDAS rules to provide citizens and enterprises with an effective method of self-identification in a cross-border environment within a single pan-European framework, as well as an exchange of personal identity attributes and certificates in a highly secure, trustworthy, and GDPR-compliant way.

5. **Topic 5: Introduction to *Personal Information Protection Law* in Mainland China**

(1) The *Personal Information Protection Law* in mainland China refers to the GDPR in a great deal to strengthen the protection of personal data, while adopting relatively strict regulations for processors of personal data. Apart from high-density control, the *Personal Information Protection Law* also imposes heavy fines and penalties on violators that may be forced to leave the mainland Chinese market, making business operators to be cautious in dealing with personal data.

(2) For those Taiwan's telecommunications operators not intending to enter the mainland Chinese market, attention must be paid to scopes that fall into the control under the *Personal Information Protection Law*, and examination must be conducted to see whether they have conducts such as "for the purpose of providing products or services to natural persons in China" or "analysis and evaluation of natural persons in China".

(3) For those who Taiwan's telecommunications operators intend to operate in the mainland Chinese market, it is necessary to follow the provisions of the *Personal Information Protection Law*, examine in detail the differences in legal compliance, and plan an overall contingency plan, so as to lower the impact of business operations.

Section 6 Recommendations on relevant decision-making process standards for the governance model of data-based innovative application services of the telecommunications enterprises

Concerning the recommendations on the decision-making process standards for the governance model of data-based innovative application services of the telecommunications enterprises, this research proposes the recommendations from the aspects of the decision-making process, laws and regulations, policy, and data governance. The current laws and regulations applicable to the use of telecommunications data are mainly of regulatory nature. For example, the laws and regulations related to the protection of personal data lack in directly giving the industry the space to use specific types of data (such as cluster data and de-identified data) under specific circumstances. What the industry competent authority may map out, when planning to promote the flexible use of data in the industry in the future, is to consider clearly defining the space for the flexible use of data by law.

In addition, as for data de-identification, although it is not faced with the challenge of compliance with laws and regulations, it lacks standards in the legal system for clear definition and treatment of the data de-identification. For example, for given original personal data, it becomes a piece of de-identified data after being processed. Can this piece of data be regarded as totally de-identified? Or can it be re-identified after other add-in identification factors?

Furthermore, due to the various usage forms and usage subjects of telecommunications data, the industries under the management of the central government authorities in charge of the industry concerned may need to use or access telecommunications data to provide innovative services. This should also be taken seriously by the said competent authorities. As the specific cross-industry cooperation models are becoming mature and normal, it is critically important to properly define

the rights and liabilities of the data provider and the data user through contracts, so as to ensure the security of the data flow throughout the process. It also relies on the government authorities in charge of the industry concerned for their collaborative discussion, coordination, and giving clear guidelines for industries to follow.

Finally, as for taking active approaches in promoting the telecommunications enterprises' use of data, there are other emerging approaches in the mechanism of facilitating data flow, including data intermediary mechanism, experimental innovative regulatory sandbox mechanism, etc. which are in a heated discussion. The development trends therein deserve the continuous attention by Taiwan.

Chapter 4 Conclusions

This research focuses on three key topics by collecting international telecommunications data application examples and legislative examples, soliciting public opinions, and compiling recommendations from expert symposiums: 1) Application of telecommunications data by the telecommunications enterprises for the purpose of national security and public interests; 2) Independently adoption of appropriate governance models by telecommunications enterprises to protect personal data and take into account the availability of the data, under the trend of data innovation applications in the industry; and 3) Through norms or mechanisms of the legal system, facilitation by the government authorities in charge of the industry concerned of the telecommunications enterprises, preparation of the environment for telecommunications enterprises' use of data in providing innovative application services. The observations and study conclusions are summarized as follows.

