Shi, Peilin; Winter, Jenifer Sunrise; Zhang, Bin

Conference Paper

Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?

23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Shi, Peilin; Winter, Jenifer Sunrise; Zhang, Bin (2021) : Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?, 23rd Biennial Conference of the International Telecommunications Society (ITS): "Digital societies and industrial transformations: Policies, markets, and technologies in a post-Covid world", Online Conference / Gothenburg, Sweden, 21st-23rd June, 2021, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/238053

Governance of Privacy Protection: How Laws Will Be Adopted to Address New Technologies?

PEILIN SHI[1], JENIFER SUNRISE WINTER[2], AND BIN ZHANG[3]
[1.]Beijing University of Posts and Telecommunications,Beijing 100876, China
[2.]University of Hawaii,Honolulu HI 96822, U.S.A
[3.]Beijing University of Posts and Telecommunications,Beijing 100876, China
Corresponding author: Jenifer Sunrise Winter(jenifer.winter@gmail.com)

Abstract

In accordance with UNCTAD data, out of 194 countries in the world, 132 countries have enacted laws to protect data and privacy. Among them, most of the laws were issued at the beginning of the 21st century. With the continuous development of digital technology, especially the widespread application of big data technology, existing legislation has been unable to deal with the privacy protection risks brought by new technologies. In recent years, Japan, South Korea, and other countries have begun to revise or expand the definition of personal information protection boundaries and content in laws and regulations to protect the personal information of their citizens in response to the development of new technologies. In early 2020, the COVID-19 epidemic suddenly broke out and quickly swept the world, posing unprecedented challenges to healthcare systems, lifestyles, economic development and social stability in countries around the world. Digital technologies and data applications have played an important role in COVID-19 detection and control, but their characteristics have also raised concerns about the security of personal data and privacy. How the law will be adjusted (or has been adjusted) to deal with new technology will be a challenge.This paper selects the countries (EU, the United States, Japan, South Korea, China) that have modified laws and regulations related to data security and privacy protection in recent years as research objects, analyzes their existing privacy protection laws and regulations governance framework, and then analyzes the privacy risks faced to the new technology. In particular, privacy regulations and compliance guidelines for the application of facial recognition, location tracking and distance learning technology during the COVID-19 epidemic. Then, the governance experience in dealing with the relationship between digital technology progress, personal information protection and public health in the special period was summarized. Finally, it summarizes the future development direction of privacy protection governance from the legal level.

KEY WORDS: Privacy Protection, New Technologies, Governance, COVID-19 epidemic

1. Background

In the era of big data, data has a profound impact on the economic development, social order, national governance, and people's lives of all countries. Driven by technologies such as cloud computing, Internet of Things, mobile internet, and artificial intelligence, the value of data has continued to increase, and the digital economy has achieved rapid development. Big data technology has promoted increasingly diversified data subjects and data application scenarios, and the fields involved in data security have become increasingly extensive (Sun et al., 2020). For individuals, big data technology is frequently applied in various life scenarios. Users have a weak awareness of the right to self-determination of personal information, ignoring data collection and open sharing capabilities. Big data aggregation analysis makes it easier to obtain user portraits, which greatly increases the possibility of personal data breaching risks. In recent years, a series of data breaches have made people realize the importance of personal information protection in the Internet age(Verizon,2020). The sudden outbreak of COVID-19 has posed unprecedented challenges to global healthcare systems and the way society operates. Legislators and regulators have reminded the public to pay attention to data security and privacy protection in the event of a public health emergency(Jin&Zhang,2020). Digital technology and data applications can play an important role in the detection and prevention of the COVID-19 epidemic, but its characteristics have also raised concerns about the protection of personal data and privacy security.

1.1 Methodology

This paper is a summary of existing public sources and explores the future direction of privacy protection governance,which rely primarily on publicly available literature sources. These resources include online resources such as public documents, government reports, general and specialized newspapers and periodicals, academic research papers, academic and business literature, company news, websites, blogs and databases .

1.2 Organization

The paper, selecting countries that have amended data security and privacy protection related laws and regulations in recent years as the research object (the European Union, the United States, Japan, South Korea, and China), analyzes their existing privacy protection laws and regulations governance framework and what laws and regulations will be adjusted (or adjusted) to respond to the development of new technologies . Then, analyze the privacy risks faced by new technologies, in particular, privacy regulations and compliance guidelines for the application of technologies such as face recognition and location tracking in countries during the COVID-19 epidemic. From the perspective of system design, the new privacy regulations and compliance guidelines issued by various countries during the new epidemic period were sorted out, sum up the governance experience in dealing with the relationship between digital technology progress, personal information protection and public health in a special period. Finally, the paper summarizes the future direction of privacy protection governance at the legal levels.

2 . Privacy protection laws

The term "privacy" is most commonly used in the U.S. laws, regulations and policies related to the handling of personal information, while it is often referred to as "data protection" in other countries. In general, there is no uniform definition of privacy, and the meaning of privacy evolves over time(Solove,2008;Acquisti et.al,2015;Igo,2018). This paper continues the theory that privacy and personal information/data protection have the same meaning as previously mentioned. In the following chapter, the paper selects the countries that have amended the relevant laws on privacy protection in recent years as the research objects, and analyzes their existing privacy protection laws and regulations governance framework.

2.1 European Union

Since the 1970s, European countries have introduced comprehensive data protection laws. Although these national laws have some common features, differences in privacy protection standards between different countries occasionally impede the free flow of information between European countries (Murray, 1997). The EU has therefore attempted to harmonize its various national privacy laws by adopting an EU-wide privacy protection regulation. In 1990 the European Commission submitted a draft, and the Directive 95/46/EC on the protection of individuals with regard to the processing of Personal data and on the Free Movement of such data was formally promulgated in 1995. Developments in technology and globalization have changed the way that data is collected, accessed and applied, and the European Commission believes that EU law should keep pace with these developments(EC, 2012). To achieve these objectives, the EU enacted and adopted the General Data Protection Regulation (GDPR), which replaces Directive 95/46/EC and came into force on 25 May 2018. GDPR is widely regarded as the EU's strictest ever online data regulation and the biggest overhaul of data protection. The EU has always been committed to building an integrated governance mechanism by combining the legal framework with organizational system of cyber security. From the perspective of "EU - member States - civil society", the coordinated participation of various institutions and countries has distinct community characteristics (Song, 2017). After GDPR officially came into effect, in order to effectively implement GDPR, the European Parliament introduced relevant laws, such as Cybersecurity Law, Framework Regulations on the Free Flow of Non-personal Data, electronic Privacy Regulations and etc.. The European Data Protection Board has issued a guideline to Personal Data Protection in Connected Vehicles, a Guideline to Proportional Principles of Personal Data Protection, a Guideline to on processing of personal data through video devices, and a Guideline to Using Data Protection by Design and by Default. EU member states have also issued supporting documents. For example, the UK has issued guidelines on processing special category data, and Ireland has issued practical Guideline on the Notification of Personal Data Breaches under GDPR.

