Journal of International Trade & Commerce (J. Int. Trade Commer.)
Vol.17, No.3, June 2021 (pp.147-165)
http://dx.doi.org/10.16980/jitc.17.3.202106.147

ISSN 1738-8112 (Print)
ISSN 2384-1958 (Online)

A Comparative Study of Consumer Trust in Major Digital Trade Agreements

Bo-Min Ko[a]

[a]Department of International Studies, Catholic University of Korea, South Korea

Received 27 May 2021, Revised 17 June 2021, Accepted 28 June 2021

Abstract

Purpose – Technological change has provided individual consumers with increased possibilities in participating in digital trade while the lack of consumer trust and confidence in digital trade prevents consumers from enjoying all the benefits of e-commerce. In this regard, it is necessary to search for means to protect the individual rights of consumers participating in digital trade with a sound assessment of digital trade agreements in terms of consumer trust.
Design/Methodology/Approach – Focusing particularly on the issue of consumer trust-building, this paper first discusses major consumer concerns for digital trade and specifies issues that embrace consumer trust-building within multilateral and regional trade agreements. It then conducts a comparative analysis of articles related to consumer trust in six major digital trade agreements and derives its policy implications.
Findings – In participating in digital trade, consumers have both general and stage-specific concerns. With slow progress at the WTO on e-commerce, articles related to digital trade are increasingly featuring in regional trade agreements (RTAs), including nine issues directly related to consumer trust: online consumer protection; personal information protection, unsolicited commercial electronic messages which means spam messages, domestic regulatory framework, transparency, cybersecurity, access to and use of the internet for electronic commerce.
Research Implications – By reviewing the six major digital trade agreements on nine issue areas of consumer trust, it is first found that all the agreements certainly share the significance of building consumer trust to facilitate digital trade. Second, the consensus of signatory countries on the five issues, such as online consumer protection, personal information protection, unsolicited commercial electronic messages, domestic regulatory framework, and cybersecurity, seems relatively easy to make since articles in those issues in six agreements are similar in their length and quality. To strengthen consumer trust internationally, in the form of multilateral or regional trade agreements, both e-commerce and competition chapters should cover the rules for digital trade. Domestically, it is necessary to find a way to regulate digital trade not only with domestic consumer law but also with the Monopoly Regulation and Fair Trade Act.

Keywords: Consumer Trust, Digital Trade, Digital Trade Agreement, Digital Trade Policy, E-commerce
JEL Classifications: F13, F53, F68

[a] E-mail: bomingo@catholic.ac.kr

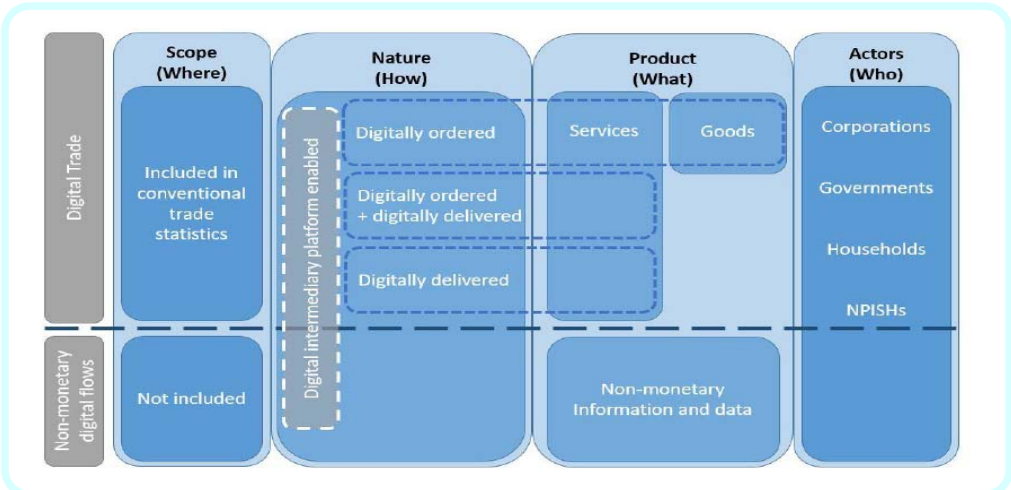
Ⅰ. Introduction

The international trade society is now eagerly searching for the right conceptual framework for digital trade as depicted by OECD (OECD, 2020). As shown in Fig.1, digital trade refers to the international trade in produced goods and services that have been digitally ordered and/or digitally delivered. The nature of the transaction - digitally ordered and/or digitally delivered - is the defining characteristic of digital trade. Most interesting is the inclusion of actors in the framework. It counts four major actors including corporations, governments, individual consumers (households), and non-profit institutions serving households (NPISHs). Technological change has provided individual consumers (households) with increased possibilities to purchase goods and services from foreign suppliers, whilst also increasing their interaction as 'producers' when supplying services (for example, educational or financial services) via Digital Intermediation Platforms (DIPs). (See Fig.2.)

As the corporate sector can be categorized as "ICT industries; Digital intermediation platforms (charging fees); Data and advertising driven platforms; Firms dependent on digital intermediation platforms; E-tailers; Digital firms providing digital financial and insurance services; and other producers only operating digitally," identifying transactions involving households (whether as producers or consumers) is more challenging (OECD, 2020).

Digital technologies enable consumers to become so-called "global consumers." (Statista, 2020). According to a recent survey of the worldwide share of consumers that shop online, in 2020, a total of over 80 percent of consumers across the globe shopped online: reaching nearly 90 percent each, the leading regions that year were South America and Asia. North America had the lowest share with just over three in four consumers buying items on the internet although the online store that was used most frequently by shoppers worldwide was Amazon.com, an American DIP (See Fig.3). Although there is no clear and complete definition of the digital economy, what we witness is that global consumers are enabled by direct interactions with foreign businesses as well as household producers can sell digitally by intermediary platforms/marketplaces (Tran, 2019). There are, however, plenty of challenges and concerns of participating or regulating digital trade. While official trade data include some transactions

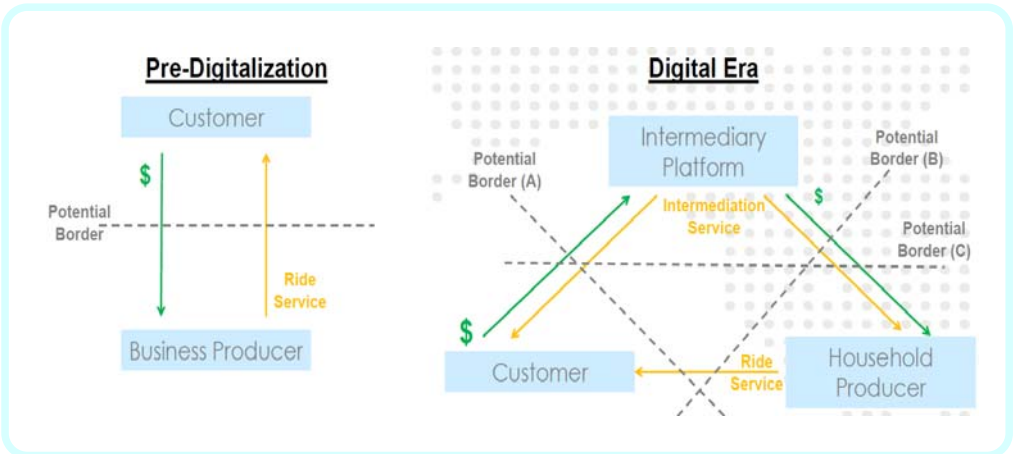
Fig. 1. The Conceptual Framework for Digital Trade



Source: OECD (2020).

