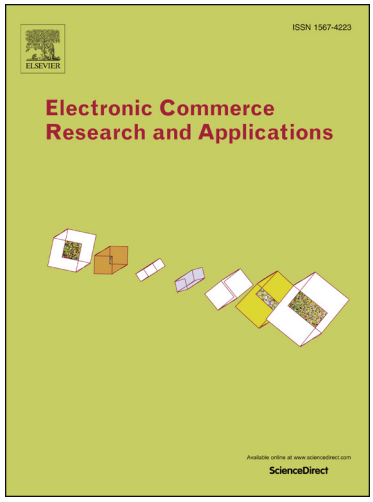

Does self-regulation provide legal protection and security to e-commerce consumers?

Djumadi, Abdul Halim Barkatullah

PII: S1567-4223(18)30056-5
DOI: https://doi.org/10.1016/j.elerap.2018.05.008
Reference: ELERAP 796

To appear in: *Electronic Commerce Research and Applications*

Received Date: 17 May 2018
Revised Date: 17 May 2018
Accepted Date: 17 May 2018

Please cite this article as: Djumadi, A.H. Barkatullah, Does self-regulation provide legal protection and security to e-commerce consumers?, *Electronic Commerce Research and Applications* (2018), doi: https://doi.org/10.1016/j.elerap.2018.05.008

DOES SELF-REGULATION PROVIDE LEGAL PROTECTION AND SECURITY TO E-COMMERCE CONSUMERS?

Djumadi, Abdul Halim Barkatullah (contact author)

Faculty of Law, Universitas Lambung Mangkurat
Jl. H. Hasan Basry, Banjarmasin 70124 South Kalimantan, Indonesia
halim.ulmbjm@gmail.com

Last revised: May 18, 2018

ABSTRACT

The development of e-commerce has reformed traditional commerce, subjecting consumers in e-commerce transactions to greater risks, while offering only a weak bargaining position when it comes to their rights. This study analyzes self-regulation as an effective means for providing legal protection and consumer security in e-commerce transactions. Using the normative legal research method, the study shows there is a difference between the United States and the European Union in the application of self-regulation. The United States focuses on a model of self-regulation, while the European Union places more emphasis on the United State's role through legislation that provides legal protection for e-commerce consumers, and Indonesia has not yet specifically regulated the protection of data privacy or used self-regulation in e-commerce transactions. Self-regulation by business actors is urgent to ensure consumer rights in e-commerce transactions are fulfilled. The findings suggest an effective model for implementing self-regulation marries the existing systems in the United States and the European Union.

Keywords: Consumer security; country analysis; customer privacy; data protection; e-commerce; European Union; Indonesia; legal issues; self-regulation; United States

---

Acknowledgments. We are grateful to the Faculty of Law Universitas Lambung Mangkurat Banjarmasin for providing financial support under grant number 2016-111-000. We thank the Dean and Head of the Department of Law for their support for our research activity.

---

1. INTRODUCTION

Electronic commerce (e-commerce) is a new form of business which is considered better than traditional business. The traditional business process with its system of payments and physical or direct meetings between sellers and buyers has changed to a telemarketing concept. *Telemarketing* is business at a distance, using the Internet as the media, where a business does not need physical meetings with consumers (Barkatullah, 2012). E-commerce has changed the way consumers perform transactions. Using the Internet, e-commerce has penetrated borders and provided greater access for the purchase of goods or services at lower prices. Competition among firms has given consumers an advantage in online transactions, especially in acquiring goods or services (Zhao, 2005)

Although consumers in e-commerce transactions do not directly meet with businesses when buying goods, they receive services online. The risks of e-commerce can include damaged goods, products not sent, lack of service, and other more serious deceptions of consumers. Because goods are bought online in an e-commerce market and then sent to the purchaser, e-commerce consumers cannot examine items thoroughly like they can in the world of traditional commerce (Andrews, 2005). Consequently, availability of appropriate and accurate information about consumers and seller is an absolute pre-requisite for e-commerce business (Shofie, 2013).

Because a seller's identity can be easily hidden in the online world, if consumers are unsatisfied with a product they purchased in an e-commerce transaction, it is difficult for them to obtain refunds or look for solutions to problems from the seller. This can lead to consumers' loss of trust in the online world (Andrews, 2005). And s a result, the advantages of e-commerce business also create risks, which may decrease consumers' trust. By using the World Wide Web, "*[t]he seller can market [his] selling [of] products beyond the jurisdiction of his country, resulting in a lot of fraudulent marketing practices, and the use of less secure payment systems for consumers, and the lack of privacy data protection for consumers*" (Alboukrek, 2003). To develop electronic international markets, the risks to consumers' safety should be eliminated or at least minimized.

In e-commerce business transactions, problems may arise about who will assume the risks if: (1) the message is dishonest, illegal, or changed; and (2) there is an error in communication caused by agents or technological problems. An example is when a server does not work or there are network problems. Although deception, integrity, and errors are not new or

special in electronic media, this technology creates unique obstacles that need innovative solutions (Zain, 2000).

E-commerce transactions are prone to fraud, and technology allows deceivers to operate without much investment. On the other hand, this technology provides more verification techniques than are available for documents written on paper. For example, digital signatures can guarantee that communications are sent by the parties to the transaction, and not by imposters. Another advantage is that receivers know that what is received is the same as what was sent, without any changes (Smedinghoff, 2010)

Online shops and websites can vanish easily after an order is placed and payment by credit card has been made. Business transactions are easier in e-commerce, but the Internet is also a media that can be misused by dishonest sellers to exploit consumers because it is an effective and inexpensive communication media. The increase in commercials on the Internet has also facilitated unfair business practices, such as misleading online commercials.