In terms of setting up privacy institutions, the EU mainly plays its role in privacy protection through the European Parliament, the European Data Protection Supervisor and the European Data Protection Commission. During the current legislative term, the European Parliament has almost completely overhauled the European Union's personal data protection rules. Having ensured that

EU protection rules are properly implemented, the role of parliament is now likely to shift more towards monitoring legislation (EP n.d.). The European Data Protection Supervisor is an independent monitoring body that ensures that EU institutions and organizations meet their Data Protection obligations. The main responsibilities of European Data Protection Supervisor are supervision, consultation and co-operation. The European Data Protection Supervisor was established in the Regulation on processing of personal data by the Union institutions and bodies (EDPS n.d.).European Data Protection Board is set up by GDPR, which replaced the WP29 working group in Directive 95/46/EC. The EDPB is an independent legal authorities with an independent secretariat, which brings together representatives of the national data protection authorities, the European Data Protection Supervisor to resolve disputes between national data regulators and provide guidance on the content of the GDPR and data protection related enforcement directives(EDPB n.d.).

2.2 United Sates

Unlike uniform legislation in the EU, the United States has not yet enacted a federal personal information protection bill that applies to all citizens nationwide and across the industries. The United States personal information protection law is relatively decentralized, fragmented, sectoral, industrial characteristics (Wang Y., 2020). The Gramm-Leach-Bliley Act (GLBA,1999) was passed by Congress on 12 November 1999. The law applies only to financial institutions which are engaged in banking, insurance, stock and bond, financial advisory and investment, and imposes detailed requirements on how financial institutions handle nonpublic personal information. Financial institutions must allow users to opt out if they do not want nonpublic personal information to be shared. Financial institutions should clarify user privacy policies and ensure the security of nonpublic personal information through security management, technical protection and other instruments. The Health Insurance Portability and Accountability Act (HIPAA n.d.) is a U.S. healthcare law that aims to clarify the regulatory requirements for the use, disclosure, safety protection, and emergency response of protected health information.The Family Education Rights and Privacy Act of 1974 (FERPA,1974) is a federal privacy law relating to educational information designed to protect educational information collected by educational institutions. It gives parents and eligible students under the age of 18 the right to control the disclosure of educational records, the right to view or modify educational records, and the right to question the accuracy of educational records.The Securities Act of 1933 is federal legislation to protect financial consumers. Companies are not only required to take control measures to prevent data leakage, but also required to regularly publish corporate information (SA,1933). In the explanatory guidance issued in February 2018, the Securities and Exchange Commission pointed out that companies may be required to disclose data breaches and other cyber incidents in their filing documents, and such incidents were discussed as part of the necessary disclosure categories (SEC,2018). The Children's Online Privacy Protection Act (COPPA, 1998), which took effect in 2000, regulates the collection and use of children's information online. COPPA requires websites and apps to obtain valid parental consent before accessing personal information of children under the age of 13, and to ensure the security, confidentiality and integrity of the child's personal information. The Federal Trade Commission Act, originally enacted in 1914, prevents unfair means of competition and unfair or deceptive acts that may affect commercial activities. It is also

one of the most important laws relating to data privacy and security. The Federal Trade Commission has used its powers under the Federal Trade Commission Act to become a privacy protection authority, effectively filling in the gaps left by the federal regulations(Solove& Hartzog, 2014).FTC uses its extensive powers to protect consumer privacy rights by restricting "unfair or deceptive trade practices". Different from federal law, the FTC is not confined to a specific area of the economy. The FTC's powers are broader and apply to most organizations involving commercial activities (Karapetyan,2018). The FTC applies a variety of regulatory tools to protect consumer privacy and personal information, mainly through enforcement to stop violations and requiring companies to take steps to correct violations. So far, the FTC has taken hundreds of enforcement actions accusing companies of "unfair or deceptive trade practices" in privacy protection such as on July 24 2019, the FTC announced that it had reached a $5 billion settlement with Facebook (FTC,2020a).

The US federal government has enacted a series of privacy protection laws in the areas of finance, education, telecommunications, health and children's information protection, but the legislation has not been unified. However, there is a growing trend for states to enact privacy laws. According to the National Conference of State Legislatures, Data Breach Notification Acts(NCSL,2021) has been enacted in all regions of the United States that requires private entities or government agencies to notify individuals who have been impacted by security breaches that may compromise their personally identifiable information.The California Consumer Privacy Act of 2018 (CCPA) was passed in 2018 and went into effect on January 1, 2020. The California Consumer Privacy Act is similar to GDPR in which provides comprehensive protection for personal information. The CCPA is designed to give consumers control over their personal information to protect their privacy rights. It also systematically clarifies the rules for enterprises to collect, use and transfer consumers' personal information.

2.3 Japan

Japan's privacy governance is a hybrid of European Union and the United States privacy governance. Prior to 2017, Japan's privacy regime lacked a strong central authority for privacy protection. Privacy protection depended on self-regulation to a great extent. In that sense, Japan's privacy regime is similar to that of the United States. However, the long-term development trend of Japan's privacy system is different from that of the United States, which is getting closer and closer to European countries. Japan's privacy system has stepped forward towards a comprehensive privacy system (Kushida et.al,2016).

In 2003, Japan passed the Personal Information Protection Act, a fundamental law on data protection. The Basic Law on Cyber Security of Japan was adopted at the end of 2014, which focuses on the deployment of cyber security strategies and the provision of basic cyber security policies. It also proposes to set up a "cyber security strategy headquarters" to unify and coordinate cyber security policies, formulate cyber security strategies and promote their implementation(Song&Jiang,2017). Japan's Personal Information Protection Act was amended extensively in 2015 and took effect in 2017. The amendment proposes a new definition of "personal information", establishes a personal information protection Committee, and sets conditions for the cross-border flow of personal data(Chai,2018). In June 2020, the Congress of Japan passed a bill to amend the Personal Information Protection Act. The proposed changes

include expanding the scope of the rights of data subjects, changing the methods of disclosure and retention of personal data, introducing mandatory rules for data breach, restricting the illegal or improper use of personal data, modifying the rules for transferring data to third parties outside Japan, increasing fines and etc.(Tanaka&Kitayama ,2020).