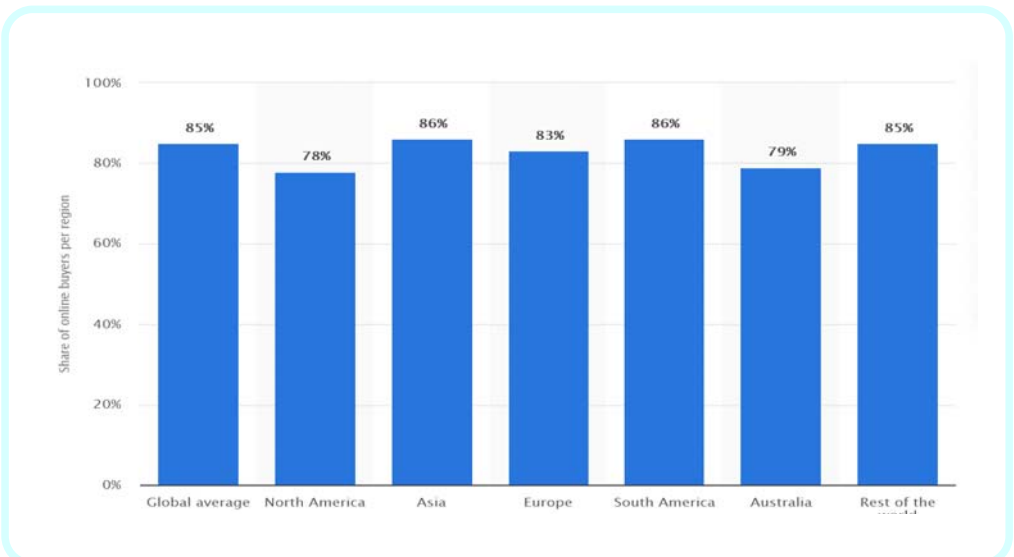
enabled by digital technologies, it does not identify all the transactions that are digitally enabled. Domestic consumers in each country who act as global consumers are more difficult to survey than corporations including DIPs, and this makes their voices less heard and detected by each government. Moreover, consumer opinions or concerns seem to be overlooked as governments consider corporations rather than consumers as the main actors in implementing domestic industrial policy. Some governments in their FTA negotiations seem to be more attentive to requests and responses of corporations than those of individual consumers.

Fig. 2. The Case: Digitally Purchasing a Ride Service



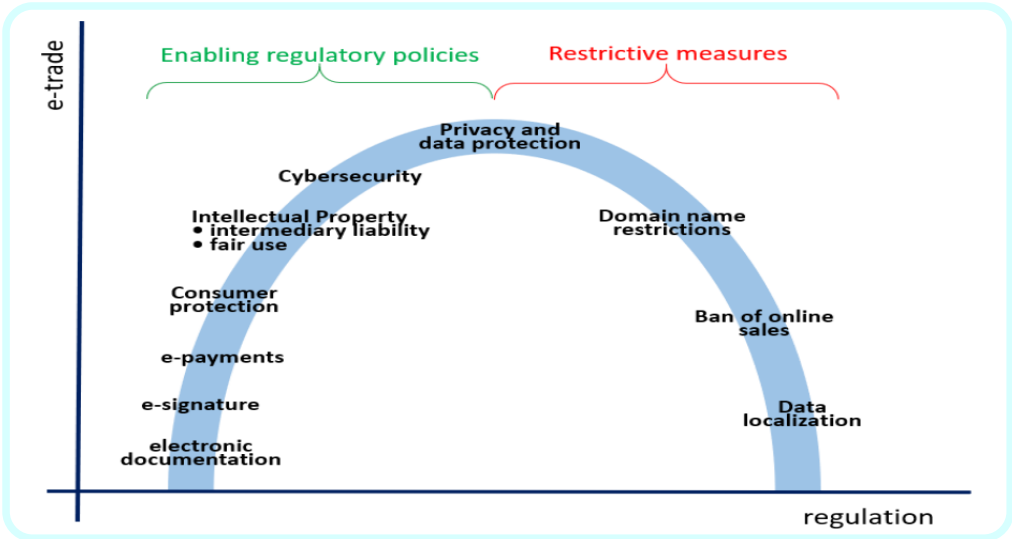
Source: Tran (2019).

Fig. 3. Total Global Share of Consumers who Shopped Online in 2020, by Region



Source: Statista (2020).

Fig. 4. Domestic Regulation Can Foster or Hinder Digital Trade



Source: Jaller et al. (2020).

In the digital era, regulation plays a central role in building the foundations of digital markets as it can provide the legal tools necessary for remote contracts, clarify the rights and obligations of the multiple actors involved in digital transactions, and establish a framework that promotes consumer trust in digital markets, even when the consumer does not know the merchant or when the merchant is in a different country (Jaller et al., 2020). As digital trade encompasses a broad variety of activities which entails a commercial transaction performed, normally remotely, through electronic means, the regulation of digital trade embraces elements of contract law, financial law in what relates to e-payments, consumer protection, intellectual property, cybersecurity, personal privacy, and data protection. These regulations a have double-sided effect as a conducive regulatory framework in each of these policy areas is necessary for vibrant digital markets while specific restrictive measures within these areas may undermine e-trade, for example by unnecessarily curbing the types of goods that can be traded remotely, or by limiting the cross-border flows of data that underpin e-trade transactions (See Fig.4). According to the WB report, one of the three key roles of regulation is that it can improve the conditions for trust in digital markets by ensuring that consumers are protected and that their information is safe and remains private, hence increasing reliance and bringing new actors to digital transactions (Jaller et al., 2020). Basic regulations such as e-documents and e-signatures provide tools for e-commerce such as facilitating document recognition and expediting processes. However, regulations to protect individual rights with regards to their private data can increase consumer trust on the internet.

The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent economies from enjoying all the benefits of e-commerce. Since the range and the depth of each country's domestic regulatory frameworks for consumer trust-building differs and some are even with no teeth, it is necessary to search for means to protect the individual rights of consumers in e-commerce with a sound assessment of each country's framework as well as digital trade agreements they sign with its partners. In digital trade agreements, there are usually three areas covered: digital trade facilitation such as e-authentication, e-contracts, e-invoicing, e-payments, and data flows and localization; trust in digital trade such as personal data protection, online consumer protection, spam, and online safety; and cooperation activities between the countries.

Focusing particularly on the issue of consumer trust-building, this paper first discusses major consumer concerns for digital trade and specifies trust-building international regulations for consumers. It then conducts a comparative analysis of articles related to consumer trust in major digital trade agreements and derives its policy implications.

Ⅱ. Consumer Concerns and Trust-Building in Digital Trade

Consumer trust for digital trade is declining (KIEP, 2021). According to a 2019 CIGI /IPSOS survey of 25,000, global consumers or users found that 78% of those surveyed were concerned about their online privacy, with 53% more concerned than they were a year ago, and 39% said they were using the internet more selectively. A December 2020 study by the Oxford Internet Institute found 71% of internet users are worried about a mixture of threats, including online disinformation, fraud, and harassment. The current digital trade environment particularly has put individuals or groups of individuals at risk (KIEP, 2021). Each government seems to put less effort into building consumer or user trust than business trust. For business stakeholders, each government is actively negotiating with their partners for the free flow of data default with exceptions or a ban on data localization and performance requirements. Of course, there are efforts made for enforcing domestic as well as international laws for privacy (or personal data protection) and spam to protect consumer welfare. To build a free flow of data with consumer trust, consumer concerns for digital trade, such as disinformation, malware, internet shutdowns, should be carefully reviewed and categorized because these can yield trade distortions or undermine market access. This section first analyzes key concerns of consumers in digital trade in a systematic way and then discusses consumer trust-building regulations mandated to each government.