1. Application of telecommunications data by the telecommunications enterprises for the purpose of national security and public interests

(1) Law enforcement authorities, for the purpose of telecommunications data use, should be made to lead the service design and propose related guidelines

In the context of national security and public interests, the application, provision, or disclosure of data by telecommunications enterprises are usually not initiated by the telecommunications operators in most cases; but rather, are

actions under the instruction or in cooperation with the specific government authorities in charge of the industry concerned for the collection, processing or use of the data. Under these circumstances, the telecommunications operators are the data processors as referred to by the GDPR of the EU, whereas the government authorities in charge of the industry concerned that take the leading role in the data used are the data controllers. Data controllers are the ones leading the overall service design, and formulate the related binding rules associated with the services, whereas the data processors are cooperative in following along. As found by this research in the example of using telecommunications data in response to the COVID-19, the local health medical enforcement departments of the subject countries are the ones leading and formulating the related laws and regulations, guidelines, and norms.

In Taiwan, no special authority exists for *Personal Data Protection Act* yet, and the respective government authorities in charge of the industry concerned business are responsible for regulating the business under its jurisdiction, and the telecommunications data therein. Under the current circumstances, as discussed in the above-mentioned circumstances, the law enforcement authorities with the targeted data use also are the one leading the service design and formulate and propose the related guidelines. The telecommunications regulatory authority is the one supervising telecommunications enterprises within its scope of responsibility to ensure that telecommunications enterprises process data within the scope as per the leader's instructions in accordance with the rules proposed by the said authorities.

(2) A more restricted interpretation must be adopted in the use of data for the purpose of "national security" and "public interest"

Since "national security" and "public interest" are uncertain legal concepts, it is hard to clearly define the boundaries thereof. "National security" and "public interest" should not be abused indefinitely in the wrong way, either. In Taiwan's *Personal Data Protection Act*, Article 16 points out "*... 2. where it is necessary for ensuring national security or furthering public interest*; …" as one of the

conditions for a government agency to use personal data for another purpose; Article 19 points out "*… 6. where it is necessary for furthering public interest; …*" as one of the conditions for a non-government agency to collect, process, and use the personal data; and Article 20 points out various conditions for a non-government agency to use personal data for another purpose. Nevertheless, the *Act* lacks related operating standards on the definition of public interest. In the event of a dispute arising from citing these conditions, judgments would need to resort to case-by-case situations, which brings about a certain degree of uncertainty during the operation; therefore, such provisions are rarely applied or cited.

In the review of the various telecommunications service applications abroad (such as the collection of location information and transmission of Bluetooth data) aimed for pandemic prevention as observed in this research, even though the purpose of pandemic prevention is of public interest and is related to national security in a broader sense, there are not any cases "forcing" people to join specific telecommunications services on the grounds of public interest or national security; nor are there any cases "compelling" telecommunications companies to retrieve telecommunications data about specific individuals without legal basis. In most the cases, when services related to the purpose of pandemic prevention are implemented, the public is informed as much as possible of complete service data for the public to exercise their right to freely opt in or out. Moreover, the public can also independently decide whether to allow such services to access their location information or other telecommunications data. Hence, trust must be won from the public and the use of telecommunications services are up to the public.

(3) Explicit legal procedure and scope are required when compelling telecommunications operators to cooperate in the retrieval of personal data

If telecommunications operators are to be compelled to cooperate in providing data, then it is suitable to stipulate the purpose, scope, and procedure

of data retrieval at the legal level, in view of the necessity of restraint of public power. Taiwan's *Communication Security and Surveillance Act* constitutes one example that regulates such at the legal level, which explicitly stipulates the procedures and formats for the authoritative supervising authority to conduct communications supervision, and retrieve communications records or data of communications users, for specific purposes. South Korea's *Infectious Disease Control Act* constitutes another example. As the collection of the telecommunications location information for the grasp of the contact history is beneficial to the prevention and control of infectious diseases, the *Infectious Disease Control Act* has been amended to explicitly require the telecommunications operators to provide user location information. That is, for the purpose of preventing the spread of infectious diseases, telecommunications operators should provide user location information in cooperation with the government, strengthening pandemic prevention measures such as tracing confirmed cases and tracing the source of infection.

