International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 10 Issue 1 Series I || January 2021 || PP 05-14

A Systematic Approach of Impact of GDPR inPII and Privacy

Xiaohua Feng
School of Computer Science&Technology.University of Bedfordshire, Luton, UK

Yunzhong Feng
Hebei Normal University, Shijiazhuang, Hebei, P.R. China

Audrey Asante
School of CST,University of Bedfordshire,Luton, Bedfordshire, United Kingdom

ABSTRACT
*Since EU (European Union) published GDPR (General Data Protection Regulation) in 2016, every countries related have started to pay more attention on PII (Personally Identifiable Information) and personal privacy. GDPR and Data Protection Act 2018 lawsbrought people's attention on how to cope with data privacy, especially in the current pandemic.Conventional personal privacy breach crimes had been boostedwith the rapid development of ICT technology. The Internet had brought rise in cybercrimes even though it had changed the stages of activities, communications, socialization and way of access to information. Internet had now been applied as a tool by many cyber criminals hunt PII and personal privacy in order to performing their malicious activities. One of the reason behind Internet being frequently exploited by most cyber criminals had been that Internet was a low-cost, relative easyapproach for interaction [*Schneier,*2019]. Although there were different strategies had been developed and approved to control these cybercrimespotentially,people in the society realized handling of these crimes were seriouslysignificant. Attacks carried online by offenders or perpetrates were considered to have importantimpact, which could be severe when compared to attacks carried out offline and in the physical domain [Lipton 2011]. A strategy was proposed with feasible method to improve on privacy protection, in terms of enhance people's awareness on PII privacy in our society.*

KEYWORDS
Cyber security,General Data Protection Regulation (GDPR), Data Protection Act (DPA 2018), Data privacy management, Personally Identifiable Information (PII), Cybercrime detection.

Date of Submission: 25-10-2020 Date of Acceptance: 10-01-2021

I. INTRODUCTION

Personally identifiable information (PII) was defined as "any data that could potentially identify a specific individual". Any information that could be used to distinguish one person from another and couldbe applied for de-anonymizing previously anonymous data couldbe considered as PII; which is closely related to personal privacy [Rouse, nd; Hawthorn, 2015].PII may be used alone or in tandem with other relevant data to identify an individual and may incorporate direct identifiers.For instance, a passport information which could identify a person uniquely or quasi-identifiers, or race that could be combined with other quasi-identifiers, or date of birth, could recognize an individual, then takenpersonal privacy into account, had impact upon them. Under the pandemic crisis nowadays, PII and personal privacy are facing more challenges to keep GDPR and DPA 2018 on contact and tracing apps and so on. [Short, 2018; Feng, 2020]. A remedy was in need urgently.

II. BACKGROUND OF PII AND PRIVACY

Before 2016, people have already started researching about PII and its impact on privacy [Hawthorn, 2015 and Feng, 2015]. However, after GDPR was launched, PIIattracted more scientific researchers' attention. [ICO, 2016].Personally Identifiable Information (PII) included:"any information that could be used to distinguish or trace an individual's identity, for example, name, social security number, date and place of birth, mother's maiden name, or biometric records; any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."Moreover, from social science function point of view, a name was an individual symbol, was a personal identification for verification. For instance, a name could be used to distinguish from other individuals. Therefore, a name belonged to PII privacy.

Examples of PII included, such as:Names: full name, maiden name, mother's maiden name, alias. Personal identification numbers: social security number (SSN), passport number, National ID number, driver's license number, taxpayer identification number, patient identification number, financial account number, professional association number, professional certificate number or credit card number, Personal address information: street address, or email address, Personal telephone numbers. Personal characteristics: location data, daily life pattern, DNA information, photographic images fingerprints, keystroke logging or handwriting. As well as biometric data: retina scans, voice signatures, or facial geometry, iris recognition and so on. Information identifying: personally owned property, VIN number (vehicle identification number or title number. Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person.Also on personal own but not constitute PII as more than one person could share these traits. However, when linked or linkable to one of the above examples, the following could be used to identify a specific person: Postal or email address, Race, Religion, Geographical indicators, employment information, Medical record information, Education information and Financial informationsocial life pattern information and so on. [Pittsburth, nd; Pennsylvania, 2005a and Pennsylvania, 2005b]