1. Key Concerns of Consumers in Digital Trade

According to the 2019 survey report by UNCTAD_CIGI, three-quarters (78%) of people are concerned about online privacy and the majority (53%) feel more concerned about this compared to one year ago. Fewer than half are confident that any of the algorithms they are using are unbiased, with social media news feeds ranking the lowest (at 32%), on this metric. Similarly, only about half (48%) agree that their government does enough to safeguard their online data & personal information, with citizens in the European (45%), North American (38%), and G-8 economies (39%) among the least likely to agree with this statement. Perhaps heightened levels of concern vis-à-vis online privacy can be traced to a perceived lack of awareness about data protection and privacy rules. As it currently stands, just two in five (44%) would self-assess themselves as being at least somewhat aware of the data protection and privacy rules in their economy, with citizens in developed economies such as Japan (16%), Canada (26%), and Australia (31%) scoring among the lowest, on this metric. Over the past year, there has been a significant increase in the proportion of global citizens who feel that product security certification markings are important when buying products (91%; +4) (UNCTAD_CIGI, 2019). For a product valued at $1k, global citizens are willing to pay as much as 30-35% extra for these markings. Citizens living in developing economies tend to assign the most relative value to such markings. To help ease some of these concerns, better product security and, more specifically, product certification markings are becoming increasingly important. Global citizens are willing to pay about thirty percent (30%) more for better product security, though as many as three in ten will not pay anything else, figures which are consistent across all Internet-enabled devices, regardless of type. Citizens in developing economies are once again more willing to pay extra for better product security as those in the developed world generally expect strong security from the onset. Most (73%) global citizens would prefer to have their online data and personal information stored on physically secure servers located in their own economy.

Fig. 5. Proportion of Internet Users Worried about Disinformation, Fraud, and Harassment on the Internet

Source: Knuutila et al. (2020).

To understand risks related to digital communication, the 2020 Oxford survey included a dedicated question: "When using the internet or social media, do you worry about any of the following things happening to you?" (Knuutila et al., 2020). The three potential risks listed were three risks as disinformation, fraud, and harassment. Out of all internet users, 71% said that they worry about at least one of these three happening to them. According to survey data collected between 8 May 2019 and 17 January 2020 for the 2019 Word Risk Poll, based on a sample of 154,195 respondents in 142 countries, the perceived threats of technology harms were even higher among more regular internet and social media users (See Fig. 5). Overall, 53% of regular internet and social media users worry about encountering disinformation online. North America is the region where the largest share of the population views disinformation as a threat, with, on average, 65% of internet users worrying about it. Within Europe, there is a significant degree of variation: more than 70% of internet users in Italy and France worry about disinformation, while the figure is less than 40% in the Baltic countries and Poland. There is even more substantial variation worldwide. In South Asia, only 7% of the general population worry about misinformation, and only 32% of internet users express this worry. The perceived risk of online harassment varies more than that of other internet-related risks. It is most prominent in what is often referred to as the "Global South," and is especially high in Latin America, Southeast Asia, and Africa, where over 40% of internet users worry about being harassed online. The fear of harassment is lowest in Europe and North America, though in Russia and Central Asian countries, the perception of harassment as a risk is also uncommon.[1] In summary, this survey finds that, globally,

1) This survey also mentions that there were some differences in perceptions of technological risks between demographic and economic groups, but as a rule, these were smaller than the differences between countries. Perhaps unsurprisingly, people living in rural areas, as well as unemployed people, are less likely to worry about internet-related risks. Globally, a little less than a third of male respondents worry about online harassment, and a little more than a third of female respondents worry about online harassment. However, in some regions, the gender divide grows. In Latin America, for example, fully half of the female respondents—51%—worry about online harassment, while the figure for men is 38% (Knuutila et al., 2020).

people are most concerned about disinformation out of all technology-related risks. Concerns about technology, especially online disinformation, are widely held. Naturally, the concern about disinformation runs highest among regular users of the internet and social media (Knuutila et al., 2020). There are important differences between which risks are most prominent among countries or regions. For instance, North Americans and people from Western Europe see disinformation as a critical risk to their technology use. Survey respondents in South and East Asia still perceive such risks but at notably lower levels.

According to the 2019 survey by Microsoft and IDC Asia/Pacific which was conducted to understand

Table 1. Consumer Concerns on Digital Trade by Stages of Purchasing Activities

		Pre-Purchase	Purchase	Post-Purchase
Description/Items		Information disclosure	Contract terms Product features	Right of withdrawal Resolution and redress
Consumer concerns	General	Concerns about connectivity (slow internet or shutdown, lack of broadband coverage, malware etc.) Concerns about online privacy and abuse of personal information Concerns about cyber-security Online disinformation (receiving false information, such as news or information which is not true) Online fraud (fraud such as someone stealing your bank information or your money) Online harassment. (online bullying, such as someone sending a hateful message or comment through social media)		
	By stage	Information asymmetry Unfair commercial practices such as aggressive marketing techniques, misleading advertising, or spams The lack of consumer protection against unscrupulous suppliers	Electronic contract (the validity of a contract concluded online) Contractual concerns (the rights and obligations involving an electronic transaction, supplier liability, plain language embodied in consumer legislation, warranties) Logistical concerns (the goods taking too long to arrive) Payment concerns (the inability to easily pay for the goods across borders, online payment security, insufficient laws, bad enforcement / cybercrime)	Liability rules (faulty or counterfeit goods, late or no delivery, the possibility of low-quality or no feedback/after-sales services from suppliers) Dispute resolution (long delays in resolving disputes)

Sources: Authors analysis from Esselaar (2020), Jaller et al (2020) and WEF (2019).

consumer trust in digital services in the Asia Pacific, only 31% of consumers in the region trust organizations offering digital services to protect their personal data. Nearly 40% of consumers in the region have had their trust compromised when using digital services, and only 5% of consumers prefer to transact with an organization that offers a cheaper but less trusted digital platform (Microsoft, 2019). By sector, consumers have the highest expectations of trust from financial services, healthcare and education sectors, and consumers feel that governments followed by technology companies should take the lead in building trust. The study, which surveyed 6,372 consumers across 14 markets in the Asia Pacific, asked respondents to provide their opinions on the five elements of trust jointly defined by IDC and Microsoft – namely privacy, security, reliability, ethics, and compliance – when using digital services. This survey revealed that consumers feel that all five elements of trust are almost equally important to them. Particularly, security (88%), privacy (87%), and reliability (84%) emerged as the top three most important elements (Microsoft, 2019).