(4) **Relevant practical applications are subject to the principle of minimum data collection**

"Principle of minimum data collection" refers to the collection of necessary data limited to the purpose of data use. This principle serves the universal value of personal data protection. For example, the terms "necessary scope for a specific purpose" stipulated in Taiwan's *Personal Data Protection Act* reveals exactly this principle.

With reference to the examples of using telecommunications data for purposes of pandemic prevention and disaster prevention abroad, the "principle of minimum data collection" is embodied. Under the circumstance where the data subjects are given the full freedom to choose whether to use the service, the design and provision of the service still try not to invade other personal data of the data subjects even if the consent is already granted by the data subjects. When it is necessary to disclose data due to the needs of pandemic prevention, such disclosure is also limited to serving its purpose without providing extra data.

Take Estonia's official pandemic prevention APP (HOIA) as an example, once a mobile phone user has close contact with someone diagnosed with COVID-19, a notification is sent to inform the user. However, such notification is not to disclose the identity of the infected person or the time and location of the contact, so as to ensure that the identity of the infected person cannot be indirectly identified, thus personal privacy is maintained.

2. **Appropriate data governance models under the trend of data innovation applications by the telecommunications industry**

(1) **Inventory-making should be done by telecommunications operators on various types of telecommunications data under their holding, with possibilities for wide innovative applications**

The data relating to users and usage behaviors, under the management of telecommunications enterprises can be categorized into three types, namely: “user data”, “communications records”, and “other data resulted from the utilization of telecommunications services”. Among them, user data is personal data that is under the protection of the *Personal Data Protection Act* without a doubt. Communications records contain data through which personal data can be indirectly identified, such as communications date, address, location, etc. which also fall into the category of personal data. Contents of data are detailed as follows:

“User data”, in Taiwan’s current laws and regulations, refers to the data such as name or title, identity card or business administration number (BAN), address, and telecommunications number of telecommunications users, which is limited to the data filled in by users applying for various telecommunications services (see Paragraph 4 of Article 3 of the *Operational Measures for Users of Telecommunications Enterprises to Inquire about Communications Records*).

“Communications records” refer to all information generated by a telecommunications system concerning the use of a telecommunications service, including calling and called party's telecommunication numbers (i.e. telephone numbers or user identification codes), communications dates, beginning and

ending times of communications, etc., where such records shall be provided to the extent that the technology of the telecommunications equipment and system allows (see Subparagraph 8 of Article 2 of the *Telecommunications Act).* Telecommunication numbers are defined in this paragraph as telephone numbers or user identification codes. In addition, according to the *Communication Security and Surveillance Act*, communication records also include records such as an address, service type, mailbox, or location information (see Paragraph 1 of Article 3-1 of the *Communication Security and Surveillance Act).*

As for "Other information resulted from the utilization of telecommunications services", its definition refers to the provisions of Article 222 of the *Telecommunications Act* of the United States which refers to information generated by the users' telecommunications use behavior in the telecommunications service relationship, which is collected and accessed by telecommunications enterprises, including usage capacity, technical configuration, type, total volume, and other information involved in the use of telecommunications. Although current laws in Taiwan lack special definitions on "other information resulted from the utilization of telecommunications services", information such as data download rate, traffic, etc. (see the *Key Points for Implementing Service Quality Norms for Mobile Broadband Services*) may be deemed as this type of information.

Each of the above three types of information has its own connotations, and the corresponding industry laws and regulations may involve different retention rules and periods. However, any information with the attributes of personal data must comply with the requirements of the *Personal Data Protection Act*. Information collection for a specific purpose must be processed and used within the specific purpose and must not exceed the necessary scope (see Article 5 of the *Personal Data Protection Act*). Any use other than for a specific purpose must comply with legal conditions.