While personal privacy was defined as "the right of people, associations or organizations to decide for themselves where, how and to what degree knowledge about them is transmitted to others". Moreover, privacy was defined "as the voluntary and temporary isolation of an individual from the wider public by physical or psychological means, either in the state of isolation or in the intimacy of a small group or a situation of anonymity or reservation by large groups". [Margulis, 2003] Another one was "defined as the right to have control over how personal information is collected and used." [Sakul, 2019]. From a systematic approach, the Data Protection Act 1984 is introduced in England, basic rules of DPA 1984 registration for users of data and rights of access to that data for the individuals to which it related to UK Legislation 1984. These rules and rights were revised and superseded by the Data Protection Act 1998 and Data Protection Act 2018.The later came into force on 20th century in UK. DPA 2018 quote all the key point of GDPR smoothly collaborate with EU GDPR and pay more attention on privacy [Swinhoe, 2019].The CIAA (Confidentiality, Integrity, Availability and Audit) security concept was implemented upon most aspects of our daily life. Personal PII and privacy is part of that. Cyber Security technology to support DPA 2018 and GDPR, to protect information data, systems and networks in the world from people with malicious intentions.Generally speaking, PII related information security should also be applied in our society. [Feng, 2015; Hawthorn, 2015 and ICO, 2016].

III. THE DPA CHANLLENGES OVERVIEW

Since the Covid-19 pandemic affected the world, people's life changed. The pandemic caused many challenges we never met before, but we had to learn to co-operate with them, in order to keep business as usual for our society.

3.1 Technical Challenges

In review on PII, personal privacy and safety had been published in the past. [Feng, 2015; Hawthorn, 2015], shortages were found. GDPR needed to be enforced for EU residence and EU relatedorganizations, the management needed also to follow the trends to think their users' requirements as the top priority. One of the technical challenge was to detect personal PII privacy and PII breaching. An in-depth discussion had been illustrated in later section. NIST (National Institute of Standards and Technology) had published some standards, guidelines and so on [NIST, 2016]. NIST launched a Framework for Online Privacy in 2018, [Lefkovitz, 2018] and updated version 1.0 in recent year. Nevertheless, there were many complicated issues under the Covid-19 pandemic crisis. According to statistics, cybercrime online cases increased since the pandemic.

To overview about PII under the current Covid-19 situation, since the Covid-19 pandemic, scientists in the world made use of AI technology to monitor and predict the trends of the pandemic. Naudé [2020] also used AI as a method for monitoring and prediction. AI was a good way of support diagnosis and forecast. AI was applied for medications and vaccination, and social regulation in the battle against the Covid-19, recognize constrains and threats. The result shown the data were fundamental evidence for short and long-term future strategy making and planning for fight the pandemic. In cyber space, Phishing was one of the most frequently happened malicious cybercrime attack in terms of obtaining personal PII and privacy information. E.g., mobile phishing, spear phishing, whaling, smishing and vishing and so on. Phishing detection had to be in place to prevent cybercrime.Moreover, DEA (Data Envelopment Analysis) [Emrouznejad, 2016] and AI technology could be applied to the pandemic data analysis,forecastand data management. Based on the monitored data statistics, carry out a significant analysis, properly data governance and data management could be executed. Then working out a strategy, such as a five years prediction or ten years trends forecast and planning.

Studies suggested citizen's trust in public administration and technology companies may be reduced due to events like revealed by lawsuits against Facebook, Zoom and the disclosure of classified information or government surveillance of people as reported by Edward Snowden in 2013 [MacAskill et al., 2013; Coyne, 2019]. Nevertheless, others around the world, such as the Australians were believed to see their PII private data used if for saving lives, or reduce the economic challenges and put a stop to the spread of the Covid-19 of virus.

