Hosted by the Personal Information Protection Commission

International Seminar on Personal Data

The Creation of Global Free Flow of Personal data with Adequate Protection

G20 side event

Event report

(Please note that all reports are provisional summaries edited by the secretariat. Speeches may not be word-by-word transcripts.)

Overview

Alongside with the dramatic development of information technology, personal information has begun to circulate widely around the world. In light of that, efforts are underway in each country to develop legal systems and put in place measures for the protection of personal information. This seminar, organized by the Personal Information Protection Commission in Tokyo, served as a place for sharing advanced knowledge about privacy protection among the personal data protection authorities of the major G20 member countries. Its aim is to vitalize discussions about personal data protection in G20, which Japan is presiding over as the chair country for the first time this year.

Opening Remarks

Minako Shimada

Chairperson, Personal Information Protection Commission (PPC, Japan)

I would like to express my sincere appreciation for the large number of people from Japan and abroad who came together for this event. With Japan chairing the G20 for the first time this year and hosting the convention of the G20 Summit in Osaka, this event is also attended by many people from the G20 member countries.

Alongside with the dramatic development of information technology, personal data has begun to flow widely around the world. In light of that, efforts are underway in each country to develop legal systems and put in place measures for the protection of personal data, and countries and regions with different cultures and values are advancing development of distinctive systems for the protection of personal data. In this context, we host this seminar to deepen awareness of the significance of creating reliable and free data flow while striving to protect personal data, and to share the information on the related issues from a global perspective. The G20 Summit season is a valuable opportunity for hosting this international seminar.

I hope that the seminar today will contribute to international cooperation among the G20 member countries, and to discussions toward promoting the free data flow with mutual trust.

Keynote Speech　Pre-conditions to enable credible digital data flow

Marie-Laure Denis

President, Commission Nationale de l'Informatique et des Libertés (CNIL, France)

Toward fostering trust in data protection

With the advancement of digitalization in the world, international trade is becoming increasingly dependent on data flow and the transfer of personal data. The ways in which consumer privacy is handled have an impact on consumer behaviors, digital services, and market conditions, and this impact is unavoidable. Now, what kind of trust do we expect in free data flow? Three assurances are needed in order to facilitate the free data flow globally. The first is the protection of personal data. In the European Union (EU), data is protected based on standards set out by the EU, and this protection is transferred alongside with the personal data. This is covered under the General Data Protection Regulation (GDPR). The second assurance is the presence of tools that the global free data flow can depend upon. For many years, the EU has put effort into developing tools for the international transfer of data, and recently updated its guidelines on binding corporate rules (BCR) and cross-border data flow. This year, EU and Japan adopted mutual adequacy decisions for safe transfer of personal data. This also served to strengthen cooperation between the Personal Information Protection Commission and ourselves. The third assurance is for regulatory authorities to coordinate initiatives related to the free data flow, and to introduce and enforce these initiatives.

Another important element is for the authorities to have the resources for the successful accomplishment of its mission. In this respect as well, the GDPR serves as a tool for pursuing that goal. Data protection authorities in Europe are currently taking concrete steps to promote international cooperation based on the provisions of Article 50 of the GDPR. I hope that these efforts can contribute to the advancement of legal cooperation among the authorities backed by friendly relations, and to securing the protection of personal data across the world.

James M Sullivan

Acting Assistant Secretary, Department of Commerce (DoC, US)

Interoperability is an important step

The world is becoming increasingly digitalized: there are 4 billion Internet users, and 2.5 quintillion bytes of data is being created every day. Moreover, this is set to increase by 10 times by the year 2025. Cross-border data makes up 22% of global economic output, and carries great importance not only for large-scale multinational businesses, but also for small and medium-sized enterprises. At the same time, the protection of privacy and data has also become a core issue for international data flow.

The policymaking authorities of many countries including the United States welcome the coordinated efforts by the 28 EU countries toward data protection. If we were to look at various countries apart from the United States, while there is still considerable disparity between courtries with regard to policies and laws on the protection of personal data, there appears to be general trend toward imposing restrictions on cross-border data transfer. There is also a number of countries that are enacting their own data protection laws based on the EU's GDPR. This is because the GDPR is regarded by many countries as the most comprehensive and advanced law. There are many things that we should learn from the GDPR.