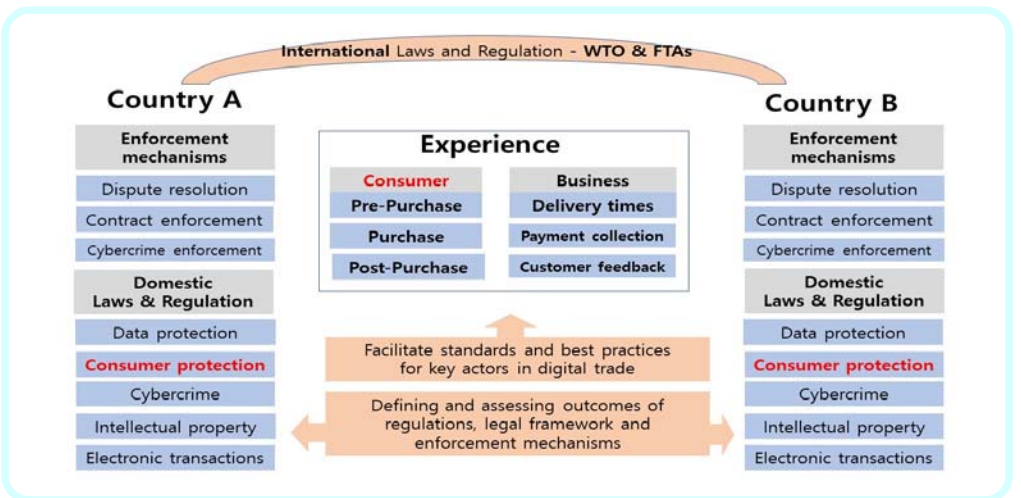
Factors shaping the confidence of consumers engaging in digital trade can be categorized by stages of consumer protection regulations in digital trade (See Table 1). While participating in digital trade, consumers have both general concerns and stage-specific concerns. General consumer concerns include connectivity-related ones, those on online privacy, abuse of personal information, cyber-security, dis-information, fraud, and harassment. In the pre-purchase stage, consumers are usually concerned with the lack of consumer protection against unscrupulous suppliers. In the purchase stage, they are mostly concerned with logistics, payment, and the means or methods related to online transactions. In the post-purchase stage, they are easily concerned with the possibility of low-quality or no feedback or after-sales services from suppliers as well as long delays in resolving disputes. In terms of consumer trust in digital trade, the government is mandated to make a safe environment that must exist for consumers to trust online suppliers. For instance, consumers want to know if they can return, at no extra cost, goods that they bought online as they can only properly evaluate the goods once they have been delivered. They also want to cancel reservations or bookings at a reasonable fee if they have to. Payments and refunds for customers should be easy to make and receive. A consumer's online transaction with the supplier should be communicated in plain language. Goods transacted should be of sufficient quality and have automatic warranties for a reasonable period and suppliers are obliged to warn consumers of risks. Under trust-building rules and regulations, suppliers should be prevented from making false promises as fraudulent schemes are prohibited. Unsafe goods should be identified and removed from the marketplace (Esselaar, 2020). As digital markets are still in their infancy, the top reason for not engaging in online purchases, at least in developed markets, remains the lack of trust in remote electronic transactions. Consumers typically have no face-to-face contact with vendors, leading to few "visual cues," such as location, facilities, and personalized interaction, which helps consumers gauge the retailer or suppliers' professionalism. In this environment, consumers are asked to disclose sensitive information and personal data either to a retailer, online intermediary, or digital platform. As a result, one important limiting factor in both developed and developing econo-mies is the perception that cross-border online transactions and delivery are less secure, and remedies do not exist for when something goes wrong. The rules for consumer protection in digital trade should be clear and understandable and better be globally coordinated between countries.[2] International coop-eration in terms of consumer trust in digital trade is essential to reduce their concerns and facilitate trust for global consumers.

2) In the meantime, there should be a balanced approach to consumer protection that acknowledges that the consumer is at fault sometimes as industry needs and problems should be also considered by the appropriate regulatory body in each country, such as the consumer protection agency.

2. Trust-Building Regulation for Consumers in Digital Trade

International society should cooperate to build a consumer trust-building mechanism for global consumers who participate in digital trade. Now is the era when the nationality of each consumer does not guarantee a sufficient level of consumer protection within his or her country's jurisdiction. Internationally coordinated rules and regulations play an essential role in bolstering digital markets by promoting consumer trust (Jaller et al., 2020). Among the three sets of regulations that are relevant to promoting consumers' trust in digital markets, an effective framework for online consumer protection helps consumers be better informed about the characteristics of the goods or services at hand as well as the terms of the transaction, promoting a greater understanding of the conditions of the transaction (Jaller et al., 2020). As distance shopping presents challenges such as the inability to assess products in person before confirming a transaction, online consumer protection laws aim to ensure "a level of protection not less than that afforded in offline commerce" (Jaller et al., 2020). The main guiding principles for online consumer protection are recognized in two main international soft-law instruments: the UNCTAD Guidelines on Consumer Protection of 1985 (revised 1999 and updated in 2015) and the OECD revised its Recommendation on Consumer Protection for E-commerce of 1998 (revised 2016) (Jaller et al., 2020). The OECD guidelines are more innovative in the sense that they embrace further issues, such as non-monetary transactions, digital content products, active consumers, mobile devices, privacy and security risks, payment protection, and product safety. Meanwhile, online consumer protection laws are scarce across the globe as 97 countries have enacted such laws, 10 percent have draft legislation, 21 percent no legislation, and 12 percent no available data (Jaller et al., 2020). More concerning is that these laws are fragmented at the national level. Consumer laws, information laws, contractual laws, etc. may encompass online consumer rights. Among the 97 jurisdictions listed by UNCTAD, some countries provide laws that only partly entitle rights for online consumers. According to international guidelines, a detailed framework for online consumer protection should include digital-specific protections at all stages of the transaction (Jaller et al., 2020). As we have seen in the previous section, consumer concerns in digital trade include whether the information they enter online is safe and the conditions for the sale (pre-purchase), whether the goods purchased online will meet their expectations

Fig. 6. Two-track Trust Building Framework for Consumers and Business



Source: Authors analysis from Esselaar (2020) and Jaller et al (2020).

when they arrive (purchase), and whether they are entitled to any remedies if any problems arise during or after the transaction (post-purchase). These can be addressed through regulations addressing information disclosure requirements, the right to withdraw from a transaction, dispute resolution, and redress at both national and international levels (See Fig. 6).

To build and facilitate consumer trust in digital trade domestically, each government needs to create relevant online consumer protection rules and there should be global governance to create and focus more on personal data protection. It is necessary to reinforce international policy cooperation to raise system-wide online trust internationally, alongside reducing international friction, with the help of multilateral as well as bilateral digital trade agreements. An increasing number of free trade agreements (FTAs) aims to reinforce standards and ensure transparent approaches.[3] Some encourage cooperation between online consumer protection agencies while others mandate putting personal information protection laws in place. In January 2019, 76 nations responsible for 90% of global trade committed to begin negotiations on the trade-related aspects of e-commerce (Banga, 2021). Although it is too early to tell the exact scope of these talks, proposals in the preparatory phase have included online consumer protection issues. These are mostly vague on substantive content, but talks could move toward global trade rules, encouraging minimum legal frameworks and convergence on the principles driving regulation. Particularly, in major FTAs concerning digital trade, articles concerning consumer trust exist: online consumer protection, personal information protection, unsolicited commercial electronic messages, domestic regulatory framework, transparency, cybersecurity, access to and use of the internet for electronic commerce, creating a safe online environment, and cooperation on competition policy. There are key questions to be asked: does the agreement mention trust?; does it enforce domestic laws regarding privacy?; does it enforce domestic law regarding consumer protection?; and does it enforce domestic laws regarding spam messages (KIEP, 2021). Certainly, a free flow with the trust template could include interoperability for personal data and consumer welfare and regulatory cooperation, the discussion of creating UNICTRAL laws for personal data protection, and consumer welfare. In the next section, specific issues or articles of consumer trust of digital trade both in multilateral and bilateral trade agreements will be analyzed. Particularly, articles related to consumer trust in six regional FTAs such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Japan Digital Trade Agreement (USJDTA), the United States-Mexico-Canada Agreement (USMCA), the Digital Economic Partnership Agreement (DEPA), the Australia-Singapore Digital Economic Agreement (DEA), and the Regional Comprehensive Economic Partnership (RCEP) will be compared in depth.