Another potentially negative impact on e-commerce consumers relates to consumer data protection at the time of an online transaction. Consumer International conducted a shopping survey in global e-commerce and concluded that although the use of the Internet to buy goods and consumer trust in the process is increasing, consumers' trust overall is low because of the lack of protection for the secrecy of consumers' data (Ferrettee, 2000). The safety of data or an individual consumer privacy and financial information is very important because a lack of security can result in data being stolen by third parties during the communication between consumers and sellers. Moreover, thieves can obtain a purchaser's credit card number by secretly entering the server or personal computer, and cheat consumers by pretending to be sellers (Makarim, 2003). The seller or third party often misuses those pieces of information to steal a consumer's identity, or the consumer's information collected by the seller is be used without consumer permission, causing a violation of the consumer's privacy.

Consumers in e-commerce transactions have greater risks than sellers and they are in an unclear situation. Moreover, those consumers who engage in e-commerce transactions receive as guarantees only the good intentions of the seller and little protection from state laws; they are in a very weak bargaining position (Sharma, 2013). Because there are no physical borders in e-commerce, there are also jurisdictional problems for consumers' courts.

Given these characteristics of e-commerce, consumer rights need to be protected. The

United Nations General Assembly on April 9, 1985, through the its Resolution Second Committee Report (A/39/789/Add.2) 39/248, addressed the legal protection of consumers. They identified the following rights of consumers, also known as universal consumer rights: (1) the right to security and safety; (2) the right to information; (3) the right to vote; (4) the right to be heard, and (5) the right to the environment.

Indonesia's Law No. 8 of 1999 on Consumer Protection (UUPK) established nine consumer rights: (1) the right to comfort, safety, and safety in consuming goods and services; (2) the right to choose goods and services and obtain the goods or services in accordance with the exchange rate and the conditions and promised warranties; (3) the right to true, clear, and honest information about the condition and guarantee of goods and services; (4) the right to be heard for opinions and complaints on goods and services used; (5) the right to appropriate advocacy of consumer protection; (6) the right to obtain coaching and consumer education; (7) the right to be treated or served properly and honestly and not discriminatively; (8) the right to compensation, indemnification, or reimbursement, if the goods and services received are not in accordance with the agreement or not as is; and (9) the rights set forth in the provisions of other laws and regulations.

If universally admitted consumers' rights are related to consumers' rights in e-commerce transactions, consumers' rights are at great risk of being violated. Moreover, when consumers engage in in e-commerce transactions, they are placed in a weak bargaining position—especially consumers of e-commerce transactions across countries.

The objectives of this research are to determine how e-commerce seller self-regulation in the United States, European Union, and Indonesia is arranged to implement protection of consumers' private data in on-line transactions and to reveal and analyze the urgency of merchant self-regulation for guaranteeing fulfillment of consumers' rights in e-commerce transactions.

2. RESEARCH METHOD

Research about seller self-regulation as an effective tool for providing legal protection and feelings of safety to consumers in e-commerce transactions is considered normative legal research (Soekanto and Mamudji, 2014), or research that refers to valid laws and regulations. This type of research can also be called *doctrinal research* (Sunggono, 2007) because the

researcher tries to determine the principals related to the problem being researched.

To find solutions to existing problems, the researcher collected legal materials by studying documents (literature study), which were classified into primary, secondary, and tertiary law. Numerous legal regulations, international conventions, legal documents, and scientific works were identified which are related to this research. The collected legal materials were processed and analyzed using a qualitative method. The analysis technique is interpretative, where legal materials are interpreted and elaborated on according to valid law norms and theories. Therefore, faulty decision making can be minimized. Decisions are made using the logical inductive reasoning, a systematic way of thinking from specific to general, and deductive reasoning, a systematic way of thinking from general to specific.

This study was conducted using *doctrine,* the *legal regulations of various countries* and *legal cases* that considered as legal protection for consumers in e-commerce transactions, including the study of Indonesian positive law and proposals of international institutions – as the first category of evidence. The type of research used is *normative juridical research*; in other words, research that is focused on examining the application of norms or norms in positive law. Because the research is normative legal research, the statutory, conceptual, and comparative approaches are used. The *statutory approach* refers to a review of legislation related to the central theme of this study. The *conceptual approach* considers juridical concepts, while the *comparative approach* in this study is used as a method to describe the events associated with the study.

The countries selected for the study are the United States, representing the common law tradition; the European Union, representing the civil law tradition; and Indonesia, representing positive law. This study uses supportive legal materials, which are divided into three categories. First, the primary legal material comprises proposals from international institutions such as the United Nations General Assembly, and regulations from various countries that already have regulations related to the theme of this research, such as the United States, the European Union, and Indonesia, among others: BW (Burgerlijk Wetboek) / Civil Code, Law No. 8 of 1999 on Consumer Protection.

The next category is *secondary legal material*, which is legal material that explains primary legal material. The secondary legal material in this study is legal material that describes the primary legal material and is non-binding. Secondary legal materials can be from the

Internet, official documents, books, articles, magazines, research results in the form of scientific reports from a seminar, and scientific reports in the form of an academic draft, or a draft constitution. Third, *tertiary legal materials* are legal materials that complement the two previous categories, such as dictionaries related to the theme of this study. Library research employs a literature study, using primary, secondary, and tertiary legal materials to obtain materials relevant to the problems being studied. Expert opinions are also needed to complement the review of primary, secondary, and tertiary legal materials. After the diverse and comprehensive research materials are collected, they are reviewed.