However, in light of differences in the respective cultures, legal systems, economic development, and pace of technological innovation of each country, it is not necessarily a good idea to simply replicate the GDPR. It is probably not possible to establish a single global standard for privacy and data protection. That is precisely why there is a need to bury their differences and enhance interoperability among authorities through innovative frameworks for privacy and data protection. The United States currently has two certification mechanisms for burying differences in personal data protection systems that could arise between countries. These are the Privacy Shield system and the Cross-Border Privacy Rules (CBPR) system of Asia-Pacific Economic Cooperation (APEC). Going forward, we hope that these will help to pave the way to a global certification mechanism.

Bruno Gencarelli

Head of Unit, International data flows and protection, Directorate-General for Justice and consumers, European Commission
(on behalf of Vera Jourova, European Commissioner for Justice, Consumers and Gender Equality)

EU-Japan cooperation based on mutual adequacy decisions

Several months have passed since EU and Japan adopted mutual adequacy decisions. Amidst the growing emphasis that is being placed on privacy protection, we share the view that it is important to consolidate a mechanism for personal data protection through a firm legal framework. Japan has been using the PrivacyMark from a long time ago, and there are many things that we can learn from it.

It is vital to maintain mutual respect for constitutional frameworks and human rights, and at the same time protect the electoral systems and the integrity of the democracy, while also fulfilling economic needs. Without gaining the trust of consumers, it would not be possible to realize the growth of a data-driven economy in a sustainable manner. In that sense, both Japan and Europe have been working on the reform of their respective data protection regulations.

The next issue would be how to make the regulatory system beneficial to businesses after they clear the hurdle of the regulatory requirements. What kind of data should they possess, and what should they do in order to develop an even stronger relationship of trust with their customers and trade partners? The strategic utilization of data is also an important element in propelling businesses forward. Through the proper development of tools, I hope that we will be able to present various criteria and standards, such as a code of conduct, to enable companies to comply with the new rules. The EU will cooperate with Japan to firmly implement privacy governance systems.

Panel Discussion 1　Mutual trust among stake holders

Moderator

Bojana Bellamy

President, Center for Information Policy Leadership (CIPL)

Using various forms of certification as bridges

Panelists

Josh Harris

Director, International Regulatory Affairs, TrustArc

Bridging different countries through the CBPR

Tetsuya Sakashita

Managing Director, Japan Information Processing and Development Center (JIPDEC)

Certification system for achieving safe data flow

Naoya Bessho

Senior Executive Director, Information Technology Federation of Japan (ITrenmei)

Toward the introduction of TPDMS

Anna Pouliou

GDPR Multistakeholder Group Expert at European Commission, Business Europe Representative, National Rapporteur for Privacy at International Federation of European Law (FIDE), Head of Privacy at Chanel

Need to cooperate above and beyond the field of legal cooperation among countries

Ken Katayama

Director of Digital Policy, Microsoft Japan

Providing Data Subject's Right to every person

Laura Juanes Micas

Director of Privacy Policy, Facebook

Constant improvement in accountability

Bellamy: In the Panel Discussion today, I would like to discuss how we can foster mutual trust among various stakeholders. The things that are happening in our digital society today, including the fourth industrial revolution and what has been described as "Society 5.0" in Japan, are very exciting. At the same time, however, it has also been pointed out efforts to foster trust are not sufficient enough. The lack of trust in the sharing of data by corporations is also present in the industry. How can we build a network of trust securely among the various countries? I would like to discuss that.

Harris: The CBPR is a network for corporate certification created by APEC. To participate in the CBPR, APEC members have to first participate in APEC's Cross-border Privacy Enforcement Arrangement (CPEA). Next, they are then required to submit to APEC a Letter of Intention to participate in the CBPR. This letter must include a statement of their intention to use at least one Accountability Agents (AA), for example. Most importantly, through the completion of an "Enforcement Map", they certify that the requirements that certified businesses are required to comply with can be enforced through the application of domestic laws.

After the completion of these submissions, the application is reviewed by the APEC Joint Oversight Panel (JOP). Once it has been approved unanimously by all APEC members, the applicant's participation in the CBPR is approved.