Ⅲ. Consumer Trust and Digital Trade Agreements

1. WTO E-Commerce Negotiation

In the WTO, there are ongoing efforts led by the leading digital economies in the North to have binding commitments through digital rules to facilitate digital trade and reduce barriers to it (Banga, 2021). From 1998 to the 10th WTO Ministerial Conference, a group of 86 countries (EU-27 plus 59 countries) have been negotiating digital rules under a 'Joint Statement Initiative on E-Commerce' which aim to facilitate exports and operations of their big-tech firms and super digital platforms.[4] At the

3) Regional trade agreements, however, have their own inherited problems such as discrimination against non-member countries as well as spaghetti-bowl phenomenon. (Cheong, 2019)

4) While these negotiations are being touted as WTO negotiations, it needs to be noted that this initiative remains outside the ambits of the WTO (Banga, 2021). In other words, any initiative to negotiate e-commerce rules was recognized by this group of countries to be outside the WTO agreements and its mandates while the WTO mandate cov-

11th WTO Ministerial Conference on 13th December 2017, Ministers of 71 countries (EU-28 plus 43 countries) declared that they would continue the work under the Work Program on Electronic Commerce in which they agreed to "maintain the current practice of not imposing customs duties on electronic transmissions until our next session which we have decided to hold in 2019" (Banga, 2021). At the World Economic Forum on 25th January 2019, the group of 76 countries (EU-28 and 48 countries) issued another Joint Statement which announced their intention to commence negotiations on trade-related aspects of electronic commerce. So far, there has been no consensus on including the JSI on E-Commerce into the WTO as a plurilateral agreement. While 60 members of JSI are engaged in these negotiations, the proposals which are shaping the digital rules are received mainly by the developed countries like Canada, the EU, the US, the UK, Japan, and New Zealand. Finally, a consolidated negotiating text was circulated in December 2020 which brings together the proposals of different members of the JSI on various digital rules which are being negotiated. The consolidated negotiating text of JSI on e-commerce has six sections and an annex dealing with different digital rules, which go much beyond traditional e-commerce. These six sections categorize digital rules as follows: Enabling electronic commerce; Openness and electronic commerce; Trust and electronic commerce; Cross-cutting issues; Telecommunications; and Market access (Banga, 2021).

In the section on trust and electronic commerce, the proposals for digital rules on online consumer protection, unsolicited commercial electronic messages, and personal data protection and privacy are directly related to consumer trust. On consumer trust, the proposals are more flexible and relate to higher cooperation and consideration to measures that encourage trust, providing equal protection to online and offline consumers as well as mechanisms for consumer redress (Banga, 2021). Besides, both developed and developing countries such as the EU, the US, Japan, the UK, Korea, Canada, the China Russian Federation, Singapore, Hong Kong, Brazil, and Ukraine have submitted proposals on the protection of personal data and privacy. Thus, countries are negotiating whether the members shall or may adopt legal frameworks to protect personal data, recognizing the importance of the protection of personal data. In February 2020, at the first meeting of the year on e-commerce negotiations, held on 5 February, co-convenor Ambassador George Mina (Australia) commended WTO members for finalizing a clean negotiating text on the issue of unsolicited commercial messages, otherwise known as spam (WTO, 2021). Moreover, at a meeting on e-commerce negotiations held on 20 April, WTO members participating in the talks announced that a "clean" negotiating text on the issue of e-signatures and authentication also has been finalized. The co-convenors of the talks – Australia, Japan, and Singapore – commended members for their hard work and urged them to accelerate their efforts to meet deadlines fixed for this year. 2021 is a critical year for the e-commerce initiative as the members of the e-commerce negotiation need to intensify the pace of talks to deliver on the goal of substantial progress by the 12th Ministerial Conference (MC12) due to take place by the end of 2021 (WTO, 2021).

2. Regional Digital Trade Agreements[5)]

With slow progress at the WTO on e-commerce, articles related to digital trade are increasingly featured in regional trade agreements (RTAs), including those on business and trade facilitation as well as business and consumer trust (Casalini and Gonzalez, 2019). Among the articles agreed, there are nine issues directly related to consumer trust: online consumer protection; personal information protection, unsolicited commercial electronic messages which means spam messages, domestic regulatory framework, transparency, cybersecurity, access to and use of the internet for electronic commerce (See Table 2). This section reviews

ers the Work Program on E-Commerce.

5) This section frequently refers to CPTPP (2018), USJDTA (2020), USMCA (2020), DEPA (2021), DEA (2020), and RCEP (2020).

and compares a selection of six major digital trade agreements, intending to identify the relevant language used in each agreement and find differences in terms of length and quality.

Table 2. Major Articles Related to Consumer Trust in Major Digital Trade Agreements

#	Articles	CPTPP (Dec. 2018)	USJDTA (Jan. 2020)	USMCA (Jul. 2020)	DEPA (Jan. 2021)	DEA (Dec. 2020)	RCEP (Nov. 2020)
1	Online consumer protection	14.7 (1-3)	14 (1-2)	19.7 (1-3)	6.3 (1-8)	15 (1-6)	12.7 (1-4)
2	Personal information protection	14.8 (1-5)	15 (1-4)	19.8 (1-6)	4.2 (1-10)	17 (1-9)	12.8 (1-5)
3	Unsolicited commercial electronic messages	14.14 (1-3)	16 (1-2)	19.13 (1-5)	6.2 (1-3)	19 (1-4)	12.9 (1-3)
4	Domestic regulatory framework	14.5 (1-2)	9 (1-2)	19.5 (1-2)	2.3 (1-3)	8 (1-4)	12.10 (1-2)
5	Transparency	n/a	n/a	n/a	13.1- 13.5	14 (1-5)	12.12 (1-2)
6	Cyber security	14.16	19 (1-2)	19.15 (1-2)	5.1(1-2)	34 (1-2)	12.13
7	Access to and use of the internet for electronic commerce	14.10	n/a	19.10	6.4	20	n/a
8	Creating a safe online environment	n/a	n/a	n/a	5.2 (1-3)	18 (1-5)	n/a
9	Cooperation on competition policy	n/a	n/a	n/a	8.4 (1-3)	16 (1-2)	n/a

Source: Authors analysis from Cheong (2019) and Ko (2020).

2.1. Online Consumer Protection

CPTPP contains a relatively complete set of provisions on online consumer protection while only USMCA has a similar structure and sentences regarding articles on online consumer protection, among the six digital trade agreements. In Article 14.7.1, “The Parties recognise the importance of adopting and maintaining transparent and effective measures to protect consumers from fraudulent and deceptive commercial activities as referred to in Article 16. 6.2 (Consumer Protection) when they engage in electronic commerce.” In Chapter 6, CPTPP includes articles on competition policy, and in Article 16.6. it stipulates as “For the purposes of this Article, fraudulent and deceptive commercial activities refers to those fraudulent and deceptive commercial practices that cause actual harm to consumers, or that pose an imminent threat of such harm if not prevented, for example: (a) a practice of making misrepresentations of material fact, including implied factual misrepresentations, that cause significant detriment to the economic interests of misled consumers; (b) a practice of failing to deliver products or provide services to consumers after the consumers are charged; or (c) a practice of charging or debiting consumers’ financial, telephone or other accounts without authorisation.” USJDTA, RCEP, DEPA, and DEA have no mentioning of the chapter on competition policy while only DEPA and DEA have a separate chapter on cooperation on competition policy.