3. RESULTS AND DISCUSSION

3.1. Implementation of Self-Regulation by E-Commerce Sellers for Protection of Online Consumers' Private Information

Legal protection for consumers includes any effort to ensure legal certainty for consumers. With the application of legal protection for consumers in e-commerce transactions, the position of consumers who previously tended to be targets of business actors whose goal was to achieve maximum profit is strengthened; with state intervention, it is expected that consumer interests in e-commerce transactions can be protected from practices that harm them. But consumers pay little attention to the safety or privacy of their private and financial information. So if information is misused, it can create losses for consumers, such as identity theft and stolen credit card numbers. In addition, consumer information collected by sellers can be misused without consumer permission, causing privacy violation problems.

To overcome this situation, some countries have standardized how sellers are required to collect, keep, use, and show private information collected from consumers. Sellers should also actively develop and combine privacy principles into a code of practice for websites used by consumers. Technological solutions, like encryption protocols, should be developed to offer more safety to consumers when they provide personal information on the Internet (Ivascanu, 2010). To guarantee the security of consumers' private data, procedures must be taken to guarantee the safety of transactions, such as using cryptography or digital signatures.

Legal protection of consumers' private data in e-commerce transactions can be obtained according to existing legislative regulations; for example. the Law of Data Protection, or other regulations that also protect the privacy of private data. In addition, legal protection can be

obtained based on rules set by the seller, such as a privacy policy or service conditions.

Some models of privacy protection have been developed through formal intervention when needed to deal with the dangerous possibilities faced by consumers. These models are for voluntary self-regulation of sellers in the industry to standardize privacy at the seller to seller level. The regulations and legislation require sellers to follow certain practices and provide their policies for protection of individual data. One problem of facultative standards is that the standards often cannot deal with technology development (Ivascanu, 2010).

The United States and the European Union have similar objectives in protecting the privacy of their citizens who are involved in e-commerce transactions. According to Ivascanu (2010), the United States has a more secular approach in adopting Organization of Economic Cooperation and Development (OECD) guidelines than the European Union. The United States uses a laissez faire approach in regulating the online industry regarding the storage of consumer information that is entered through online transactions. A sophisticated privacy protection system has been available in the United States. When governments regulate the public sector, private regulators create systems so that online businesses will benefit sellers as well as consumers.

Although the United States has established uniform privacy policies, the government intends to let sellers regulate their own protection of consumers' privacy. The United States believes that to develop e-commerce, the private sector must take responsibility for developing and implementing a privacy policy. Moreover, it is stated in this report that the federal government must promote a form of self-regulation. To support this approach, the United States reports the success of many sellers that use self-regulation to protect the secrecy of personal information (Ivascanu, 2010).

In the United States, there is an effort to deal with illegal e-mail, privacy, and deceit through electronic communications. However, arguments about whether it is important for the government to introduce legal protection for privacy like the European Union are still going on. In contrast, the European Union's arguments are for laws to protect online consumer transactions, use of seller self-regulation, referring to risks for consumers' privacy, threats of consumers' refusal to participate in e-commerce transactions, and obstructions to development of e-commerce transactions (Ivascanu, 2010). Privacy protection laws are needed to regulate the consumer-seller relationship apart from the promising market potential (as the result of the existence of e-commerce). If consumers do not trust sellers to protect their privacy, sellers will

not profit from online consumers.

The European Commission has proposed the use of a directive on certain legal aspects of electronic commerce in internal markets, where sellers are supposed to present their complete information, and provide consumers with a means to authenticate the seller's identity (Ferrera, 2001). Regulations of advertisement accuracy will be implemented for e-commerce, and consumers are permitted to filter unwanted emails. This guideline also determines the kinds of contracts that can be entered into online and their duration. This guideline also limits the responsibility of Internet service providers (ISP) acting as a mediator between sellers and consumers.

Other proposals from the commission are to use the 1999 Council Regulation on Jurisdiction and Recognition and Enforcement of Judgments in Civil and Commercial Matters (Council of the European Communities 1999). This made it possible for consumers to demand that sellers who supply goods and service in countries where members are domiciled ignore any agreements made by consumers and sellers.

When using guidelines, the United States and the European Union's implement them differently. The United States government allows the private sector to implement their own privacy policy, whereas the European Union chooses to drive trust by increasing the transparency of online transactions. The European Union has taken over maintenance of online privacy policies from the private sector and asked its countries to implement this directive.

The United States, members of the European Union, and consumer protection organizations worldwide want e-commerce to develop. Each group realizes that technology is not enough though. Establishing consumers' trust in electronic markets is the main problem currently mentioned in the global discussion of e-commerce. All parties involved must consider consumers' problems related to making purchases online. The United States, European Union, and legal protection organizations must observe whether businesses are concerned with the same problems. In fact, every party must consider who is responsible for driving consumer trust.

According to the United States, sellers in e-commerce transactions must develop a model of self-regulation to obtain consumers' trust (Latifulhayat, 2002). The Federal Trade Commission (FTC), an independent federal agency charged with protecting the economic interests of businesses and consumers in the United States, has promoted self-regulation for sellers as an important part of legal protection for consumers. This self-regulation is in line with

principles established in the Electronic Global Regulation (Global Electronic Business Work Regulation) promoted by President Clinton and Vice President Gore to prevent government regulations that inhibit high technology investment (Clinton White House 2000).