After a business acquires the CBPR certificational through an AA (such as TrustArc or JIPDEC), the AA will issue a seal or stamp as proof of the certification. From the viewpoint of the consumer, this signifies that the business in question is being properly monitored by the enforcement authority. The most important point about the CBPR system is that even under different legal systems, a certain level of protection standard is assured as long as the requirements are fulfilled. To begin with, the CBPR was not created to replace the domestic laws of each country. Hence, in promoting the CBPR certification, it is also sometimes necessary to enact complementary laws to fill the gap. By recognizing the similarities or differences between domestic laws and the CBPR, it is possible to close the gap between the legal systems of each country.

Sakashita: JIPDEC was established in 1967. The PrivacyMark has been in use since April 1, 1998. Japan has the Act on the Protection of Personal Information, while JIS Q 15001 is the standard for the management of personal data in businesses. We are engaged in the work of conducting independent checks on businesses that carry out management based on JIS Q 15001, awarding the PrivacyMark, and giving authorization for the right to use the PrivacyMark. Currently, as many as 17,000 companies have acquired the PrivacyMark, and this number is still on the rise even now. We also work together with the PPC on activities to promote the CBPR. We make presentations about data flow and trust in Ho Chi Minh City, Hong Kong, Taipei, and other places to recruit participants in the CBPR. The purpose of our work is not to offer certification; rather, we consider certification as one of the methods of providing support toward encouraging organizations to carry out data flow safely. Through the awarding of the PrivacyMark and the CBPR certification, we aim to continue supporting businesses to help them gain greater trust from consumers and employees.

Bessho: The Information Technology Federation of Japan is Japan's largest organization for the IT industry. We are now considering the introduction of the Trusted Personal Data Management Service (TPDMS) based on the premise of Japanese laws related to data use. Through the services offered by TPDMS, users entrust their data to TPDMS, and this data is then provided to suitable companies. The data is not provided to companies assessed as unsuitable, or only the necessary data is provided from among all the data that has been collected. One of the concepts of TPDMS is that is incorporates a privacy policy within the terms of service. Furthermore, it also requires TPDMS to establish a Data Ethics Board. We generate a large volume of data in our everyday lives, and seem to be swimming in a sea of data. In the current situation, it is as if we were being told to dive unknowingly into this sea of data. Hence, it is necessary to have a swimming coach there, and this role is fulfilled by the Data Ethics Board. The Data Ethics Board exists so that we can swim in the sea with peace of mind. As it would be difficult for people to trust a single company to do this job, we decided to create a framework in which the IT Federation of Japan provides certification for TPDMS that can be trusted.

Pouliou: In the EU, 28 countries used to have 28 different laws. Their privacy laws were not necessarily aligned with one another. Moreover, there were conflicting laws even in a single country. I worked in Germany for eight years, and there were regulatory authorities for each state. If I were in Frankfurt and the customer were in Munich or Berlin, the regulatory authority of the area that my customer was in might not approve a project that has been approved in my area. I wonder how much costs were incurred in order to resolve such issues. However, the introduction of the GDPR has secured consistency.

The GDPR is now gradually becoming a global standard, but there are still countries that are taking it a little too far, as well as places that have over-localized it. There are also countries that have strict rules in place. Now, how can we be of help in these circumstances? It is not appropriate to consider the issue only within individual areas of jurisdiction while neglecting the presence of cross-border data flow. Although there are conflicting laws depending on the country, they are gradually becoming more harmonized with one another. At the very least, it is vital for the strongest and most important countries in the world to hold one another's hands firmly and cooperate on the flow and transfer of data.

Katayama: Our company has 120,000 employees and conducts business in 160 countries. We have approximately 2,000 employees in Japan. Our corporate mission is to "empower every person and every organization on the planet to achieve more." Although the GDPR is a law of the European people, our company enables not only the people of Europe, but people around the world, to manage their own information, delete data, and exercise their data subject's right through our privacy dashboard. A very interesting and noteworthy point is that the largest number of people who have managed and checked their own information in some way after the enforcement of the GDPR was not in Europe, but in the United States. This was 6.7 million people in the United States as compared to 4 million people in Europe. In Japan, this figure was 1.4 million people. In January this year, the European Commission adopted adequacy decision on Japan. The PPC has announced its stance on a so-called three-year review of the Act on the Protection of Personal Information, and this stance touches on accountability, or in other words, privacy impact assessments. In the GDPR as well, Data Protection Impact Assessments (DPIA) are recognized legally as a means of evaluating whether corporations maintain transparency regarding privacy in an accountable manner. Japan has the Act on the Protection of Personal Information, while the EU has the GDPR. However, the United States does not have the federal law. It has been proposed that the United States federal law on privacy is a necessary element within the global privacy framework, and since 2005, our company has also been advocating the need for such a law.