Article 14.7.2 of CPTPP is the key part which contains an obligation as “Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities” and the following three digital trade agreements are similar in length and meaning. All of the six trade agreements have this article with an obligation on domestic consumer protection laws. Meanwhile, RCEP shares the first two articles with CPTPP, but its Article 12.7.3 is similar to Article 16.6.6 of CPTPP while its Article 7.4 to Article 14.8.4 of CPTPP.

2.2. Personal Information Protection

All the six trade agreements have similar articles regarding personal information protection. In Article 14.8.1 and 14.8.2 of CPTPP, “The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.” All of the six trade agreements have this article with an obligation on a legal framework that provides for the protection of the personal information of the users of electronic commerce. In its footnotes of CPTPP, however, “Brunei Darussalam and Viet Nam are not required to apply this Article before the date on which that Party implements its legal framework that provides for the protection of personal data of the users of electronic commerce” while RCEP has a footnote as “ Cambodia, Lao PDR, and Myanmar shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement.” Also, all of the six trade agreements contain “For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.”

2.3. Unsolicited Commercial Electronic Messages

All of the six trade agreements have similar articles regarding unsolicited commercial electronic messages. In Article 14.14.1 and 14.14.2 of CPTPP, “1. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; (b) require the consent, as specified according to the laws and regulations of each Party, of recipients to receive commercial electronic messages; or (c) otherwise provide for the minimisation of unsolicited commercial electronic messages.” And “Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages that do not comply with the measures adopted or maintained pursuant to paragraph 1.” In its footnote of CPTPP, however, “Brunei Darussalam is not required to apply this Article before the date on which it implements its legal framework regarding unsolicited commercial electronic messages” while RCEP has a footnote as “Cambodia, Lao PDR, and Myanmar shall not be obliged to apply this paragraph for a period of five years after the date of entry into force of this Agreement. Brunei Darussalam shall not be obliged to apply this paragraph for a period of three years after the date of entry into force of this Agreement.”

2.4. Domestic Regulatory Framework

All the six trade agreements have similar articles regarding domestic regulatory framework. In Article

14.5.1 and 14.5.2 of CPTPP, "Each Party shall maintain a legal framework governing electronic transactions consistent with the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the United Nations Convention on the Use of Electronic Communications in International Contracts, done at New York, November 23, 2005." which mandates countries following the international agreement on contracts of e-commerce. And "Each Party shall endeavour to: (a) avoid any unnecessary regulatory burden on electronic transactions; and (b) facilitate input by interested persons in the development of its legal framework for electronic transactions."

2.5. Transparency

Regarding transparency, only three digital trade agreements have relevant articles, including DEPA, DEA, and RCEP. DEPA has two modules mentioning the issue of consumer trust: Module 5. Wider Trust Environment with Article 5.1 (Cybersecurity cooperation) and Article 5.2 (Online safety and security) and Module 6. Business and Consumer Trust with Article 6.1 (Definitions), Article 6.2 (Unsolicited commercial electronic messages), Article 6.3 (Online consumer protection), and Article 6.4 (Principles on Access to and use of the internet). In addition to the two modules, DEPA has the lengthiest articles on transparency in Article 14. The article contains 5 issues as definitions, publication, administrative proceedings, review and appeal, and notification and provision of information. In Article 14.2 and 14.3 of DEA, "Each Party shall promptly publish, or otherwise promptly make publicly available where publication is not practicable, its laws, regulations, procedures and administrative rulings of general application with respect to any matter covered by this Chapter. Each Party shall respond promptly to any request by the other Party for specific information on any of its actual or proposed laws or regulations referred to in paragraph 2" which are like those in RCEP.

2.6. Cybersecurity

All the six trade agreements have similar articles regarding cybersecurity while CPTPP contains a relatively complete set of provisions on this issue. In Article 14.16 of CPTPP, "The Parties recognise the importance of: (a) building the capabilities of their national entities responsible for computer security incident response; and (b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties." In Article 5.1.2 of DEPA, it adds "(c) workforce development in the area of cybersecurity, including through possible initiatives relating to mutual recognition of qualifications, diversity and equality," similar to the one in Article 34.2 of DEPA.

2.7. Access to and Use of the Internet for Electronic Commerce

Regarding access to and use of the Internet for electronic commerce, only four digital trade agreements have relevant articles, including CPTPP, USMCA, DEPA, and DEA while CPTPP contains a relatively complete set of provisions on this issue. In Article 14.10 of CPTPP, "Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to: (a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management; (b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and (c) access information on the network management practices of a consumer's Internet access service supplier."

2.8. Creating a Safe Online Environment

For creating a safe online environment, only DEPA and DEA have relevant articles since those are the most recent and advanced forms among the six digital trade agreements, in terms of specificity

of issues and depth of discussion. In Article 5.2 of DEPA, " The Parties recognise that a safe and secure online environment supports the digital economy. The Parties recognise the importance of taking a multi-stakeholder approach to addressing online safety and security issues. The Parties shall endeavour to cooperate to advance collaborative solutions to global issues affecting online safety and security." In Article 18.1 of DEA, it has an article with obligation as "The Parties shall create and promote a safe online environment where users are protected from harmful content, including terrorist and violent extremist content, and where businesses, innovation and creativity can thrive." It adds as "The Parties also recognise that industry has a responsibility to adopt or maintain preventative measures to protect natural persons, especially children and vulnerable members of the community, from harmful online experiences. The Parties shall work together and within international fora to create a safe online environment, in accordance with their respective laws and regulations. In working together to create a safe online environment, the Parties shall endeavour to maintain an open, free and secure Internet in accordance with their respective laws and regulations."

2.9. Cooperation on Competition Policy

As mentioned in 2.1, for cooperation on competition policy, DEPA and DEA have relevant articles within digital agreements, not in a separate competition chapter. In Article 16 of DEA, "Recognising that the Parties can benefit by sharing their experiences in enforcing competition law and in developing and implementing competition policies to address the challenges that arise from the digital economy, the Parties shall consider undertaking agreed technical cooperation activities, subject to available resources, including: (a) exchanging information and experiences on the development of competition policies for digital markets; (b) sharing best practices on the enforcement of competition law and the promotion of competition in digital markets; (c) providing advice or training, including through the exchange of officials, to assist a Party to build necessary capacities to strengthen competition policy development and competition law enforcement in digital markets; or (d) any other form of technical cooperation agreed by the Parties. Subject to each Party's available resources, the Parties shall endeavour to cooperate, where practicable and in accordance with their respective laws and regulations, on issues of competition law enforcement in digital markets, including through notification, consultation and the exchange of information." In Article 8.4.3 of DEPA, it adds "The Parties shall cooperate in a manner compatible with their respective laws, regulations and important interests, and within their reasonably available resources."