(2) **Relevant laws and regulations shall be observed to protect personal data and ensure consumers' rights and benefits**

For all data with the nature of personal data that is held by telecommunications enterprises, once it enters the planning and use stage, it should be examined to see whether the original purpose of the collection, processing, and use of the data is still maintained. If the original purpose deviates, it should be examined whether the user has a legitimate basis of rights for secondary use.

The most radical reform method is to obtain the acknowledgment and consent of the data subjects, and the data subjects must be informed of complete contents and be allowed the convenience of exercising their rights. In practical implementation, telecommunications operators in Japan have formulated the *NTT DOCOMO Personal Data Charter – Behavioral Principles for Innovation Creation* – to utilize personal data on the premise of disclosing the protection of the personal data of the data subjects. This example in Japan can be used as a reference example. In addition, consideration can be given to applications with technology integration and the development of a dynamic consent mechanism, so as to implement flexible data use centered on the consent of the data subjects.

3. Preparation of the environment for telecommunications enterprises' use of data with the promotion of the government

(1) Formulating guidelines or standard service contract samples to assist telecommunications operators in practicing law-abiding

According to the "List of Central Government Authorities in Charge of the Industry Concerned for Non-Government Agencies for Personal Data Protection" by the Ministry of Justice ("MOJ"), NCC is designated as the central government authorities in charge of the industry concerned for telecommunications enterprises for personal data affairs. Under the authorization of the *Personal Data Protection Act*, NCC has formulated the *Measures for Maintaining the Personal data File Security of Non-Government Agencies as Designated by NCC* (referred to as the "*Information Security Maintenance Measures*"). The items covered in these Measures are measures that shall be adopted for the protection of personal data technical-wise and organizational-wise. However,

these Measures still lack suitable implementation procedures for data use of directionality (or data use beyond the purpose).

a. Formulating guidelines as the specific bases for telecommunications operators to develop data-based innovative services

Matters such as data risk impact assessment and ensuring due right basis for data use are still lacking details in the current normative framework in Taiwan. In addition, data related to telecommunications is actually used in conjunction with data or application requirements in other industrial fields. Therefore, it is very important to have labor divided between the telecommunications operators and external operators to ensure the protection of the rights of the data subjects and information security. However, details still lack in this regard to go by.

It is recommended to refer to the Guidelines for the Development and Deployment of Location Services issued by the Cellular Telecommunications and Internet Association (CTIA) in the United States, where the approach is to define each role in the value chain (including program creator, collector of location information, and provider of network location information). In situations where information in the telecommunications field may be collocated with information in other industries, solid approaches need to be taken on the following matters: including, how to have the data subjects informed to consent on data processing and use beyond the original collection purpose; how to satisfy the data subjects' request rights (e.g. request to view, supplement, correct, stop collection, process or use, delete, etc.); how labor should be divided between the telecommunications operators and external operators to ensure information security; as well as implementing influence & impact assessment before innovative services are launches, etc. Possible approaches to take include having NCC or urging the industries to formulate guidelines on a self-discipline basis, so as to provide the basis for business operators to follow upon using data in design, and providing innovative application services.

b. Developing **standard** service contract sample to ensure data transparency

Article 17 of the *Telecommunications Management Act* states that "*Telecommunications enterprises designated by the competent authority shall set forth terms and conditions of standard service contract, specify the rights and obligations between them and subscribers,… The terms and conditions of the standard service contract as described in the preceding paragraph shall including the following matters: … 7. Restrictions on and conditions for the collection, processing and utilization of subscribers' personal information;…"* Accordingly, the competent authority may consider formulating a standard service contract sample, guide the business operators to fully disclose in the contract the following matters, including: how to use the data; the conditions for using the data; what method should be used under what circumstances to re-obtain the data subjects' acknowledgment and consent; under what conditions the data is to be disclosed in cooperation with the public power; as well as having consumers be aware of channels through which they can exercise their rights; granting consumers sufficient rights to opt in and out, and the effects therein; etc., so as to strengthen consumers' trust in the data use by the telecommunications operators, and avoid resistance due to lack of understanding.