Personal Information Protection Act of 2017 transferred and centralized the supervision power in various fields which was originally subordinate to the chief ministers of provinces to the Personal Information Protection Commission, thus Japan tended to establish an integrated supervision system for the protection of personal information. Japan's Personal Information Protection Commission is the highest body to ensure the protection of personal information. In addition to formulating and supervising laws based on the Personal Information Protection Act and the Number Law, the daily work of the Personal Information Protection Commission also includes evaluating the personal information protection of administrative organizations, making preparations for the cross-border flow of personal data, conducting strategic dialogues with relevant international organizations; and publicity campaigns to raise awareness of privacy protection(PIPC, 2020).

2.4 South Korea

Korea's data privacy system is a hybrid system between the European Union's comprehensive data privacy legislation model and the United States' departmental legislation approach (Ko et.al, 2017). In 2011, Korea passed and implemented the Personal Information Protection Act which is the basic Law of Korea on the Protection of Personal Privacy, and issued the enforcement Order and the Enforcement Rules of the Personal Information Protection Act in parallel with the implementation of the Personal Information Protection Act. The Personal Information Protection Act makes clear provisions on the disclosure and use of personal information, and constructs a complete system concerning about preventing the disclosure of personal information beforehand, protecting personal information in the event and relieving afterwards. In accordance with PIPA, the Personal Information Protection Commission directly under the jurisdiction of the President and the Personal Information Dispute Mediation Committees were set up. The personal information impact assessment system, the personal information disclosure notice and complaint system were introduced. The national certification system for personal information and the personal information group litigation system were also established (Chi,2016). Act on Promotion of Information and Communications Network Utilization and Information Protection (IC Network Act) applies to data privacy issues involving Information and communication service providers and therefore covers a large proportion of network activity(KCC,2016). The IC Network Act has a lot in common with PIPA in terms of the statutory structure. The Credit Information Use and Protection Act is a specialized statute that is applicable to personal credit information, which aims to properly protect personal privacy from abuse of credit information(KCC,2017). In terms of new technologies and new services, the Cloud Computing Development and User Protection Act enacted in March 2015 which requires cloud service providers to timely inform users of infringement accidents, user information disclosure and service interruption(Yao,2017).

In recent years, Korea has constantly updated its existing information protection laws. On January 9, 2020, the National Assembly of Korea passed the amendment of the Three Data Acts, namely the Personal Information Protection Act, the Credit Information Use and Protection Act

and Act on Promotion of Information and Communications Network Utilization and Information Protection in order to expand the scope of personal information collection and utilization by individuals and enterprises, and to develop the big data industry. At the heart of the Korea's three data laws is the Personal Information Protection Act. The main content of the amendment to the Personal Information Protection Act is that the pseudonymized information that has been processed and cannot be identified by specific individuals can be used for statistical and research purposes without their consent. In addition, the relevant provisions of personal information protection will be unified and standardized by the Personal Information Protection Act(NAON, 2020).The main content of the amendments to the Credit Information Use and Protection Act is to use or provide pseudonymized information without the consent of the credit information subject for the purpose of formulating commercial statistics, research, and preservation of public welfare records(YHA,2020). In July 2020, according to the latest amendment of the Personal Information Protection Act, Korea plans to issue Enforcement Decree of the Personal Information Protection Act, focusing on details of sensitive personal information, the duties of regulators and the amount of administrative fines(FSC, 2020).

Korea established a complex administrative enforcement structure.Taking PIPA as an example, before the amendment, matters related to the personal information protection were handled by the Personal Information Protection Commission (PIPC) , The ministry of Interior and Safety, The Korea Internet Security Agency, The Personal Information Dispute Mediation Committees, and The Korea Communications Commission(Greenleaf&Park, 2014). The PIPA of 2020 has unified the supervisory authority related to personal information protection into the PIPC in order to give the PIPC greater powers, including the transformation of the PIPC into a central administrative agency(Eun,2020). Matters concerning the establishment or execution of policies, systems or plans relating to personal information protection are transferred to the PIPC (PIPA, 2020). The Korean Internet and Security Agency (KISA n.d.) performs work entrusted by PIPC, including but not limited to receiving reports of personal information breach and collecting relevant materials from personal information controllers in the case of reporting violations of PIPA.

2.5 China

Influenced by the European Union's General Data Protection Regulations, which came into effect in 2018, privacy protection has attracted great attention from governments and the public, and many countries and regions have gradually strengthened legal and regulatory measures for personal information protection. How to protect personal information and balance the interests of all parties in data governance has become a challenge faced by modern society and a global legal issue. Understanding the global legislative trends is of great significance in guiding Chinese citizens' sense of rights, regulating government and social behaviors, and balancing the interests of all parties. As a major digital economy, China is also actively establishing and improving legislation on personal information protection. At present, China has passed a number of laws, regulations and rules relating to cybersecurity and personal information protection, such as criminal law of the People's Republic of China ,civil code of the People's Republic of China, general rules of the civil law of the People's Republic of China, Law of the People's Republic of China on the Protection of Consumer Rights and Interests, Cybersecurity Law of the People's Republic China, and so on. Different from most countries around the world, China has not passed

a unified law of personal information protection. However, uniform legislation is necessary (Zhou,2018). In the field of personal information protection, China adopts the model of decentralized legislation(Chen,2019). The legislative system consists of laws, regulations, rules and all kinds of normative documents, forming a multi-level, multi-field, decentralized and complex legal system of personal information protection.

The typical legal models of international personal information and privacy protection are represented by the European Union and the United States. The European Union adopts the unified legislative model to manage the whole life cycle of personal information through the formulation of comprehensive personal information protection laws. The United States adopts the mode of the combination of decentralized legislation and industry self-discipline to carry out fragmented legislation on personal privacy protection. At the present stage, all countries are successively issuing or updating the Personal Information Protection Law to meet the increasingly severe needs of privacy disclosure governance. A larger majority would prefer the EU model, while a smaller number of countries would prefer a combination of the European Union and the United States. In addition, various countries have set up special privacy management agencies according to relevant laws. The main objectives are to formulate and promulgate supporting rules and regulations of privacy laws, carry out impact assessments on information protection, conduct strategic dialogues with relevant international organizations, and publicize activities to raise national awareness of privacy protection.