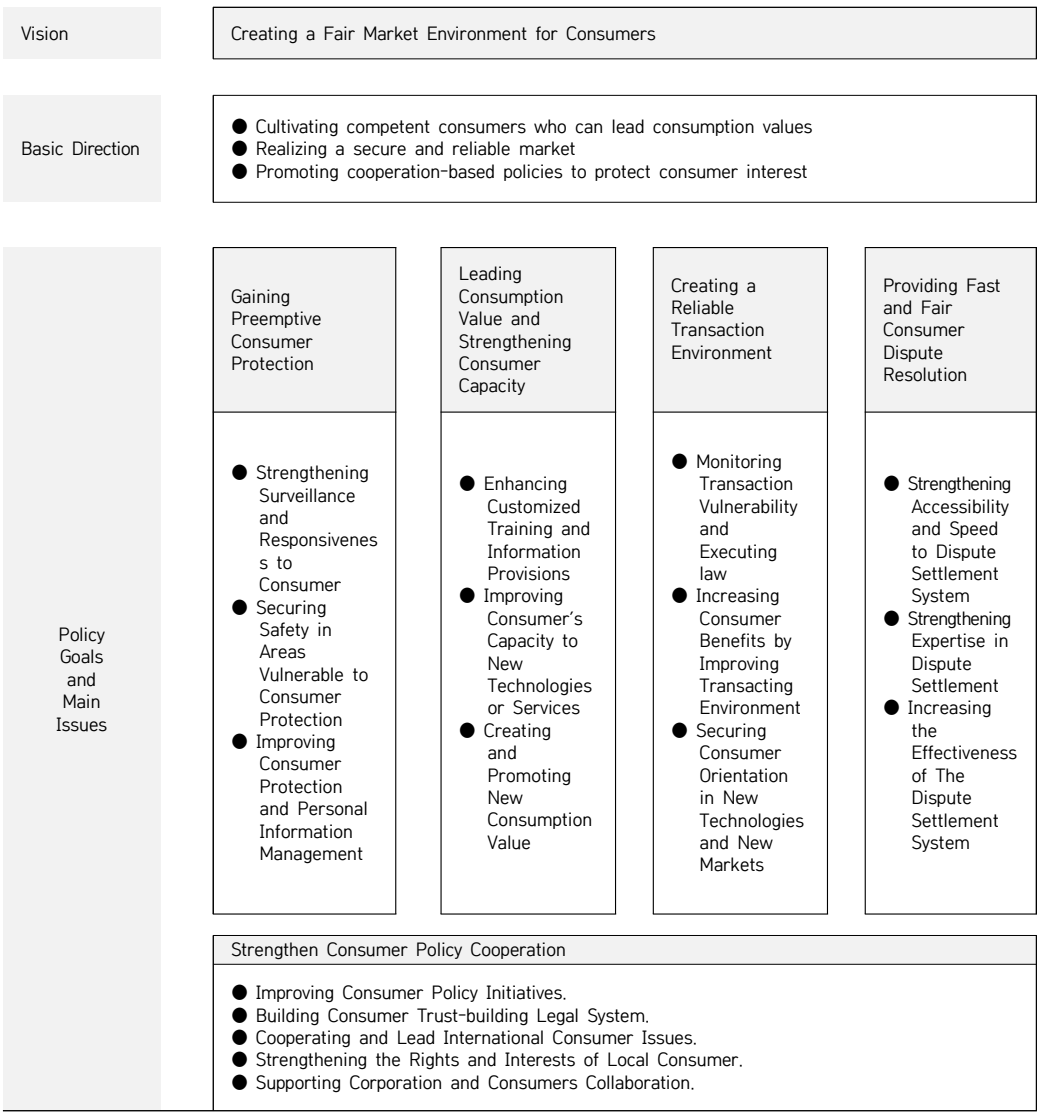
3. Analysis and Implications

By reviewing the six major digital trade agreements on nine issue areas of consumer trust, we can find the following. First, all the six agreements certainly share the significance of building consumer trust to facilitate digital trade while they broaden the concept of digital trade from that of traditional e-commerce. Particularly, DEPA and DEA explicitly mention consumer trust in their articles. All six agreements have articles with obligations for enforcing domestic laws regarding privacy as well as consumer protection and spam messages. Second, the consensus of signatory countries on the five issues, such as online consumer protection, personal information protection, unsolicited commercial electronic messages, domestic regulatory framework, and cybersecurity, seems relatively easy to make since articles in those issues in six agreements are similar in their length and quality.[6] Third, the remaining three issues, compared to the five mentioned, are relatively new

6) CPTPP, however, has the footnotes mentioning the exempted countries concerning their primitive stage of development of the domestic e-commerce market as well as domestic regulations.

and started to be discussed as DEPA and DEA are the leading agreements in terms of length and specificity of articles stipulated.

Fig. 7. Korea's Fourth Roadmap for Consumer Policy



Source: Yoo (2020).

It is the right to ask how each country works together to agree on a digital trade agreement that substantially reflects consumers' concerns and ultimately protects their rights and privacy while still facilitating digital trade and lowering digital trade barriers. It is appropriate to consider more binding digital trade agreements with articles not only on transparency, cooperation, and stakeholder engagement but also those on other institutional arrangements such as joint committees, contact points, dialogue,

or consultations. Regarding cooperation, all except for USJDTA with DEPA have the highest level of obligation with consumer trust-building-related articles in the cooperation chapter. For dispute settlement, among the six agreements, only CPTPP, DEPA, DEA, and RCEP have relevant articles to which the scope of dispute settlement is limited[7] (DEPA, 2021). Besides regional or bilateral digital trade agreements, countries may start to discuss having UNICTRAL (United Nations Commission on International Trade Law) laws for personal data protection and consumer welfare (KIEP, 2021). To strengthen consumer trust internationally, in the form of multilateral or regional trade agreements, both e-commerce and competition chapters can cover the rules for digital trade. Domestically, there is a limit to applying the traditional consumer law and e-commerce transactions including non-monetary ones, so it is necessary to find a way to regulate digital trade, not only with consumer law but also with the Monopoly Regulation and Fair Trade Act, which is the basis of consumer protection as well as the transaction environment[8] (Lee, 2020; Yoo, 2020; Shin, 2020). Besides, the domestic digital trade policy of each country consists of three pillars: trade promotion (engagement in international for domestic policy settings, development cooperation, and capacity building); trade negotiation (engagement in international for negotiation of international trade rules and internal negotiation with domestic trade stakeholders), and trade dispute settlement (domestic, foreign, or WTO disputes, enforcing, monitoring agreed on international rules, and domestic policy settings). Digital trade policy should incorporate policy elements as strengthening consumer policy cooperation with other countries (See Fig. 7).

Ⅳ. Conclusion

Strengthening consumer trust is the engine for digital growth (Esselaar, 2020). The key to accelerating digital transformation is to build a trust framework. This means new or updated laws and regulations both at the domestic and international levels. Focusing particularly on the issue of consumer trust-building, this paper attempts to categorize major consumer concerns for digital trade and suggest consumer trust-building in international regulations, then conducts a comparative analysis of articles related to consumer trust in six major digital trade agreements. Emerging concerns includes not only the amount of information gathered, but also the use made of it is not always clear to the consumer (Honey, 2021). The data gathered can be monetised in another form, such as by selling it to other firms who may make use of it for marketing or other purposes, not only just recording our activities that we may wish not to share with a company. Of course, consumers benefit from sharing personal information, helping them reconnect with long-lost friends using social networks or using ‘free’ software solutions for email, scheduling or navigation. But price of these services is often the personal data of the individuals, generated while the services are provided. The economics of privacy is ambiguous such that we access free online services, but at the expense of less privacy. While consumers have both general concerns and stage-specific concerns, six major digital trade agreements already have nine issues directly related to consumer trust: online consumer protection; personal information protection, unsolicited commercial electronic messages which means spam messages, domestic regulatory framework, transparency, cybersecurity, access to and use of the internet for electronic commerce. In summary, all six agreements certainly share the significance of building consumer trust to facilitate digital trade while they broaden the concept of digital trade from that of traditional e-commerce. Moreover, the consensus of signatory countries on the five issues, such as online consumer protection, personal information protection, unsolicited commercial electronic

7) In the case of DEPA, it has not only transparency, cooperation, joint committee, and contact-point but also disputes settlement, mediation mechanism, and arbitration mechanism.