In the rapid development of the Internet era, seller groups are in a better position to implement new and dynamic solutions for consumers' legal protection problems. In line with the development of this new technology, sellers can also develop ways to minimize technology misuse. Groups of sellers weigh and determine standards of performance and service that will increase consumers' trust in the Internet.

One of the methods used by sellers is to obtain certificates. For example, a seller could follow Better Business Bureau (BBB) guidelines for reliability by meeting some of the following requirements (Federal Trade Comission, 2017): (1) providing information about their physical location, which can be traced by the BBB; (2) having operated the business for a minimum of one year; (3) having a satisfactory system for handling consumers' complaints; (4) agreeing to online advertising regulations related to the substance of claims and advertisements directed toward children; (5) providing responses to consumers' complaints immediately; and (6) agreeing to solve disputes if asked by consumers.

Another autonomous self-regulation adopted by merchants on the Internet is applying authentication services, such as VeriSign. These services control the identity of Web sites and assure consumers that information like credit card numbers will be kept secure to avoid third parties acquiring the information (Dickie, 2000).

In some cases, sellers do not provide privacy protection. Perceiving this problem, the federal government has attempted to support the standard of industry self-regulation by reintroducing an online privacy bill of rights. This proposed bill of rights includes three items similar to the European Union Directive. The first is guaranteeing individual rights to access the information collected about them. The second is the right to know whether information collected by a seller about a certain individual will be used again. The third is that a bill submitted in a transaction payment account system must give consumers the ability to object and block their information from companies (Dickie, 2000)

In Dickie's (2000) opinion, the European Union and India have not made their own arrangements to regulate legal protection for e-commerce. The European Union has focused more on regulating the privacy and confidentiality of consumer data in e-commerce transactions.

The European Union has different perspectives than the United States on protecting consumers' data privacy and secrecy, as well as in developing consumers' trust in online transactions. The European Union gives consumers choices about protecting their privacy in its member countries in the form of legislation regulations. In their own country, the European Union asks member countries to legislate their own privacy policy: (1) to increase consumers' trust through international data protection and (2) establish consistent protection across the European Union and their business partners.

The European Union's Comprehensive Privacy Legislation, Directive on Data Protection was effective on October 25, 1998. In general, the European Union Directive establishes three objectives. First, the directive protects individuals' rights to privacy of their personal information. Second, it promotes free information flow by adjusting members' data and data protection laws. Third, the directive guarantees that data protection can safeguard inter-border data that flows to third world countries (Dickie, 2000).

As of April 19, 1999, seven of the fifteen member countries of the European Union used this directive, with eight other countries intending to use it in the future. According to the directive, electronic consumers must be given a privacy policy; they must use an open way to give information and have access to their data to change or object to its use. The European Union intended to block any activities, such sending or interacting with data from any countries that do not use the same steps to protect personal data (Dickie, 2000).

The European Union Directive (95/46/EC) is used for legislation regulation of member countries and is intended to give a uniform level of protection to personal information. The main element of this directive (Section 25) includes terms that anyone in non-European Union countries who intends to get consumers' personal information from a European Union country must guarantee "enough" protection of the information. However, other countries in the world have different systems for providing regulations because they have different traditions and approaches to personal privacy; this makes it difficult for some countries to have access to other countries' private information. For example, the United States relies on a combination of special sector legislation, regulations, and private sector codes of conduct and market strength to achieve privacy protection (Ivascanu, 2010).

The United States' reluctance to put federal legislation similar to that of the European Union (which is based on the data secrecy directive) into effect has become the subject of

debates between the two. The United States is of the opinion that seller self-regulation is a better solution than legislative regulations and refers to a survey by Jupiter Communications showing that only 10% of European Union websites have privacy policies or secrecy on their homepage, compared to 70% in the United States (Ivascanu, 2000). Finally, on March 17, 2010, they agreed to a protective program submitted by the United States in 2008 for its sellers who choose to follow a certain secrecy policy, providing protection for data about European Union citizens, making it possible for them to accept data from European Union consumers (Ivascanu, 2010)

There are several legal protection programs about web-based consumers' privacy found in the United States. They include the Online Privacy Alliance, TrustE, the Better Business Bureau (BBB) Online, and AOL Certified Merchants, among others. These programs provide certificates of ratification and confirmation for online operators who meet their requirements. The objective is to build trust and the conviction of Internet users in Internet transactions conducted via the Internet between consumers and merchants. TrustE and BBB Online are labeled with a seal or certificate of agreement, which strengthens the profile of merchants or governments. The license they offer to websites and the display of their special certificate on sites shows their support for and full trust in the website (Ivascanu, 2010)

The concept of TrustE comes from an initiative of the Electronic Frontier Foundation (Pethia, 2017) and Commerce Net Consortium in 1996 by acknowledging the need for a symbol of special trust (Pethia, 2017) with two main principles: (1) users have the right to know about the agreement; and (2) there is no one privacy principle that suffices for all situations (Pethia, 2017). After announcing a sampling program on October 16, 1996, followed by one hundred sites, Trust E was formed on June 10, 1997 with a staff and two formal auditors who were ready to operate globally.

TrustE contacted some main sites including Infoseek and Yahoo!, American Online, IBM, Netscape, and Compaq, which accepted them as a "symbol of trust" (Pethia, 2017). TrustE is commercially ready and provides services to guarantee and control consumers' privacy as an instrument of merchant self-regulation.