(2) **Providing a legal basis for the use of cluster and de-identified (anonymous) data**

Where the data is not personal data to begin with, naturally there is no need for the application of the *Personal Data Protection Act*, which needs to be explained first. However, where the data is personal data to begin with, but has been processed, deleted, covered, or replaced in a specific way so that it cannot identify a specific individual individually, or has been presented in a statistical way, so that such data becomes impossible to identify any specific individual, or is presented in a statistical or clustered manner, then such data has been "processed". As for data "processing", it must be carried out on the same legal basis as that when the data is originally collected (see Letter fa-lu-zi No. 10703512280 from the Ministry of Justice). In another word, data "processing" such as de-identification or clustering of data is not within the specific purpose

of the original collection. The acknowledgment and consent from the data subjects shall be re-obtained, unless otherwise such data processing is in line with the reasons for use other than the statutory purposes;

Under the current norms of the *Personal Data Protection Act*, there are no reasons applicable to the telecommunications enterprises for use other than the statutory purpose. As a result, the de-identification or cluster processing of telecommunications data for use other than the original collection purpose, it is necessary to re-obtain the consent of the data subjects. When such data processing is obviously no harm and no other unfavorable situations to the data subjects, such condition of legal applications is no different from increasing the cost of data application. Therefore, it is recommended to evaluate what kinds of circumstances under which the use of clustered data or de-identified data would not infringe on the rights and interests of the data subjects, or bring unfavorable situations to the data subjects, and specify such circumstances in the related telecommunications laws (e.g. *Telecommunications Act* or *Telecommunications Management Act*), so that such specifications become special provisions to the *Personal Data Protection Act*, thus enabling the use of clustered or de-identified data by the telecommunications enterprises is backed up by a solid legal basis. For example, Article 222 of the *Telecommunications Act* of the United States allows telecommunications operators to use, disclose, or provide access to clustered data for purposes other than telecommunications services, which enables US telecommunications operators to directly land on a legal basis for the cluster processing of the related customer data.

(3) Considering the creation of an innovative experimental space to promote the innovation in the data used by the telecommunications enterprises

At present, Taiwan has adopted innovative experimental mechanisms in the financial field and the unmanned vehicle industry. This relies on the creation of a safe experimental space through the legal system, so that there is no concern about violating the law during the process of innovative experiments. It is worth continuous observation and exploration whether the telecommunications

enterprises themselves in Taiwan are a highly regulatory businesses, such that the use of data to provide innovative services is to increase the risk of legal violations, thus resulting in the suppression of innovative ideas or activities to the business. Where it is thought to be necessary to create a special space for innovative experiment through the legal system, it is feasible to adopt the approach of formulating special laws in terms of law-making, or the approach of introducing or amending special chapters to the existing law (e.g. *Telecommunications Act* or *Telecommunications Management Act*), so as to clarify the conditions for applying for innovative experiments and to exemplify the laws and regulations that may be excluded during the innovative experiments.

(4) Considering the promotion of other mechanisms to facilitate the data used by the telecommunications enterprises

Lately, major countries have discussed mechanisms such as data intermediary mechanisms or data banks for the facilitation of data circulation and data sharing. However, in view of the development of such mechanisms overseas, most of them are small-scale pilot projects. Among them, the concept of Open Banking, which is closely related to people's livelihood and economy, has been operated in the most mature way, which allows the same data subject’s data to circulate among different organizations (under the premise of the data subject’s consent). However, this mechanism may indeed become a prototype for running innovative services with different types of data/information co-configured, and co-used cross-industry, thus worth continuous attention.