8) Lee (2020) suggests that it is necessary to prepare the Guidelines for Examining the Abuse of Status in Transactions by Digital Platform Operators (tentative name) to properly regulate non-monetary transactions.

messages, domestic regulatory framework, and cybersecurity, seem relatively easy to make since articles in those issues in six agreements are similar in their length and quality.

Privacy itself is so difficult to define that the value we attach to it, whether as individuals or in society, can be subjective. As privacy protection differs across countries, reflecting different cultural and social traditions and norms, personal information is defined differently across countries. That is why privacy and personal data protection is more challenging when data cross jurisdictions. In this sense, global consumers should work together for better international rules for online consumer protection, strengthening cross-border cooperation as well as protecting vulnerable consumers in the digital age such as children, young people, and elderly consumers. (OECD, 2019) According to an analysis of 1,500 cases related to overseas businesses over the past five years, that of 2020 (411 cases) increased by 35.2% (107) from that of 2019 (304 cases), and the number of related cases has increased every year since 2017. (Korea Fair Trade Commission, 2021) Of the 1,500 damage relief cases, 51.6% were compensated, including refunds, compensation, and cancellation of contracts, while 48.2% (723 cases) were not compensated due to the return of official documents for damage relief and loss of contact with businesses. Therefore, to make it easier for consumers who have traded with overseas operators to receive damage relief, it is necessary to introduce a system that allows them to actively respond to consumer disputes by having domestic agents representing their headquarters. In other words, it is necessary to strengthen the responsibility of foreign operators to protect consumers in Korea. For future studies, it is recommended to survey Korean consumers participating in digital trade, either by the government or by academia.[9] Studies on institutional arrangements in digital trade agreements are also attractive in which we can find out how binding the rules are when enforced.

References

Banga, R. (2021), *Joint Statement Initiative on E-Commerce (JSI): Economic and Fiscal Implications for the South* (UNCTAD Research Paper, No. 58), Geneva, Switzerland: UNCTAD, 1-30.

Casalini, F. and J. López González (2019), *Trade and Cross-border Data Flows* (OECD Trade Policy Papers, No. 220), Paris: OECD, 1-40. http://dx.doi.org/10.1787/b2023a47-en

Cheong, Sun-Tae (2019), "A Study on the Performance and Limitations of Regional Trade Agreements in the Liberalization of Digital Trade", *Journal of International Trade and Commerce*, 15(5), 315-335. http://dx.doi.org/10.16980/jitc.15.5.201910.315

CPTPP (2018), *The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Text.* Available from https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/text-texte/index.aspx?lang=eng

DEA (2020), *The Australia-Singapore Digital Economy Agreement Text.* Available from https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

DEPA (2021), *The Digital Economy Partnership Agreement Text.* Available from https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/depa-text-and-resources

9) The survey data available, though extensive in its geographic reach, only included a small number of questions about technology-related risk. More detailed research on the topic is required to fully describe the range of differences in the risks created by technology and how they are experienced by people in different positions. Further research would also be required to be able to explain these differences and to see whether they relate to differences in technological environments or, for instance, cultural or social institutions. The results do remind us, however, that the impact of social media and new information technologies varies from country to country, culture to culture, and person to person (Knuutila, 2020).

Esselaar, P. (2020), *Trust Building Framework*. Available from file:///C:/Users/PC/AppData/Local/Temp/_AZTMP10_/E%202020%20Digital%20trade%20and%20trust.pdf

Honey, S. (2021), "Asia-Pacific Digital Trade Policy Innovation". In I. Borchert and L. Winters (Eds.), *Addressing Impediments to Digital Trade*, London: CEPR Press, 217-238.

Jaller, L. D., G. Simon and M. Martín (2020), *The Regulation of Digital Trade Key Policies and International Trends*. Available from file:///C:/Users/PC/AppData/Local/Temp/_AZTMP14_/WB%202020%20The%20Regulation%20of%20Digital%20Trade.pdf

KIEP (Korea Institute for International Eonomic Policy) (2021), *Webinar on Trade Policy of Biden Administration.* Available from https://www.youtube.com/watch?v=Lu32WfUn3jQ&form=MY01SV&OCID=MY01SV

Knuutila, A., N. Lisa-Maria, N. H. Philip (2020), *Global Fears of Disinformation Perceived Internet and Social Media Harms in 142 Countries* (COMPROP Data Memo2020.8, 15.12.2020), Oxford, UK: Oxford Internet Institute, 1-5.

Ko, Bo-Min (2020), "Major Digital Trade Agreements and the Implications for the Korea-Singapore Digital Partnership Agreement (DPA)", *Journal of International Trade and Commerce*, 16(6), 229-248. http://dx.doi.org/10.16980/jitc.16.6.202012.229

Korea Fair Trade Commission (2021), *Announcement of Consumer Damage Analysis in E-commerce 2020.* Available from https://www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=8923

Lee, Seung-Jin (2020), "Digital Platform and Consumer Issues: Non-Monetary Transaction", *Law Review*, 30(4), 497-535.

OECD (2019), *Challenges to Consumer Policy in the Digital Age.* Available from https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf

OECD (2020), *Handbook on Measuring Digital Trade*. Available from OECD_WTO_IMF 2020 Handbook-on-Measuring-Digital-Trade.pdf

RCEP (2020), *The Regional Comprehensive Economic Partnership Text*. Available from http://rcepsec.org/legal-text/

Shin, Hyeon-Joo (2020), "A Study on Recent Trends in Digital Trade Rules and Implications for the Personal Information Protection Act", *Journal of International Trade & Commerce*, 16(2), 491-502. http://dx.doi.org/10.16980/jitc.16.2.202004.491

Statista (2020), *E-Commerce - Digital Shopping Behaviour*. Available from https://www.statista.com/statistics/1192578/worldwide-share-of-consumers-that-shop-online/

The Official Website of Korea's FTAs (2020), *Korea's Free Trade Agreements*. Available from www.fta.go.kr

The World Trade Organization (2021), *News about Electronic Commerce.* Available from https://www.wto.org/english/news_e/archive_e/ecom_arc_e.htm

Tran, T. (2019), *Approach to Measuring the Digital Economy: Global Affairs Canada.* APEC Workshop on the Digital Economy: Measurement, Regulation and Inclusion, Santiago, Chile, March 6. Available from file:///C:/Users/PC/AppData/Local/Temp/_AZTMP24_/Canada_APEC%202019%20Measuring%20the%20Digital%20Economy.pdf

UNCTAD CIGI (Center for International Governance Innovation) (2019), *Fake News: A Global Epidemic Vast Majority (86%) of Online Global Citizens Have Been Exposed to it, With Most (86%) Admitting to Having Fallen Victim to It*. Available from file:///C:/Users/PC/AppData/Local/Temp/_AZTMP8_/CIGI_IPSOS%20survey%202019.pdf

USJDTA (2020), *U.S.-Japan Digital Trade Agreement Text.* Available from https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text

USMCA (2020), *The US-Mexico-Canada Agreement Text.* Available from https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

WEF (World Economic Forum) (2019), *The Global Governance of Online Consumer Protection and E-commerce Building Trust.* Available from http://www3.weforum.org/docs/WEF_consumer_protection.pdf