A technical challenge example was about Zoom security issue, Zoom was not secure. This falls into three areas: a) Zoom has no good privacy feature, but is better than Facebook platform in this aspect. b) Zoom has weak implementation capability, for instance, in encryption. c) As a special case of above, Zoom is the lack of user specific credentials by default. This was worse before the last update, which forced the use of a password. However, it is only one meeting identification and password for the meeting and shared amongst users. To be fair, Webex had been doing this for years, but no one "bombed" them. Not to mention every conference called you had attended. When considering privacy securityevaluation depends on who you think your potential adversary was. Probably not the state or not organized crime. More likely an obsessive with a grudge did the breach.In this situation, they could put time into hacking you. If that was the case, it was not a problem. If people names were all in the public domain anyway as in the case of trustees, Zoom was only one more platform to target. Moreover, poor implementation was not a problem. Although Zoom were disordered. Amateurs would not break their system directly.As for the lack of user specific credentials by default was one to be cautious though. Using a paid for account, you could set Zoom up to force users to sign-in individually. Alternatively, you could think about Microsoft Skype for Business or Microsoft Teams; alternatively Signal or WhatsApp.When Zoom developed rapidly, a few perpetrate took advantage of it, making Zoom-bombing attempt to cause public disorder. Some user found fault with confidentiality. Zoom service reputation was affected. Zoom admitted to this expanding trend during the pandemic, Zoom was not fully prepared to solve the social needs of community resonance, especially in terms of personal PII privacy and security concerns. Zoom had put their resources and energy taken personal PII privacy and security issues into account, to improve from now on.Schneier Bruce [2019] is one of authority panel on this. He had published this in response to Zoom bombing. In the previous version, the meeting link was posted via email and such, the password for the meeting was often available in the meeting address[Short, 2020]. The fact is, although Zoom or Microsoft Teams and others were not properly tools, at this moment, we did not have much choice to maintain business.

3.2 Social Challenges

Although the COVID-19 pandemic was the top priority of government, liberty and well-being were still in strategy making list. In order to solve the current pandemic, test and trace were necessary. UK, Denmark, Germany, Italy, Latvia and Switzerland all use Gapple API (Application Programming Interface) app. In Pan-European Privacy-Preserving Proximity Tracing project, most states used Bluetooth Low Energy (BLE) as one of the choice, to save mobile phone in active state to distance measurement power consuming. However, in terms of enforced GDPR, personal PII and privacy become key factor to the challenges.

The global COVID-19 pandemic crisis had made each of the government in the world had to make their own strategyfrom time to time, according to the pandemic developed. However, there were a number of challenges would influence the governments' decisions based on AI scientific result. AI assistant security strategy should be on one of the top priority to influence governments in the world. AI security would help governments' strategy makers to work reasonably balancing between technologies, socially and politics. Feng et al. [2020] had indicated, strategy should related to challenges of AI and Security. The paper pointed out, AI security and governments' politics had to have a better trade-off from an initial planning to the near future development.Nevertheless, the current scientific research output demonstrated, with the potential of emerging epidemic control technologies, the possible advantage of combating existing pandemic threats or future occurrences possibility should be included in governments strategy planning.

3.3 Legal Challenges

A three-part composite shown Sundar Pichai, Jack Dorsey and Mark Zuckerberg, three chiefs faced tough questions over Internet Law. There were several cases of personal PII and privacy revealed from social media. These companies hadshortages about Internet Law in their platforms, urgent remedy required to patch holes, or other solutions. (BBC, 2020a) Although GDPR and the UK version DPA 2018 have been in position, there were still many incidences, which had not been imagined taken place. After 2018, for instance, Web form with personal information, due to the data that organization hold on their customers should be adequate for the purpose of record file holding the information. Nevertheless, organization should avoid holding more information than necessary for their customers. The best practice was to calculate the information organization need in terms of achieving the goals, a practice term called "minimisation". An example of this would be, in a case, when an individual customer unsubscribes from a service, the company should only keep hold of the minimum information needed in order to hold records on former customers. Fair [2020] made an argument. He said being infected with COVID-19 is not a crime. Therefore, GDPR or DPA 2018 on PII privacy still apply. Even for law enforcement, the case document could be hold for less than limited years.

The legal changes under GDPR or DPA since 2018, personal PII and privacy noticed on "how organizations use customers' information" guide now needed to be clearer than before. This meant that mere consent was not enough; the individual must be informed of exactly what their data was being used for. Furthermore, organizations must inform the customer of their right to withdraw consent at any time. That effectively protected customer from organization abusing their personal PII and privacy data. For example, under GDPR and DPA, in University of Bedfordshire student union (SU), they already had student data by virtue of a data sharing agreement with the university for representational purposes; this simply allowed student union to assign University of Bedfordshire existing student records as student representatives. Because of Data Protection Act 2018 and GDPR, the student representational election form claimed: before completing the course representational notification form, explicit permission was given to pass the students' details to the SU for the purpose of running the academic representatives system only and for no other purpose. SU could confirm the students understood that the SU would hold this information for 18months maximum and there was an email address to trigger its deletion. This was to ensure that communications with representatives could be facilitated throughout the academic year. The students understood that one could access PII and these information on what data the SU holds, how the personal PII privacy data was managed, ones rights and how to make a complaint through referring to the SU privacy policy online had been confirmed.