Micas: Businesses should continuously put effort into improving accountability in order to protect users' privacy. We are constantly developing new management methods, delivering clear explanations to the relevant parties, investing in research, and making improvements in cooperation with the privacy community. We are currently implementing many related projects and campaigns. It is also important for the top management to fulfill its accountability. Our CEO, Mark Zuckerberg, has called on the government to put in place privacy-related regulations. At the same time, the GDPR could be described as both a starting point as well as an inspiration for the establishment of privacy and portability regulations.

Our organization has established three pillars aimed at strengthening trust from the users. The first, as explained earlier, is related to the initiatives implemented internally in the business, in the sense of the kind of measures we put forward and how we interact with users. The second is our cooperative involvement in policy formulation, and we cooperate with external organizations on that front. For example, together with policymakers and experts, we conduct the "Design Jam" workshop globally. Thirdly, we also consult with privacy experts. Going forward, we will put in our best efforts and continue to improve, with the aim of fostering trust with our users and stakeholders.

Bellamy: It is clear that various methods and tools are available. Various methods already exist for the cross-border transfer of data, but it is essential for every individual and country to recognize these mutually. In addition, we also have to further develop certification as a bridge that links everyone. There is much to learn from the GDPR, the CBPR, Japan's PrivacyMark, and other systems.

Panel Discussion 2　The role of public sector for global data flows

Moderator

Takayuki Kato

Ph.D., Professor, Asia University (Japan)

Moving beyond differences in legal systems between countries

Panelists

Andrea Jelinek

Chair, European Data Protection Board (EDPB)

EU and Japan as key partners

Anne Carblanc

Head of the Digital Economy Policy Division, Organisation for Economic Co-operation and Development (OECD)

Pursuing the possibilities of data flow

Gopalakrishnan S.

Joint Secretary, Ministry of Electronics and IT (MeitY, India)

Fostering trust in cross-border data flow

Yeong Zee Kin

Deputy Commissioner, Peronal Data Protection Commission (PDPC, Singapore)

Realizing the introduction of the TrustMark scheme

Mari Sonoda

Secretary General, Personal Information Protection Commission (PPC, Japan)

Toward safe and smooth data flow

Clarisse Girot

Data Privacy Project Lead, Asian Business Law Institute (ABLI)

Creating frameworks that extend beyond national borders

Boris Wojtan

Director of Privacy, GSM Association (GSMA)

The bridging role of the GDPR framework

Kato: There are different legal systems for the protection of personal data depending on the country. Today, we have invited great experts from the G20 countries to discuss the recent situation and challenges from their respective viewpoints.

Jelinek: One year has passed since the GDPR was first enforced on May 25 last year. The EU is already engaged in adopting adequacy decision unilaterally with a number of countries, but Japan marks the first instance of the EU adopting mutual adequacy decision with a third country. This sets out the direction of similar agreements going forward, and it can be regarded as a successful model for international cooperation. There are about 500 million consumers in Europe, and there is growing awareness in each country. The GDPR sets out provisions that can be applied corresponding to various circumstances of data transfer, and encompasses various elements including BCR. The adoption of adequacy decision is precisely a principle, while also acting as a safeguard. For Japan, the EU deemed it possible to adopt adequacy decision in a way that reflects Japan's unique social, cultural and historical background. In Europe, the GDPR has contributed to growing awareness among individuals on the protection of personal data. At the same time, it is also believed to have brought about the beginnings of a substantive culture of privacy compliance among businesses.