3. How laws will be adopted to the privacy risks of new technology?

With the continuous development of new technologies such as artificial intelligence, new challenges have emerged in personal information/privacy protection. The number of network attack points increases, and once security problems occur, it will bring more disastrous consequences. While AI can protect citizens' safety and allow them to enjoy their basic rights, citizens are also concerned that AI may produce unexpected effects or even be used for malicious purposes (EC, 2020). Developers of AI are already bound by rules on consumer protection, product safety and liability, but there is still a need to study whether existing legislation can address AI risks and whether it needs to be changed or new legislation is needed. In 2019, High-level Expert Group On Artificial Intelligence under the European Commission published guidelines on Trusted Artificial Intelligence, identifying requirements such as privacy and data governance. Given AI is evolving fast, the regulatory framework must make room to accommodate future developments. Regulatory frameworks should focus on risks to fundamental rights, including protection of personal data and non-discrimination (HLEGOAI, 2020).

Advances in artificial intelligence (AI) have brought innovation in all aspects of life. With the increase of data volume, sufficient data has been formed for many situations, which can be used to train the algorithm and enhance the performance of the learning model(Chen&Lin, 2014;Jordan& Mitchell, 2015).As deep learning algorithms become more complex, they can be used to correlate disparate data sources to enhance predictive analysis(Bates et al.,2014) In the health sector, data not protected by HIPAA can be combined with personal information from other sources, including healthcare providers and pharmaceutical companies, to create potential hazards such as

discriminatory analysis, manipulative marketing, and data breaches(Montgomery et al., 2018).

3.1 Contact Tracing Apps

At the beginning of 2020, the COVID-19 pandemic (COVID-19) suddenly broke out and rapidly spread across the globe, posing unprecedented challenges to healthcare systems, lifestyles, economic development and social stability in countries around the world. Digital technology and data applications can play an important role in the detection and prevention of COVID-19, but the nature of COVID-19 has also raised concerns about personal data protection and privacy security(Blasimme&Vayena, 2020; Budd et al,. 2020)

To track and control outbreaks, many countries have developed contact tracking apps. Location data is highly sensitive and can be used to identify the identity of a specific person or reflect the activities. In addition, once it is disclosed, illegally provided or abused, it may endanger personal and property safety which directly relates to the personal privacy interests and safety of personal data(Akinbi et.al, 2021).South Korea, Singapore, Israel and other countries have adopted location-based contact tracking apps in the early stages of the epidemic. In South Korea, government agencies have used surveillance footage, smart phone location data and credit card purchases to help track the recent movements of patients with COVID-19 and establish chains of transmission(Kharpal, 2020). Contact tracing may be a viable method for controlling COVID-19 transmission. But concerns about online security and privacy, and a lack of trust in government, are major obstacles to its implementation(Altmann et.al, 2020). Designers of emerging technologies should make it clear to the public, as well as to the institutions and companies that deploy their technologies, how they are designing devices to avoid damaging users' privacy(Hartzog&Richards, 2020).

Personal data protection regulators have developed specific guidelines for contact tracing apps to ensure that users are informed, data collection is limited to legal limits and data storage is secure. Statement on the processing of personal data in the context of the COVID-19 outbreak. European Data Protection Board recommends that public authorities should first seek to process location data anonymously to generate reports on the concentration of mobile devices in a particular location.When it is not possible to deal only with anonymous data, Member States may, in accordance with Article 15 of the E-Privacy Directive, take legislative measures to deal with non-anonymous location data (EDPB, 2020a).In April 2020, the EDPB(2020b) published guideline on how contact tracing apps should comply with the General Data Protection Regulation , in response to the potential risk that COVID-19 contact tracing apps may infringe on personal data. The EDPB recommends that applications should not collect irrelevant or unnecessary information. The implementation of contact tracing can follow a centralized or decentralized approach. Both should be considered viable options, provided adequate security measures are in place. But at the same time, it is suggested that decentralized solutions are more consistent with the principle of minimization. Also, applications should be made voluntary and disabled when they are no longer needed.The Information Commissioner's Office of UK (ICO) has set out a series of privacy concerns when individuals use contact tracing and location tracking technologies in COVID-19 in order to help the public avoid privacy risks(Denham, 2020). As with any new technology, the public needs to have confidence that tracking technology is being used in a fair and proportionate manner. Applications require a high level of transparency and governance,

and a focus on continued review of the data collected and used is necessary and proportionate.Therefore, the current EU privacy regulation measures for contact tracing technology are mainly the guidelines of GDPR, including application data collection minimization, anonymity, test review, risk assessment, overdue deletion, source code disclosure, other guarantee requirements and etc..

3.2 Distance learning technology

During the COVID-19 period, the regulation of the physical public sphere pushes the public to shift their life field from offline to online, making social life more dependent on the support of digital technology. The demand for online education and online office increase greatly, and the application of Internet access and digital technology will be further explored(Cucinotta et.al, 2021). The COVID-19 has transformed traditional classroom education into online learning on a global scale(Khalili, 2020). At the government work conference, Japanese Prime Minister Shinzo Abe proposed to make full use of IT technology to fight the epidemic, formulate strategies for the use of IT and big data technology in various fields, advocate the digitization of administrative procedures, and speed up the process of online education programs(NHK, 2020).At the same time, participants' concerns about security and privacy in online education directly affected their participation.Due to security concerns, participates may hesitate to use online tools in the absence of safeguards. In terms of online education, Student Privacy Policy Office under the administration of U.S. Department of Education has issued guidance on online education for students during the outbreak. SPPO(2020) emphasize the need for schools or educational institutions to strictly comply with the Family Education and Privacy Act (FERPA) when handling personally identifiable information (PII) in students' educational records during online education.At the same time, educational institutions should communicate their Privacy policies to students and parents in a way that is easy to read and understand, should not undercut the Privacy of students when take online classes at home, and should not profit from student data, according to the Privacy Technical Assistance Center's recommendations(PTAC, 2014).On April 9, 2020, the U.S. Federal Trade Commission (FTC) released guidance for the Children's Online Privacy Protection Act (COPPA) during COVID-19 for operators providing distance learning technology for online education during the epidemic. The guidance allows schools to authorize the collection of personal information from students under the age of 13 on behalf of parents, as long as the authorization meets the requirements for educational purposes and necessary notice(Schifferle, 2020).