The legislative regulations in Indonesia have not addressed special data protection or privacy or the use of self-regulation in e-commerce transactions. The existing regulation is a general determination for merchants in Law No. 8, 1999 about Consumer Protection, where merchants' responsibilities are described in Article 7. The responsibilities of merchants are: (1)

having good faith in performing business activities; and (2) giving true, clear, and honest information about the condition and guarantee of goods and services, as well as offering explanations about their use, repair, and maintenance; (3) treating or serving consumers sincerely, honestly, and exclusively;[1] (4) guaranteeing quality and services produced and traded according to valid quality standard stipulations of goods and services; (5) giving consumers the opportunity to test and try certain goods and services and guaranteeing the goods and services traded;[2] and (6) giving compensation, refunds, and replacement if goods and services accepted or used are not suitable based on the agreement.

The responsibility of merchants to have good faith in their business activities is one of the principles known in contract law. The determination of good faith is included in Article 1338 that a contract must be carried out with good faith. In the Law of Consumer Protection, merchants are responsible for good faith in running their businesses; consumers have the responsibility to engage in transactions to purchase goods and services in good faith.

In the Law of Consumer Protection, good faith by the merchant is emphasized. This good faith comprises all stages of running a business, meaning that it is the responsibility of the merchant to exhibit good faith beginning when the goods are planned or produced until after the sale. On the other hand, consumers' responsibility is only in engaging in the transaction to buy goods or services. Of course, this difference is because the possibility of carelessness by the merchant begins with planning and production, while for consumers the possibility of harming the merchant begins at the time of the transaction with the merchant.

Based on the merchant's good faith, the merchant will undertake other responsibilities such as giving true, clear, and honest information; giving good service to consumers; guaranteeing the quality of produced goods or service; and so on. If it is understood well, it is clear that those responsibilities are manifestations of consumers' rights; in other words, "targeted" to create a responsibility "culture" for merchants.

The Law of Consumer Protection also lists various prohibitions for merchants in Article 8. For example, merchants are prohibited from producing or trading goods or services that do not meet: (1) the standards required in the legal stipulation; (2) the net weight, net content, and

[1] We further note that, according to Article 7, "[m]erchants are prohibited from giving different service to consumers. Merchants are prohibited from giving different quality of service to consumers."
[2] In addition, we also must note that the article also states that "[w]hat is meant by certain goods and/or service are goods that can be tested or tried without causing damage or loss."

counted number as stated on label or protocol of goods; (3) the size, measuring container, weight, and counted number according to actual size; (4) the condition, guarantee, specialty, or effectiveness as stated on the label, protocol, or information of goods or service; (5) the quality, level, composition, process of preparation, style, mode or certain use as stated on the label or information of goods or services; and (6) the promise stated on the label, protocol, information, advertisement, or sale promotion of goods and services.

Further, the law states that: (7) an expired date or span of best time of use and advantage of the goods must not be present; and (8) halal production regulations must be met when the statement "halal" is on the label. In addition, (9) there should not be a label or explanation of goods containing the name, size, net content, composition, direction, production date, side-effects, name and address of merchant and other information for use which according to regulation must be provided, and (10) there should not be information or direction for use of goods in Indonesian according to legal regulations in effect.

The Law of Consumer Protection defines consumers' legal protection as all legal principles and rules that regulate and protect consumers in their relationships and various problems with providers of consumer goods or services. The legal relationship between the goods or service providers and consumers bears rights and obligations as the basis for responsibility. Principally, responsibility is the same as the general concept of legal obligation.

Considering the basic norms, it can be said that merchants have obligations and responsibilities to obey the regulations. In principle, merchants can be asked to take responsibility if there is any loss by consumers as the result of a transaction failure. It also can be seen that the relationships among the parts of an e-commerce or Internet business transaction should involve not only merchants and consumers, but also providers. Although there are other supporting contracts for the ease of transaction processes, what is more important are the positions of each part related to the rights and responsibilities created by legal relationships in the world of commerce.

State intervention has occurred through arrangements to protect consumers in e-commerce transactions. As the European Union has adopted the Council Directive on Legal Aspects of Electronic Commerce, it certifies the Distance Selling Directive and Privacy Directive. In the United States, the Federal Trade Commission (FTC) is active in asserting that its laws, regulations, and guidelines can be applied to electronic commerce transactions as in

other traditional forms of transactions. The FTC offers various publications, such as Advertising and Marketing on the Internet, The Rules of the Road, A Guide to Online Payment, and Dot Com Disclosures.

Each country is different in providing legal protection for consumers in e-commerce transactions. In Indonesia, for example, Act No.11, the Law of Information and Electronic Transactions, regarding electronic information and transactions, has been the law since 2008. Substantively, since the law has been implemented, it regulates whether electronic and electronic documents or printing are valid legal proof. Merchants have the responsibility that all data and documents which have been provided through an electronic information network are complete and correct, and that the accuracy and reliability can be trusted. This is meant to make the merchant able to supply a clear picture about legal subjects related to merchant identity, status, kind of business, and competence of the merchant in this business, whether a producer, provider, mediator or caretaker (Barkatullah, 2016). However, the Law of Information and Electronic Transactions does not discuss in detail regulation of self-regulation, legal security protection, and consumers' personal data.

3.2. Urgency of Merchant Self-Regulation to Guarantee Consumers' Rights in E-Commerce Transactions

Merchant self-regulation in e-commerce transactions does much to provide legal protection for consumers by guaranteeing their rights when entering into transactions on merchants' websites. Self-regulation cannot work by itself though. It requires the intervention of the country that issues regulations and information about merchants with whom transactions can be made. Consumers need to be careful to choose merchants who provide them with protection.