Up to date, the latest crisis investigation analysis and risk assessment shown, relative to first half of 2020, the number of new COVID-19 cases per day in the UK has reasonably changed at the national level as of the beginning 2020. There was, to date, minimal or inadequate scholarly analysis and evidence to show whether these changes witnessed in the daily rate of new COVID-19 case were subject to the users' willingness to compromise their personal privacy with the AI and digital technology solution. [Adegoroy, 2020]

The emerging threat themes were:

- Increase of online breach and harassment etc.
- Under reporting – reports said only 80-90%.
- Inconsistent response across and within the forces.
- Evidential difficulties.
- Problems with prosecution.
- Lack online bulling or stalking clinics–best practice.
- Victim impact–requires greater acknowledgment.
- Necessity of assisting victims as advocates.
- Perpetrators–communities and motivations are still in early stages of study/research.

Core messages from the investigation obtained were: good practice was apparent in several police forces, where multi-agency working where information sharing facilitates had the best management of perpetrators and safeguarding of victims. New understanding on motivations of online perpetrators and the communities, which support them was necessary. This research had identified evidential difficulties in personal PII and privacy breach cybercrimes, such as online bullying, stalking, harassment and revenge porn are the main barrier to proactively prevent andprosecution. [Short, 2018; Feng 2020]

IV. PII DATA PROTECTION BREACHCASE STUDY

4.1 Cybercrime on PII Consequence Statistics

The methodology of this investigation research usinga systematic approach, combination ofboth quantitative methods and qualitative methods were used. With the systematic approach, based on the law enforcement collected data related, refer to the wide and several record statistics in UK,carried out Personal PII privacy breaching cybercrime analysis [Feng, 2020].When NCCR (National Centre of Cybercrime Research)investigated PII and privacy were compromised cases, the consequence impact on victims' daily life were shown as follows: > 32.0% victims felt fearful about their personal safety; > 9.5% moved home; > 26% stopped answering their telephone. According to the police record,the privacy being breached victim portion within the investigation hadbeen illustrated as following in Figure 4.1.Consequently, the data had demonstrated enough necessity of PII and privacy protection to wellbeing in the society.

4.2 Possible PII and Privacy Cyber Crime

According to the police record, statistics of cybercrime percentage demonstrated in Figure 4.1. In addition, the statistics data shown the following fact:

- Over 17,000 case records from Hampshire, Bedfordshire, South Wales and Greater Manchester Police were analysed.
- Privacy break or cybercrime overlap needed to be understood comprehensively.
- Dispelling myth of the evil, in fact genius–most attacks are quite mundane.
- Necessity to increase skills and confidence in cyber field were in demand.These shown there were plenty work to be done to maintain GDPR and DPA2018 in the future [Short, 2018].

4.3 Personal Privacy and PII Risk

There were increasing personal PII and privacy breach threat with Internet technology growth rapidly worldwide. These crimes could even be multi states cases.The risk could be phishingidentity theft cybercrimes.
To havepeople’s credentials controlled.
To havesomebody’s online accounts (user name and password) being taken over.
To havepeople’s contact address details obtained and used.
To bullying, stalking or harassment of somebody’sfamily, friends and relatives, or colleagues (according to police’s statistics record, on average a cybercriminal will contact about 21 people connected to the victim).
Use of personal image-revenge porn and others being provoked to attack individual victim, escalation to physical violence, taking over victim’s online accounts,verification and so on; the list is endless [Feng,2017].

4.4 Possible PII and Privacy Cyber Criminals

For years, computer scientist and IT professionals were engaged on how to reduce the increasingly cybercrime. In Figure 4.1,it illustrated an analysis of possible personal PII and privacy attack source.

- Stranger – whose identity was established 21.7%.
- Acquaintance 20.4 %.
- Someone dated casually 18.2%.
- Unknown 16.4 %.
- These categories represented 76.4% of the groupand so on.These resulted in a challenge emerging for scientist how were the remaining 68% risk could be assessed reasonably in a professional manner [Short, 2018].