Today, no matter in business meetings, school classes or academic discussions, ZOOM has become indispensable. COVID-19 has made Zoom, a remote video app that connects people to one another, increasingly popular. Because of its excellent stability, ZOOM has become the first choice of many competing products. In April 2020, Zoom suffered a series of privacy crises, including data hijacking, encryption, and data collection problems(Young, 2020), and students expressed concerns about the use of web-cams in online classes(Rajab &Soheib, 2021). The Dutch Ministry of Defense, considering the serious privacy risks posed by Zoom, has banned the use of the Zoom video conferencing service in the Ministry of Defense and has ordered that the Zoom app can not be installed on smart phones, tablets, laptops or PCs in the Ministry of Defense(Telecompaper, 2020). In response, the FTC asked Zoom to enforce the security standards

as advertised to ensure the privacy of users' communications (FTC,2020b). The European Union Agency For Cybersecurity has published the "Tips for selecting and using online communication tools". Security and privacy Settings for online communication tools are critical to effective operation, the document said, adding that online communication tools should support encrypted communications.The document states that security and privacy settings of online communication tools are critical to effective operation, and proposes that online communication tools should support encrypted communications (ENISA 2020). Many institutions have decided to ban Zoom, but have struggled to find a stable and reliable alternative. How to maintain normal online activity without being over-tracked has become an educational dilemma during the epidemic. Both Teams for Education(Christl, 2020) and ClassDojo (Manolev et.al, 2019) have privacy issues. The privacy issues of online communication tools need to be further explored.

3.3 Facial recognition

In addition to contact tracing apps, artificial intelligence technologies such as facial recognition, drones and thermal imaging cameras have also been widely used in the epidemic. These technologies can effectively reduce person-to-person contact, detect people with abnormal body temperature who may be infected, and supervise citizens to reduce their outside exposure (Sullivan, 2020; Braithwaite,2020). The GDPR specifies how to collect, store, and use facial recognition data. There are fewer restrictions in the U.S.. With the exception of Illinois and California, which have passed legislation regulating the commercial use of hot body temperature and facial information, most of these laws do not extend to the collection of hot facial data for non-commercial purposes.(Van N.M. et al., 2020) In response, the state of Washington passed the first regulation on Facial Recognition Technology in the United States, which will allow government departments to use facial recognition technology for public safety purposes. It will take effect in July 2021(WSL, 2020). Under strict restrictions, it would allow government law enforcement to use facial recognition technology for public safety purposes. In non-emergency situations, law enforcement agencies need permission before they can use facial recognition technology to investigate. It also requires government agencies to ensure that recognition software passes fairness and accuracy tests, and to regularly report to the public on the use of facial recognition technology.

4. Legal strategies faced to new technology

The European Union and the United States reserved policy space for emergency and exception clauses in the previous privacy related legislation, which ensured the consistency and stability of legislation. But since the United States does not have federal privacy Act as the GDPR, laws were put in place to fill the gap during the outbreak of COVID-19. At the European level, the European Union issued guidance documents in accordance with the GDPR to standardize and guide data and privacy protection during the epidemic.

In the United States, two privacy legislation bills were introduced in Congress during the epidemic, with the intention of promoting privacy legislation at the federal level.Influenced by the

liberal economic system, the path of data security and privacy protection in the United States mainly relies on industry supervision and enterprise self-discipline. The intensity of privacy legislation issued by various states for supervision are at multiple levels. On April 20, 2020, Republicans introduced the COVID-19 Consumer Data Protection Act (CCDPA) in Congress (Congress U.S. 2020a).On May 14, 2020, the Democratic Party proposed the Public Health Emergency Privacy Act (PHEPA) as a countermeasure (Congress U.S. 2020b). Both acts are interim rules for the collection, use and disclosure of emergency health data during epidemic. They aim to enhance the security of consumers' personal health information and data while effectively preventing and controlling COVID-19 through tracking technology, and ensure that the data is not used for non-public health purposes. Both are likely to form the basis for a comprehensive federal privacy bill (Yang&Chen, 2020).

Article 23 of the GDPR allows countries to restrict the rights of data subjects if necessary, so the EU issued a statement after the outbreak to remind member states that they could take urgent measures to help prevent and control the epidemic. Since the outbreak, data protection authorities of all 27 EU member states have published data protection guidelines for COVID-19 outbreaks (IAPP,2020). All guidelines are based on the GDPR. Thus, GDPR is the basis of data protection in EU countries. For European countries, the profound cultural tradition of privacy has long been integrated into the privacy protection laws such as GDPR. In the face of new technology, Europeans are relatively cautious at a strong sense of privacy. For example, even though the location information that companies share with governments has been anonymized, Patrick Breyer, member of the European Parliament, still expressed concerns about the potential possibilities for mass surveillance in the future(Perera, 2020). Thus, EU guidance documents often refer to the need to restore people's freedoms and end surveillance measures after public health emergencies.

As for the application of new technology, there are huge differences in acceptance and promotion scope among countries. South Korea, Japan and China are close to the European Union in terms of "legislative form", but there are still huge differences rooted in the cultural view of privacy. Guidance documents on new technologies were not frequently issued during the epidemic. China, Singapore and South Korea all developed contact tracing apps in the first quarter of 2020. Despite the lack of privacy protection, it has also been rapidly promoted (Utzerath J. et.al, 2020) China’s Alipay Health Code app performed the worst among the 21 apps evaluated in terms of data protection standards and public health benefits (Kolasa K. et.al, 2021) When the value of "health", which is more closely related to the public interest, conflicts with the value of "privacy", which is more concerned with the protection of private freedom, Asians are more inclined to focus on the public interest (Wang&Yan2020).

5. Conclusion: Prospect of Privacy Protection Governance

The governance of privacy protection mainly relies on legal means. In form, It is mainly divided into the unified legislation (the European Union) and the sector-specific legislation (the United States) and the combination of the two.Most countries make reference to the EU's General Data Protection Regulation and introduce or update their national privacy protection laws according to their own situations. A special privacy management agency will be established to assess the risk of privacy leakage in the context of technological development such as big data,

artificial intelligence, etc., formulate a regulatory framework, and regularly carry out publicity activities to raise national security awareness.