Carblanc: The OECD Privacy Guidelines is the first set of privacy guidelines agreed upon by the OECD member countries in the 1980s. Its goal is to protect privacy, and at the same time, promote free data flow. To begin with, these two elements have a very strong correlation. The protection of privacy must not hinder the free data flow. The OECD Privacy Guidelines were revised in 2013. It describes three major mechanisms through which data flow is facilitated. Firstly, only minimal requirements are required with regard to cross-border data flow. Secondly, restrictions must be commensurate with the situation and risk levels. Thirdly, data managers must fulfill their accountability. OECD has participated actively in international discussions on data protection policies. Alongside with maximizing merits, we have also strived to minimize the risks to individuals. It is vital to provide support in order to ensure that the personal data flow advances in a positive direction. OECD will continue to put effort into facilitating the sharing of good practices around the world.

Gopalakrishnan: International data flow has a positive and a negative aspect in India as well. Cross-border data flow is extremely valuable. At the same time, however, alongside with the spread of the Internet across the globe in the past few years, its dark side has also begun to emerge. For example, it is linked to a surveillance society and surveillance economy, and markets that possess data now hold influence over other market players. Furthermore, consumers who are online have also been acknowledged to be subjected to these influences. Although digitalization is advancing in India, electronic transactions still make up an extremely low proportion at just 0.2% of all transactions. Literacy rate is also still low in the country, and there is still poor digital knowledge among the people. Yet, that is precisely why we must deal with the problems caused by data flow.

At the same time, attention is also drawn to localization. Some countries are attempting to restrict access to the government only through localization. From India's perspective, this is not acceptable. The stance of India's legal system is to firmly protect privacy, and on the other hand, to incorporate localization within an appropriate scope.

Yeong: Singapore adopted the Data Protection Trustmark (DPTM) in January 2019. This scheme provides assurance for the presence of sound data governance structures and policies within organizations. To acquire this accreditation, organizations have to be open about their personal data protection practices. Firmly embedding such practices within an organization fosters the trust of consumers. With regard to personal data, accreditation under this scheme can also give consumers the sense that the company is securely protecting their data. They can also rest assured that personal data will not be used beyond the scope of law. DPTM is created based not only on Singapore's domestic laws on data protection, but also in line with the CBPR and OECD Privacy Guidelines. I believe that DPTM can contribute to securing trust in cross-border data flow in the future.

Sonoda: We see expressions such as personal information and personal data appearing in news headlines almost every day. However, privacy and the approach to privacy differs from country to country. This is because they are dependent on various factors, such as history, culture, and common knowledge. However, there is still a need for some kind of global standard. In that sense, the formulation of the OECD Privacy Guidelines in 1980 was an extremely important step taken in history. The OECD Privacy Guidelines are comprised of eight principles. These have become the foundation for the privacy laws of many countries, including Japan, and form the basis for personal data protection. The Guidelines also include principles on international application and set out the policies for the free data flow. Based on these policies, the PPC cooperates with the countries of various regions including the Asia-Pacific region and Europe.

With regard to measures to promote the free data flow alongside with the protection of personal data globally, there are three ideas. The first is initiatives in existing bilateral frameworks to enhance interoperability. This refers to efforts to promote the cross-border transfer of personal data under existing systems. The second is the introduction of global certification systems for the cross-border transfer of personal data. I believe that global certification systems with interoperability can offer significant benefits to businesses. PPC has launched a trilateral discussion with relevant authorities in the United States and the European Commission. Thirdly, we are now moving forward on discussions, including with the OECD Secretariat and experts, with a view to revising the OECD Privacy Guidelines and dealing with undesirable risk factors.

Girot: At ABLI, we are engaged in activities for the convergence of laws. We are currently implementing a data privacy project that covers 14 areas of jurisdiction in Asia. While examining the similarities and differences among these, we are attempting to bring the laws as close to one another as possible. Consumer laws, cybersecurity laws, and data protection laws all fulfill a role in the global digital economy. On the other hand, there is also increasing fragmentation of laws. In this respect, I think that the authorities should take up the responsibility of bringing clarity to the legal system; that is, securing certainty and consistency to enable actual cross-border activities. ABLI ensures consistency in systems as a part of its legal convergence work. An example is creating a framework that goes beyond national boundaries, which can be implemented in the regions. As organizations such as OECD and APEC have their respective frameworks, the approach is to create something like the CBPR based on those frameworks. Another one of our initiatives is to improve compatibility through the legal systems. We strive to reduce the unnecessary burden of compliance shouldered by corporations. At the same time, privacy is positioned at the core of business models and systems. This is because it can offer a competitive edge even in Asia. Data protection frameworks that offer greater compatibility are needed in various areas. The United Nations Conference on Trade and Development (UNCTAD) is also already engaged in activities related to cross-border data flow and the establishment of domestic laws.