4.5 PII&Privacy Closely Related to Digital Forensics

Digital forensics was the process of identifying, preserving, analyzing, and documenting digital evidence. This was prepared in order to present evidence in a court of law when required. Digital forensics was an investigation and analysis science to gather and preserve evidence from a particular computing or digital device compromised, in a suitable way and in legallystandard for presentation in court.The goal of computer forensics was to perform a structured investigation with chain of custody to find out what happened and who was responsible for the digital attack[Feng, 2019]. Evidences couldbe extract from digital device. Forensics was track down the evidence with the aid of AI technology, report to law enforcement, and pin down the identity of cyberstalker or cyber criminals. One of the key focus currently is how to proactively detect and prevent or defend this kind of cybercrime. McFarlane [2003] put forward a comprehensive definition for cyber criminal as “A group of behaviors in which an individual, group of individuals or organization used information technology to harass one or more individuals.This kind of behavior may include (but were not limited to) transmission of threats and false accusations, identity theft, damage to data or equipment, computer monitoring and solicitation of minors for sexual purposes. Harassment was defined as a course of action that a reasonable person, in possession of the same information, would think causes another person to suffer emotional distress."

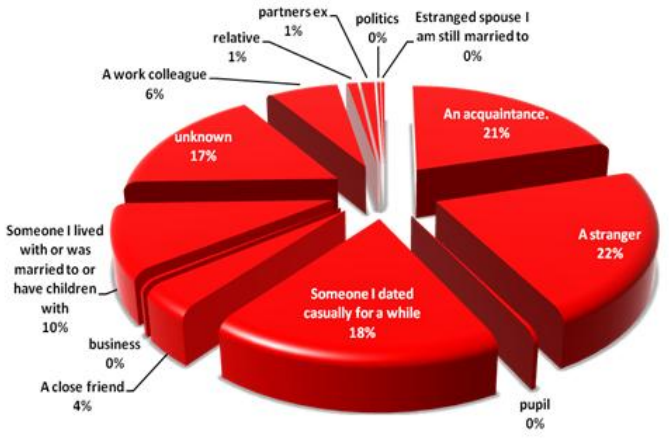

Figure 4.1 Source analysis

4.6 PII and Privacy Data Identification & Detection and Legal Consideration

Although Adegoroy, et al. [2020] hadcarried many works on privacy, including enabled the identification, filtering, detection, capturing and documentation of evidence and profiling of cyber-bullying and cyber-stalking offenders' data. There were still lack of research on personal PII and privacy crimes that occur at physical locations [Reyns. 2011]. There was also lack of accurate data about the prevalence of cybercrime cases. Furthermore, these updated data management. Nevertheless, NCCR hadworked out many data classification and analysis with real cases, bycollaboration with Bedfordshire Police. Later section gave detailswhich shown in Figure 4.2 [Short, 2018].

Personal PII and privacy data breaching had also been discussed in terms of DPA Laws previously [Feng, 2015; 2018]. Further development was in progress at NCCR, IRAC (Institute of Research Application Computing), University of Bedfordshire.In Cyber Law aspect, from legal theory of cyber science [Bainbridge, 2004] to a practical design application [Holt, 2011], GDPR, DPA 2018, Network Security Act, E-Commerce Act and so on needed to be embedded to the data analysis process in our society.[Feng, 2019]

4.7 Data Breach Framework and Application

According to the collected personal PII and privacy information, these data could be appliedto use DEA method [Emrouznejad, 2016; 2014] to analyses and using AI technology to process.AI technology on prediction applications, such as the current pandemic development trends, the R factor forecast, NHS beds needed, test and tracing, and so on accordingly. In order to detect PII offenders and non-offenders, the application involved use a proposed framework to carry out experiments.The proposed system would run on the systems' device to enable the capturing of evidence. The Figure 4.2 is one of the PII cybercrime detection frameworks, that Ghasem proposed during the research carried out at NCCR. This system was based on the 2015 report [Ghasem, 2015]. It demonstrated proposed architecture of the detection framework in Figure 4.2. As it illustrated, this cybercrime detection framework adopted for detecting cyberstalking was based on machine learning methodology, text data mining techniques, profiling and digital forensic investigation methodology. Supervised learning approach was adopted by training data examples to allow wider application of this approach to different domains identified under cyberstalking. Understanding the characteristics and behavior of traditional and cyber stalkers would help understand how messages or information could be filtered, analyzed and stored as evidence.The system was made up of six modules which are message identification, filter, content detection, identification and profiling of cyber stalker, analysis and evidence modules. Under the evidence module, two modules that were normal evidence and encrypted evidence were collected. Contacts, trained example profiles and database wouldsupport the detection process. Testing had been carried out with this framework [Feng, 2018]. Summarize above, personal PII privacy proactive protection strategy were in need and with high priority in the world currently.