Unified legislation at the national level is the general trend of privacy protection.Even in the United States, technology is making it increasingly likely that a federal privacy law similar to the CCPA will emerge (Rayome, 2019).The sudden outbreak of COVID-19 provided a new opportunity for a federal uniform privacy bill. The governor of the US state of Virginia has signed the Consumer Data Protection Act, which will take effect in January 2023. Virginia became the second state, after California, to enact a basic privacy law.Privacy and data protection legislation is being stepped up in several US states, such as Colorado, Illinois, Massachusetts, New York, and Texas (IAPP, 2021).

Although at the EU level, the GDPR sets out uniform directives for member states, the GDPR leaves many aspects of the public interest base to individual member states. The reality is that the law creates inconsistencies and hinders joint processing.The COVID-19 experience offers lessons for national legislatures. It requires clear and uniform laws and the global collaborative research to deal with epidemics. (Becker et.al,2020) .In the era of artificial intelligence, the pattern and trend of international communication are more complex and diversified, and there is a contradiction between the "globalization" of artificial intelligence application and the "nationalization" of data privacy protection.Countries should strengthen cooperation and promote global governance of data privacy protection.

Reference

Acquisti, A., Brandimarte, L., and G. Loewenstein. (2015). Privacy and human behavior in the age of information. Science 347(6221):509-514. https://doi.org/10.1126/science.aaa1465

Akinbi, A. , Forshaw, M. , & V Blinkhorn. (2021). Contact tracing apps for the covid-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies. Health Information Science and Systems, 9(1), 1-15. https://doi.org/10.1007/s13755-021-00147-7

Altmann, S. , Milsom, L. , Zillessen, H. , Blasone, R. , Gerdon, F. , & Bach, R. , et al. (2020). Acceptability of app-based contact tracing for covid-19: cross-country survey study. JMIR mHealth and uHealth, 8(8).https://doi.org/10.2196/19857

Bates, D. W. , Saria, S. , Ohno-Machado, L. , Shah, A. , & Escobar, G. . (2014). Big data in health care: using analytics to identify and manage high-risk and high-cost patients. Health Aff, 33(7), 1123-1131.https://doi.org/10.1377/hlthaff.2014.0041

Becker, R., Thorogood, A., Ordish, J., and Beauvais, M. J. S. (2020). COVID-19 research: navigating the European general data protection regulation. J. Med. Internet Res. 22:e19799. https://doi.org/ 10.2196/19799

Blasimme, A. , & Vayena, E. . (2020). What's next for covid-19 apps? governance and oversight. Science, 370(6518), 760-762.https://doi.org/10.1126/science.abd9006

Braithwaite S..(2020). Italian police can now use drones to monitor people's movements, aviation authority says. Cnn.com. March 24,2020. Accessible at: https://edition.cnn.com/world/live-news/coronavirus-outbreak-03-24-20-intl-hnk/h_b5c13ce244635a6e5b945f6462b4a37

Budd, J. , Miller, B. S. , Manning, E. M. , Lampos, V. , & Mckendry, R. A. . (2020). Digital technologies in the public-health response to covid-19. Nature Medicine, 26(8), 1-10.https://doi.org/10.1038/s41591-020-1011-4\

Chai Y.(2018).Summary of Japan's personal information protection law.People's Court Daily,008

Chen S.,(2019). Research on the Legislation Concept and Mode of Personal Information Protection (Master's Dissertation, Lanzhou University). https://kns.cnki.net/KCMS/detail/detail.aspx?dbname=CMFD201902&filename=1019875080.nh

Chen, X.W., & Lin, X. (2014). Big data deep learning: Challenges and perspectives. IEEE Access, vol. 2, 514-525. https://doi.org/10.1109/ACCESS.2014.2325029.

Chi J., (2016). A comparative analysis of systems for protecting personal information in japan and korea. Journal of Intelligence. 35(12):,63-68. http://en.cnki.com.cn/Article_en/CJFDTotal-QBZZ201612013.htm

Christl, W. (2020). WolfieChristl'sTweet on Microsoft Teams for Education. Twitter.com. December 13,2020. Accessible at: https://twitter.com/WolfieChristl/status/1338165010967748608

Congress U.S. &(United States Congress).(2020a) S. 3663-COVID-19 consumer data protection act of 2020. Congress.gov. May 07,2020. Accessible at: https: / /www. congress. gov /116/bills /s3663/BILLS-116s3663is. pdf.

Congress U.S. &(United States Congress).(2020b). S. 3749-Public health emergency privacy act. Congress.gov. May 14,2020. Accessible at: https: //www. congress. gov /116/bills/s3749 /BILLS-116s3749is. pdf.

COPPA. &(The Children’s Online Privacy Protection Act).(1998). Accessible at: https://www.federalreserve.gov/boarddocs/supmanual/cch/coppa.pdf.

Cucinotta, C. E. , Martin, B. J. E. , Melvin Noé González, Raman, P. , Teif, V. B. , & Vlaming, H. . (2021). Strength is in engagement. EMBO reports, 22. https://doi.org/10.15252/embr.202152612

Denham E.(2020).Blog: Combatting COVID-19 through data: some considerations for privacy. ico.org.uk.April 17,2020. Accessible at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/04/combatting-covid-19-through-data-some-considerations-for-privacy

EC. &(European Commission).(2012). Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. ec.europa.eu. January 25,2012. Accessible at: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46.

EC, &(European Commission).(2020).WHITE PAPER On Artificial Intelligence -A European approach to excellence and trust. ec.europa.eu,February 19,2020. Accessible at: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

EDPB, &(European Data Protection Board).(2020a).Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. edpb.europa.eu, March 16,2020. Accessible at: https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

EDPB, &(European Data Protection Board).(2020b).Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. edpb.europa.eu, April 21,2020. Accessible at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

EDPB. &(European Data Protection Board). (no date).Who we are. Europa.eu. Accessible at: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en

EDPS. &(European Data Protection Supervisor).(no date). About. Europa.eu. Accessible at: https://edps.europa.eu/about-edps_en

ENISA, &(European Union Agency For Cybersecurity).(2020).Tips for selecting and using online communication tools. Enisa.europa.eu, April 27,2020. Accessible at: https://www.enisa.europa.eu/news/enisa-news/tips-for-selecting-and-using-online-communication-tools

EP. &(European Parliament).(no date). About Parliament. Europa.eu. Accessible at: https://www.europarl.europa.eu/about-parliament/en

Eun,L.S(2020), The Amendment of Personal Information Protection Act of Korea - Focusing on the Grounds for Processing Personal Data without Data Subject's Consent, Law paddy field house, Volume 24, Issue 3, 249-286

FERPA.&(Family educational and privacy rights).(1974).20 U.S. Code § 1232g - Family educational and privacy rights. Accessible at: https://www.law.cornell.edu/uscode/text /20/1232g.