To make self-regulation run smoothly, the quality of the self-regulator must be guaranteed; this is very important for the actual implementation of self-regulation. Merchants must be very good in a regulated industry; they must have a broad understanding of the industry and relationships with other related industries. A self-regulator must be objective and work quite independently in its operations. In addition, merchants must be motivated to regulate and be creative in handling complicated situations in the industry (Zhao, 2005).

The regulators involved in the regulation process determine its success. There are some kinds of self-regulators that are created to handle different aspects of regulations, as well as to act as checks and balances for one another. Successful self-regulation industries do this by using

facilities from the state's regulations (Zhao, 2005). ThesState strengthens the credibility of self-regulation and increases fulfillment of the regulations by providing legal protection for consumers based on the merchant's strong convictions.

The merchant's good faith plays a big role in increasing consumers' trust in e-commerce transactions between countries. Merchants who can provide legal protection are needed to participate and support e-commerce transactions across countries. With self-regulation, the way transactions are conducted, safety systems, payment, shipping of goods, and resolution of disputes will be performed better. These are all done to increase consumer trust, and merchants will gain an advantage by increasing the number of consumers who do business on their websites.

Self-regulation has many advantages similar to what has been implemented in the United States. This is not a new concept in the Internet. Many online businesses like the FTC, OECD Guidelines, and ECGG have been developed through this process and become a standard in addition to government regulation (Alboukrek, 2003) The flexibility of self-regulation makes it possible for the industry to respond quickly to changes in technology and use new technologies to overcome digital problems (Zhao, 2005)

To provide legal protection to consumers, merchants must be concerned about a number of aspects. They include: (1) giving true, clear, and honest information to consumers related to products offered; (2) protection for consumers from all other merchants who offer products using unjust or misleading ways; (3) protection for obtaining goods according to what has been promised or offered; (4) protection for consumers to receive compensation or a refund as a result of unsuitable products that are not as promised; (5) protection for getting a suitable product based on what has been offered or promised; if the contract contains a clause that the merchant is free from responsibilities, then it must be clear and visible; (6) and merchants are obliged to pay special attention in promotions or ads and marketing to children, old people, or others who cannot completely understand the information given (Ramli, 2002).

The Electronic Commerce and Consumer Protection Group (ECCPG) gives guidance to merchants involved in e-commerce transactions across countries. They are (Alboukrek, 2003):

(1) Merchants must be fully open about their business and goods and services provided, as well as the requirements and conditions of transactions. ECCPG Guidelines determine openness. This includes vendor contact information (name, address,

telephone number, and e-mail address), correct pictures of goods and service, and other additional costs related to transactions (such as shipping, consumer service, and support information, and guarantee information).

(2) Merchants must establish a clear policy about cancellation, returned goods that have been bought by consumers, and giving refunds not required by ECCPG guidelines. However, this requires a letter with a statement of freedom from claims, where the level and scope of claims should be put on the website.

(3) For merchants to do business in accordance with fair business cases, ECCPG guidelines suggest the merchant "not to represent the content of the transaction or any cases to deceive, mislead, or be dishonest." This guideline also requests that merchants take reasonable steps to save consumers' transaction information. This comprises use of portal password protection, encryption, or similar technology. In addition, merchants must adopt a privacy policy which is suitable based on industry standards and legal requirements.

(4) Merchants must use a fair process in resolving disputes and finding a solution. ECCPG guidelines implement mechanisms for solving consumers' complaints. Merchants must decide their own internal mechanism and "participate in a program of solving disputes using an independent and reputed third party."

Security technology can secure Internet communication routes, but it does not protect consumers from people with whom they choose to conduct e-commerce transactions. Websites should use extra caution to provide system security. It is important to protect consumer information, maintain a secure server, and provide personal software and passwords (Dudeja, 2002).

In running a business, a merchant engages in activities based on the merchant's and public's needs, importance, and principles that must be fulfilled by merchants as well as consumers (Ramli, 2002). They include the following: the principles of balancing, where in marketing strategies, merchants are not always profit-oriented, by ignoring principles of right and honest business without paying attention to the position of consumers as product users; and principles of safety and security, in which every consumer has the right to their safety and security when using goods offered by merchants.

Responsibility for information. Merchants must give sufficient and clear information that is important to consumers in choosing goods. According to Beales (1981), the general standard for information that must be given to consumers includes price, quality, and other information that can help consumers decide what to buy according to their needs and the quality of goods. This can help merchants implement a form or standard of products offered to consumers. According to the principle of caveat, a vendor has an important role when the merchant must be able to give consumers information about unsafe products. Therefore, merchants must be careful in releasing products to the industry. The most important thing is that information must be free from data manipulation.

According to legal protection for consumers that is "creating a legal protection system for consumers which contains legal certainty and information openness as access to obtain information," there are three different parts to information responsibilities in Internet transactions.

Responsibility for information in Internet advertisements. The responsibility for information in advertisements relates to when products are offered in moving or still forms by a merchant on the Internet, the offering must contain information that does not create a misinterpretation about the condition of the goods. The responsibility for providing full information about a product refers to some general principles in the advertisement code of ethics (Nasution et al., 1994) as follows: (1) **a**n advertisement must be honest, responsible, and not conflict with valid legal stipulations; (2) an advertisement may not insult or humiliate status, religion, ethics, customs, culture, ethnicity, or group; and (3) aAn advertisement must be inspired by healthy competition principles.