Wojtan: GSMA is an association for mobile operators with as many as 800 member companies worldwide, including KDDI and SoftBank that are members in Japan. Cross-border data flow is an element of great importance to our industry. During your regular use of your mobile phone and smartphone devices, highly complex data processing is happening in places that you cannot see. Often, these processes do not take place in just one country but straddle multiple countries. This is not limited to the times when we are operating our mobile phones and smartphone devices. Mobile phones also fulfill the functions of personal identification and authentication as well as mobile money, and cross-border data flow is becoming extremely important today. Particularly in developing countries, it is important to be able to carry out transactions even when one does not have a bank account. Like connected cars, IoT, drones, and Big Data, data flow is necessary to enable all of these to function properly. Moreover, the world of 5G is upon us. Although 5G coverage extends only to some areas at the moment, it will eventually spread out to cover all areas, making it absolutely vital for data to flow across an even wider area. This is precisely why data flow is important for the mobile communication industry. Now, what is GSMA engaged in doing? We are working to make the effects of the GDPR effective across the world. I have heard that there are attempts in both APEC and the Association of Southeast Asian Nations (ASEAN) to build frameworks. If there are frameworks in place, the countries of the region will be able to align themselves with one another. However, I think that there are still elements that are lacking. That would be the "connective tissue," or in other words, the element that fulfills a linking role. How would we translate this? I would like you to think of it as something akin to a "glue." In short, it is the presence of an element that binds the respective regions and carries out all the practical work. I believe we are advocating that in the G20 agenda.

Kato: This has been a beneficial session where we shared various thoughts and issues such as the significance of the EU-Japan mutual adequacy decision, marking a first in the world, the importance of safe and smooth data flow, the localization of data, DPTM, and the promotion of global data flow.

Guest Speaker

Angelene Falk

Australian Information Commissioner and Privacy Commissioner Office of the Australian Information Commissioner (OAIC, Australia)

Creating models for fostering trust

We see a need to strengthen public trust and confidence in protection of personal data. That is especially the case when it comes to digital platforms. The number and serious nature of privacy issues associated with these platforms has led to increased scrutiny around the world, such as the Facebook and Cambridge Analytica issues. Research in Australia has found that 73% of consumers choose a brand they trust the most with their personal information. The Australian government charged me with developing a new regulations to increase online protections for Australian's privacy, with a view to preventing the occurrence of privacy issues. We will start to develop the regulation this year, and will include a focus on ensuring greater protection for more vulnerable groups online such as children. Based on a survey on consumer psychology, people have shifted their trust to the relationships within their control. Nowhere is this truer than in data protection where individuals seek control and the ability to self-manage their privacy. Done well, privacy self-management allows individuals to exercise choice and control, by understanding how their personal information is being handled. However, it is dependent on the extent to which organizations make this information accessible and understandable. For consumers to have a fair chance of making choices, there needs to be a way of presenting information that is meaningful to consumers.

To conclude, our data offers enormous potential for individuals, business and government, and it no longer stops at national borders. We therefore need a model for data flow that includes strong privacy protections that build public confidence and consumer trust.

Moderator

Bojana Bellamy

President, Center for Information Policy Leadership (CIPL)

Starting with discussion on accountability

Data is a core element of our economy, and forms the basis for economic growth and social progress. The global playing field is becoming increasingly level, with poor countries drawing closer to the more prosperous countries. There is sustainability, and it is being utilized. On the other hand, there are also issues such as legal fragmentation, growth in uncertainty, and the rise of digital data sovereignty. How do we find solutions to these problems?