FSC(2020). FSC Introduces Amendments to Enforcement Decree of Credit Information Act.March 30,2020. Accessible at: http://meng.fsc.go.kr/common/pdfjs/web/viewer.html?file=/upload/policy1/20200331101439_fc1016cf.pdf

FTC.&(Federal Trade Commission).(2020a).Privacy and Data Security Update 2019.Accessible at:https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

FTC. (2020b). FTC RequiresZoom to Enhance its Security Practices as Part of Settlement. Ftc.gov.November 9,2020. Accessible at: https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement

GLBA. &(Gramm-Leach-Bliley Act).(1999).PUBLIC LAW 106–102. govinfo.gov.November 12,1999. Accessible at: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/ PLAW-106publ102.pdf

Greenleaf, G. , & Park, W. I. . (2014). South korea's innovations in data privacy principles: asian comparisons. Computer Law & Security Review the International Journal of Technology Law & Practice, 30(5), 492-505.https://doi.org/10.1016/j.clsr.2014.07.011

Hartzog, W. , & Richards, N. M. . (2020).Privacy's constitutional moment and the limits of data protection. Social Science Electronic Publishing.https://doi.org/10.2139/ssrn.3441502

HIPAA.(no date).The HIPAA Privacy Rule.Accessible at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

HLEGOAI, &(High-level Expert Group On Artificial Intelligence).(2020). The Ethics Guidelines for Trustworthy Artificial Intelligence (AI).ec.europa.eu,June,2018. Accessible at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

IAPP. &(International Association of Privacy Professionals). (2020). DPA guidance on COVID-19.iapp.org. April 2020.Accessible at: https://iapp.org/resources/article/dpa-guidanceon-covid-19/.

IAPP. &(International Association of Privacy Professionals). (2021). US State Privacy

Legislation Tracker.iapp.org.May 26,2021. .Accessible at: https://iapp.org/resources/ article/us-state-privacy -legislation-tracker

Igo, S. E. (2018). The known citizen: A history of privacy in modern America. Cambridge, Ma.: Harvard University Press.

Jin S.&Zhang L.,(2020). Research on Personal Information Protection under Public Health Emergencies: On the Background of Novel Coronavirus Pneumonia Epidemic Situation. Information theory and practice. 43, 16-22.https://doi.org/CNKI:SUN:QBLL.0.2020-06-003

Jordan, M. I. , & Mitchell, T. M. . (2015). Machine learning: trends, perspectives, and prospects. Science, 349(6245), 255-260. DOI:10.1126/science.aaa8415

Limbu, Y. B., Wolf, M., & Lunsford, D. L. (2011). Consumers'perceptions of online ethics and its effects on satisfaction andloyalty.Journal of Research in Interactive Marketing,5(1),71–89. https://doi.org/10.1108/17505931111121534

Karapetyan A.(2018). Developing a Balance Privacy Framework. Southern California Review of Law and Social Justice, (27),197-283. https://gould.usc.edu/students/journals/rlsj/ issues/assets/docs/volume27/Summer2018/2.Karapetyan.pdf

KCC.&(Korea Communications Commission).(2016).ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.Article 1. klri.re.kr. March 22,2016. Accessible at: https://elaw.klri.re.kr/eng_service/law View.do?hseq=38422&lang=ENG

KCC. &(Korea Communications Commission).(2017).CREDIT INFORMATION USE AND PROTECTION ACT,.Article 1. klri.re.kr. November 28,2017. Accessible at: Article 1, https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=46276&type=part&key=23

Khalili, H. . (2020). Online interprofessional education during and post the covid-19 pandemic: a commentary. Journal of Interprofessional Care(3), 1-4. https://doi.org 10.1080/135618 20.2020.1792424

Kharpal A.(2020) Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. Cnbn.com. March 26, 2020.Accessible at: https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pande mic-privacy-concerns.html

KISA. &(Korea Internet&Security Agency).(no date). Internet Security. Accessible at: https://www.kisa.or.kr/eng/mainactivities/internetSecurity.jsp

Ko, H., Leitner, J., Kim, E., & Jeong, J. (2017). Structure and enforcement of data privacy law in South Korea. International Data Privacy Law.7,100-114,https://doi.org/10.1093/idpl/ipx004

Kolasa K, Mazzi F, Leszczuk-Czubkowska E, Zrubka Z, Péntek M. (2021). State of the Art in Adoption of Contact Tracing Apps and Recommendations Regarding Privacy Protection and Public Health: Systematic Review. JMIR Mhealth Uhealth 2021;9(6):e23250. https://doi.org/10.2196/23250

Kushida, K. E., Kasuya, Y., & Kawabata, E. (Eds.). (2016). Information Governance in Japan: Towards a New Comparative Paradigm. Stanford Silicon Valley New Japan Project.249-283 https://ssrn.com/abstract=3046663

Manolev J., Sullivan A. & Slee R. (2019) The datafication of discipline: ClassDojo, surveillance and a performative classroom culture, Learning, Media and Technology, 44:1, 36-51, https://doi.org/10.1080/17439884.2018.1558237

Montgomery, Chester, & Kopp. (2018). Health Wearables: Ensuring Fairness, Preventing

Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment. https://doi.org/10.5325/jinfopoli.8.2018.0034

Murray, P. (1997). The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard? Fordham International Law Journal, 21, 932-1018. https://heinonline.org/HOL/LandingPage?handle=hein.journals/frdint21&div=62&id=&page=

NAON(2020).South Korea's National Assembly Passes' Three Data Laws'. January 9,2020. Accessible at: http://www.naon.go.kr/content/html/2020/01/09/0ae208d6-7462-4761-bdbf-d1d6c6a4cfd5.html

NCSL. &(National Conference of State Legislation). (2021). ncsl.org. April 15,2021. Accessible at: https://www.ncsl.org/research/telecommunications-and-information-technology/security- breach-notification-laws.aspx

NHK. (2020). Novel coronavirus, prime minister‘s IT strategy. nhk.or.jp. April 22,2020. Accessible at: https://www3.nhk.or.jp/news/html/20200422/k10012401011000.html?utm_int=word_contents_list-items_001&word_result=IT%E3%83%BB%E3%83%8D%E3%83%83%E3%83%88

Perera D.(2020). Covid-19 pressures privacy as pandemic spreads globally. mlexmarketinsight.com. March 19, 2020. Accessible at: https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/cross-jurisdiction/covid-19-pressures-privacy-as-pandemic-spreads-globally.