Responsibility for electronic contract information. Responsibility for electronic contract information means merchants are responsible for providing information to consumers at a certain stage of the transaction which reflects the rights and responsibilities of each party. Very important information in contracts concerns problems of when and where a contract is formed and when a contract is legally valid, bound parties, related to consumers of any country, or any valid principle.

Certainty about whether an electronic contract must be closed and signed is not required to create a contract. In Common Law and the European Continental legal system, including Indonesia, unwritten stipulations are also binding in the same way as written stipulations.

However, special stipulations require certain formalities of a contract. For example, the statute of frauds (Badrulzaman et al., 2001) requires that land trade must be in written form and signed, so if one party does not carry out the terms of the contract, other parties cannot force it. This is connected to the need to prove whether a contract has been agreed upon.

Information about whether parties of a certain age can transact business is also important. This must be notified when contract is made. The problem of the capability of involved parties will be important in recognizing the responsibilities of the merchant.

In Indonesia, Section 1329 BW/KUH Civil law and Section 1330 determines the legal ability of those who are making an agreement. Section 1329 BW/KUH Civil law states that "every person is capable of making agreements if not legally stated as incapable." The determination of those who are incapable is stipulated in Section (Article 1330 KUH Civil law), which says: "those who are adults, guardians and women; in cases stipulated by law and in general all that legally prohibited to make certain contracts."

This cannot be broadly implemented because there is no institution that controls the parties who engage in e-commerce transactions, whether they are under age or not. Finally, merchants can take precautions by stating the minimum age to access transactions on the Internet. In e-commerce transaction cases such as on the website Smazon.com, the age of 18 is sufficient to legally perform transactions. If this is not stated though, the merchant usually limits its responsibility for not creating *canailles problems* involving various people.

As an example, Amazon.com's (2016) terms and conditions state that: "*If you use this site, you are responsible for maintaining confidentiality of your account and password and for restricting access to your computer, and you agree to accept responsibility for all activities that occur under your account or password. Amazon.com does sell products for children, but it sells them to adults, who can purchase with a credit card. If you are under 18, you may use Amazon.com only with involvement of a parent or guardian. Amazon.com and its affiliates reserve the right to refuse service; terminate accounts, remove or edit content, or cancel orders in their sole discretion*."

The merchant, in this case Amazon.com, places the responsibility on consumers who become members of the website to be used by those who have rights or the consumer's permission. The confirmation of age limit is also given by Amazon.com. It means that if an underage child is not accompanied by parents or caretakers, Amazon.com is not responsible for

improper use of credit cards or other mistakes.

Information for settling industrial disputes. One very important legal aspects in e-commerce transactions is information about the solution of industrial disputes. This problem often becomes complicated between merchants and consumers from different legal jurisdictions. One condition that must be explained in the Internet business is jurisdiction, as well as equal choice, and which court forum will investigate disputes. The discussion about jurisdiction becomes important because a geographic location in certain physical area is not appropriate if used to solve disputes in e-commerce transactions across countries.

Responsibility for safety. Electronic transaction networks must have the capability to guarantee the safety and security of the information stream. Every party involved in a transaction must believe in a strong infrastructure network. Of course, the merchant needs to prepare to control the safety of transactions.

An e-commerce transaction needs trust. Consumers will choose to conduct a transaction with a trusted merchant because of the money they are providing. Besides depending on trust, e-commerce and face-to-face transactions also depend on communication, which makes it important to be understood by consumers; for example, whether a message has been sent and received by and only to the correct address. For merchants, it is also important to keep the message content confidential and avoid trade competitors who can always mix up network data.

Protection of the safety of the computer system must absolutely be done since consumers want to be involved in a safe transaction. Safety in transactions consists of a system to save communications, safety of computers, physical safety, safety of individuals involved, administrative safety, and safety of media used (Purbo and Wahyudi, 2010). The safety provided is meant to avoid threats which may occur before they are realized, to minimize the possibility of the threats, and decrease the impact after the threat is realized. The safety system needs attention in relation to the type of e-commerce business and the form of payment mechanism system on the website.

4. CONCLUSION

Regulations to implement merchant self-regulation in e-commerce businesses to protect the privacy of data and consumers' private information on the Internet are very important for increasing consumers' trust in e-commerce transactions. Some countries have established various

standard regulations regarding how merchants collect, keep, use, and show private information they have collected from consumers. Merchants also actively develop and combine privacy systems to each code of practice website. There are different approaches to regulations between the United States and the European Union. The United States's opinion is that to gain consumer trust, merchants in e-commerce transactions must create a model for self-regulation. On the other hand, the European Union pays more attention to the role of the state through legal regulations that provide legal protection to e-commerce. In Indonesia, specific regulations to protect data or privacy have not been issued nor is self-regulation used in e-commerce transactions. The only existing regulations are general regulations included in the Law of Consumer Protection and Law of Information and Electronic Transaction.

Merchants' self-regulation in e-commerce transactions contributes much to giving legal protection to consumers by guaranteeing fulfillment of consumers' rights on merchant websites. Self-regulation cannot work by itself without the intervention of the state, which makes regulations and provides information for consumers about transaction safety. To make self-regulation run smoothly, something needs to be guaranteed; that is the quality of the self-regulator, which is very important for the actual implementation of self-regulation. The merchant must be an expert in the regulated industry. They must have a broad understanding of the industry and its relationship with other related industries. The self-regulator must be objective and work quite independently. In addition, the merchant must be motivated to regulate and be creative in handling complicated situations in the industry. Transactions in e-commerce demand that merchants understand and implement the concept of responsibility to increase consumers' responsibility and the state of the system of e-commerce transactions. To understand the concept of responsibility of the merchant in problems faced by consumers, their responsibility is divided into two parts: responsibility for information and responsibility for safety.