In Panel (1), we talked about how the fulfillment of their accountability by businesses can serve as a "bridge" to close up the gaps caused by legal fragmentation. This is because entities act under the same rule of accountability even though it is true that rules in general differ from country to country. The panelists also showed us examples that demonstrate how businesses can exercise accountability. For example, Europe has the BCR. APEC has the CBPR, which can demonstrate accountability in the same way as the PrivacyMark in Japan. The discussion also touched on the importance of transparency to individuals, and on accountability as a repetitive process. It is not something that is completed after a one-time implementation; rather, there is a need to constantly build and maintain it. At CIPL, we consider the accountability to be a possible solution. Many members of data prctection agencies, from many G20 countries, including Asia Pacific, Europe, and the United States, are participating in the seminar today. It is precisely in such forum that discussions are needed.

Takayuki Kato

Ph.D., Professor, Asia University(Japan)

Harnessing the autonomy of business operators

I would like to talk about the points that should be taken into consideration with regard to the international transfer of personal data. There are two approaches with regard to efforts to secure data flow without losing a high level of data protection. They are the government-led approach, and the autonomous approach. The government-led approach carries out personal data protection and the enforcement of domestic laws at the national level, and seeks to realize this outside of the country as well. To achieve this goal, it is necessary to incorporate provisions for extraterritorial application, or to demand the same legal system in a third country, or alternatively, a legal system that is on par with its own legal system. On the other hand, the approach that places emphasis on autonomy involves formulating standards that business operators who are focused on personal data protection should comply with firmly. To achieve this, it is necessary to enact soft laws on an international or national basis, or to establish some form of rules for the private sector. These will be different from the laws of the country that have binding power. We call this the "voluntary approach." It is important to implement both approaches in parallel with each other.

Conclusion

Elizabeth Denham

Information Commissioner, Information Commissioner's Office (ICO, UK)

Toward the realization of interoperability

It is important to place the focus on the shared expectations of the citizens for the building of a bridge that connects various diverse elements such as law and culture, and the protection of their privacy. How can we find a form of interoperability that enables data flow under the appropriate protection of personal data? Interoperability begins with an understanding of the commonalities and differences between the systems. It is only with this understanding that we can then devise tools to enable data flows with trust. The EU adequacy decision process is one approach to achieve interoperability, and it has been used successfully to find common ground in legislative approaches as diverse as that of New Zealand, Israel and Japan. The GDPR sets a high standard for data protection. On the other hand, the legal concept of accountability is another possible route forward in interoperability. The EU's BCR and APEC's CBPR are both examples of accountability mechanisms. Our Commissioner, too, plays a significant role in fostering trust as a part of interoperability. The first is cooperation in regulatory action. While protecting the safety of the citizens by carrying out investigations, enforcement, audits, handling of complaints, and sanctions, it is vital to understand each other's views on issues and case studies in order to realize effective cooperation. The second is the policy rationalization. Commissioners should rationalize policy effort aimed at realizing reliable data flow, share work related to social risks that are truly common across all countries, and act to benefit businesses and citizens.

Data protection laws differ according to areas of jurisdiction, but trust is universal across the world. It can also serve as the foundation for international cooperation, trade, and data flow. What is of importance here is whether or not we can cooperate as a global community to foster trust. The G20 member countries have been given this important opportunity.

Closing Remarks

Minako Shimada

Chairperson, Personal information Protection Commission (PPC, Japan)

It has been an exciting day. On behalf of the organizers, I would like to express my sincere gratitude to all the participants.

The two moderators have summarized the panel discussions. Ms. Falk, Commissioner of the OAIC, spoke about the roles that authorities should fulfill and the importance of trust in privacy. Ms. Denham, Commissioner of the ICO, summarized the discussions for the day by speaking in detail about interoperability and the importance of international cooperation.

Based on the meaningful discussions held in this seminar, I believe the various stakeholders involved in the protection of personal data who are present here today have gained a fresh understanding of the importance of your respective roles.

Today, we have also brought together the three parties of Japan, the United States, and EU, and succeeded in finding consensus in advancing discussions toward the appropriate protection of personal data and facilitating data flow. Going forward, I hope that we can accelerate this initiative further, while also engaging in discussions with all the G20 member countries.

While this seminar has come to an end, the discussion today has only just begun. I hope that you will all take this as an opportunity to further deepen discussions on the significance of creating reliable and free data flow, the importance of personal data protection, and the issues surrounding these topics.