PIPA.(2020) PERSONAL INFORMATION PROTECTION ACT, August 5,2020. Accessible at: https://www.pipc.go.kr/eng/user/lgp/law/lawDetail.do#none

PIPC,(2020). 2019 Annual Report of the Personal Information Protection Committee. ppc.go.jp. June,2020. Accessible at: http://www.ppc.go.jp/files/pdf/020612gaiyou.pdf.

PTAC, &(Privacy Technical Assistance Center). (2014). Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices. tech.ed.gov. February, 2014. Accessible at: https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

Rajab, M. H. , & Soheib, M. . (2021). Privacy concerns over the use of webcams in online medical education during the covid-19 pandemic. Cureus, 13(2). https://doi.org/10.7759/cureus.13536

Rayome, A. D. (2019). Will we see a federal privacy law in the US? TechRepublic. techrepublic.com. , March 8,2019. Accessible at: https://www.techrepublic.com/article/will-we-see-a-federal-privacy-lawin-the-us/

SA. &(Securities Act of 1933).(1933). 73d CONGRESS. SESS. I.CII. 38. MAY 27, 1933 . Accessible at: https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/48/STATUTE-48-Pg74.pdf .

Sang, S. K. . (2021). Motivators and concerns for real-time online classes: focused on the security and privacy issues. Interactive Learning Environments(1). https://doi.org/10.1080/10494820.2020.1863232

Schifferle L.W. (2020). COPPA Guidance for Ed Tech Companies and Schools during the Coronavirus. Ftc.gov. April 9, 2020. Accessible at: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus

SEC. &(Securities and Exchange Commission).(2018).83 FR 8166 - Commission Statement and Guidance on Public Company Cybersecurity Disclosures.February 26,2018.Accessible at:

https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf.

Solove, D. J. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Colum. L. Rev., 114, 583. https://heinonline.org/HOL/LandingPage?handle=hein.journals/clr114 &div=19&id=&page=

Song K., &Jiang X. (2017). A brief analysis of the evolution and mechanism of Japanese network security strategy. East China science and technology.07, 45–47. https://doi.org/CNKI:SUN:HDKJ.0.2017-07-015

Song W.L.(2017). Research on EU Cyber Security Governance, Doctoral dissertation, Foreign affairs college.

SPPO, &(Student Privacy Policy Office). (2020). FERPA & Coronavirus Disease 2019 (COVID-19) Frequently Asked Questions (FAQs).studentprivacy.ed.gov.March 2020. Accessible at: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPA%20and%20 Coronavirus%20Frequently%20Asked%20Questions_0.pdf.

Sullivan M.(2020).Updated: This AI camera detects people who may have COVID-19. Fastcompany.com. March 19, 2020. Accessible at: https://www.fastcompany.com/90479220/ this-ai-camera-detects-people-who-may-have-covid-19.

Sun, Z., Strang, K.D., Pambel, F., (2020). Privacy and security in the big data paradigm. Journal of Computer Information Systems 60, 146–155. https://doi.org/10.1080 /08874417.2017.1418631

Tanaka, H.&Kitayama N. ,(2020). Japan enacts Amendments to the Act on the Protection of Personal Information. Iapp.com. June 9,2020. Accessible at: https://iapp.org/ news/a/japan-enacts-the-act-on-the-protection-of-personal-information/

Telecompaper. (2020). Dutch defence ministry bans use of Zoom.telecompaper.com. April 17,2020. Accessible at: https://www.telecompaper.com/news/dutch-defence-ministry-bans-use-of-zoom--1335022

Utzerath J., Bird R., &Cheng G. (2020). Contact tracing apps in China, Hong Kong, Singapore and South Korea. lexology.com. April 24,2020. Accessible at: https://www.lexology.com /library/detail.aspx?g=99dca469-455d-4f7a-b025-00bf1d10ff6b

Van N.M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., Vattikonda, N.(2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. Journal of Law and the Biosciences 7, lsaa038. https://doi.org/10.1093/jlb/lsaa038

Verizon,(2020). 2020 data breach investigations report. Accessible at: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Wang R., Yan J. (2020).Decision-making balance between "privacy" and "public health".tisi.org. March 31,2020. Accessible at https://mlexmarketinsight.com/insights-center /editors-picks/Data-Protection-Privacy-and-Security/cross-jurisdiction/covid-19-pressures-privacy -as-pandemic-spreads-globally

Wang Y.(2020). Legal Adjustment of Network Privacy Policy and Personal Information Protection: American Practice and Its Implications. Global Law Review, 2020, 42(02), 149-161. http://www.globallawreview.org/Magazine/Show/71641

WSL. &(Washington State Legislature).(2020). SB 6280-Concerning the use of facial recognition services. March 20,2020 . Accessible at: http://lawfilesext.leg.wa.gov

/biennium/2019-20/Pdf/Bills /Session% 20Laws/Senate/6280-S.SL.pdf?q=20200702235951.

Yang C.,Chen T.(2020). Epidemic response and data protection in Europe and the United States. Information and communication technology and policy. 63-67. http://www.cnki.com.cn/Article/CJFDTotal-DXWJ202008012.htm

Yao C.,(2017). Key legal system of network security in South Korea and legislative consideration for China. Information security and communication confidentiality, 05,17-24.

YHA(2020).South Korea's National Assembly Passes' Three Data Laws. January 13,2020. Accessible at: http://kr.mofcom.gov.cn/article/jmxw/202001/20200102929813.shtml.

Young, S. . (2020). Zoombombing your toddler: user experience and the communication of zoom's privacy crisis. Journal of Business and Technical Communication. https://doi.org/10.1177/1050651920959201

Zhou H.,(2018). Exploring compatibility of personal data governance -- the legislation direction of China's personal information protection law. Law Research,40(02):3-23. https://doi.org/CNKI:SUN:LAWS.0.2018-02-001