The goal of this study has been to find an effective model for implementing self-regulation by marrying the existing system in the United States, which emphasizes the awareness of business actors, and the European Union system, which emphasizes state intervention in the form of legislation. The self-regulation model cannot operate on its own without intervention from the state, which provides the arrangement and information for the consumer. Business actor awareness is also very important in providing protection, security, and fulfillment of consumer rights in performing e-commerce transactions.

REFERENCES

Alboukrek, K., 2003. Adapting to a new world of e-commerce: The need for uniform consumer protection in the international electronic marketplace. George Washington International Law Research 35, 425–460.

Andrews, R., 2005. Electronic commerce: Lessons learned from the European legal model. Intellectual Property Law Bulletin 9, 81-96.

Amazon.com. 2017. Reach hundreds of millions of customers. Available at: www.amazon.com/b/ref=nav_cs_sell?_encoding=UTF8&ld=AZUSSOA-sell&node=12766669011.

Badrulzaman, M.D., 2001. Union Law Compilation (Kompilasi Hukum Perikatan). PT. Citra Aditya Bakti, Bandung.

Barkatullah, A.H., 2012. Telematics law (Hukum telematika). P, 3AI Unlam, Banjarmain.

Barkatullah, A.H., 2016. Legal harmonization as legal protection by the state for stakeholders in International electronic transaction (Harmonisasi hukum sebagai perlindungan hukum oleh negara bagi para pihak dalam transasi elektronik internasiona). Jurnal Hukum Ius Quia Iustum. 1, 1–22.

Beales, H., Craswell R., Salop, S., 1981. The efficient regulation of consumer information. Journal of Law and Economics 24, 491–539.

Clinton White House, 2000. Initiatives: Al Gore, Vice President of the United States. Archives, U.S. Government, Washington, DC. Available at: clintonwhitehouse2.archives.gov/WH/EOP/OVP/initiatives_bottom.html.

Council of the European Communities. 1999. Proposal for a council regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. European Commission, Brussels, Belgium. Available at: eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51999PC0348&from=EN.

Dickie, J., 2000. Internet and Electronic Commerce Law in the European Union. Hart Publishing, Oxford.

Dudeja, V., 2002. Cyber Crimes and Law. Commonwealth Publishers, New Delhi.

Ferrera, G.R., 2001. Cyber Law Text and Cases. South-Western Cengage Learning, Boston.

Ferrettee, C.P., 2000. E-commerce and International political economics: The legal and political ramifications of the Internet on world economies. ILSA Journal of International and Comparative Law, 7, 15–37.

Ivascanu, D., 2010. Legal issues in electronic commerce in the western hemisphere. Arizona Journal of International Comparative Law, 17, 219-221.

Latifulhayat, A., 2002. Personal data protection in e-commerce trade (Perlindungan data pribadi dalam perdagangan secara elektronik). Jurnal Hukum Bisnis 18, March.

Makarim, E., 2003. Telematics Law Compilation (Kompilasi Hukum Telematika). PT Raja Grafindo Persada, Jakarta.

Nasution, A.Z., 1994. Report of legal aspects studies: Legal aspects and business ethics

advertising in Indonesia (Laporan tim pengkajian hukum tentang aspek hukum dan etika bisnis periklanan Di Indonesia). BPHN, Jakarta.

Pethia, R., Crocker, S., Fraser, B., 1991. Guidelines for the secure operation of the Internet. RFC 1281, Network Working Group, March 7. November: Available at: www.ietf.org/rfc/rfc1281.txt.

Purbo, O.W., Wahyudi, A.A., 2010. To Know E-Commerce (Mengenal E-Commerce). Elex Media Komputindo, Jakarta.

Ramli, A.M., 2002. Legal protection for consumers in e-commerce transactions (Perlindungan hukum terhadap konsumen dalam transaksi e-commerce). Jurnal Hukum Bisnis 18, March, 51-61.

Sharma, S., 2013. Encyclopedia of Cyber Laws and Crime. Anmol Publications, New Delhi.

Shofie, Y., 2013. Consumer Protection and Legal Instruments (Perlindungan Konsumen Dan Instrumen-instrumen Hukumnya). PT. Citra Aditya Bakti, Bandung.

Smedinghoff, T.J., 2010. Online Law: The Spa's Legal Guide to Doing Business on the Internet. Addison-Wesley Developers Press, New York.

Soekanto, S., Mamudji, S., 2014. Normative Law Research (Penelitian Hukum Normatif). Rajawali Press, Jakarta.

Sunggono, B., 2007. Law Research Methods (Metode Penelitian Hukum). Rajawali Press, Jakarta.

Zain, S., 2000. Regulation of e-commerce by contract: Is it fair to consumers? University of West Los Angeles Law Review 31, 163–186.

Zhao, Y., 2005. Dispute Resolution in Electronic Commerce. Martinus-Nijhoff, Leiden/Boston.

HIGHLIGHTS

- Consumers are subject to greater risks in e-commerce transactions.
- Consumer security and legal protection are necessary for e-commerce growth.
- A combination of self-regulation and legislation may be the best model.
- This assertion is evaluated through a cross-country study.
- The countries include the United States, the European Union, and Indonesia.