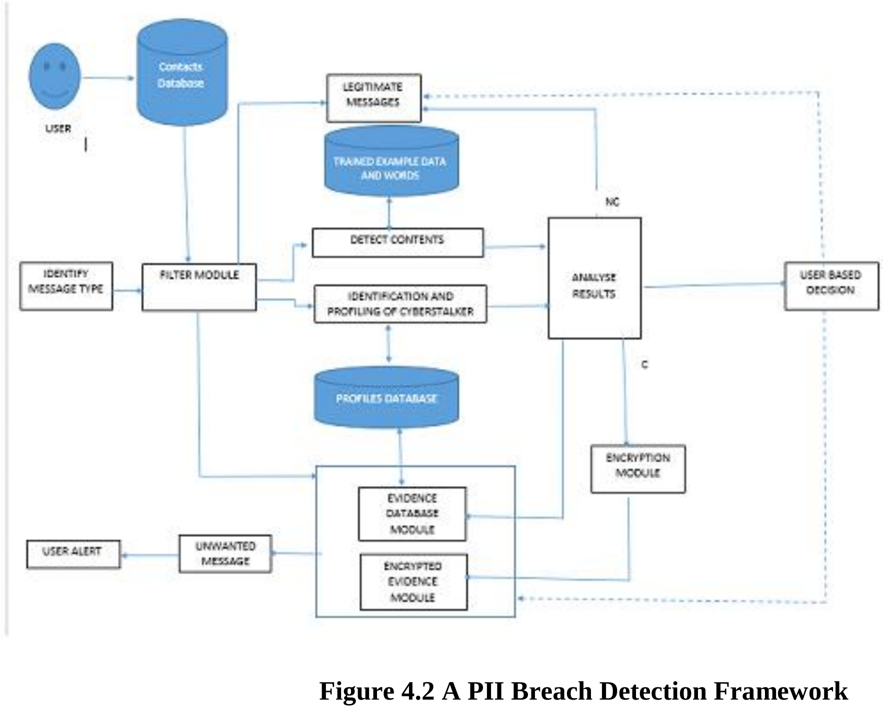

Figure 4.2 A PII Breach Detection Framework

V. DISCUSSIONS

Here, as demonstrated in Figure 4.1 and Figure 4.2, personal PII and privacy data protection breach and cybercrime detection service were supplied. In fact, all of these requirement about safety and security protection solutions were consideredabout PII and privacy data cyber security being considered as earlier as before GDPR and DPA 2018 in place [Hawthorn, 2015; Feng, 2015]. During a COVID-19 pandemic crisis period, PII and personal privacy security involved of every stage and aspect of human beings' daily life. A strategy on PII privacy protection should be necessary.

The framework testing had been carried out successfully, and that similarly shown data protection was very important, in order to ensure the society life quality.One of the challenges in biometrics security of PII privacy remained outstanding. There were people lack of fingerprints. When recognize special individuals, there were still had no any solution.Up to date, we have to admit, there was still without a thoroughly appropriate solution in the outstanding cyber security issues to protect the online application and services for personal PII and privacy. Professionals and scientists were all trying their best to achieve a better trade-off withgood online services and cyber security in terms of improving personal PII and privacy in society.

To summarize personal PII and privacy under the current Covid-19 pandemic situation, AI technology demonstrated on monitor and predict the trends of the pandemic perform to be the most significant for both nature science and social science researchers to consider to be the future solution. To reasonable applying of AI technology foragainst the pandemic, while concerning public health might overshadow personal data protection issues. A mission maybe arise, with governments maintaining their citizens' unnecessary monitoring longereven after the pandemic ended. Kapa [2020] specified "further research should be needed as to whether privacy-enabled measures minimize the effectiveness of contact tracing due to reliance on private consumer response rather than strict implementation by a central authority" [Kapa, 2020; Adegoroy, 2020]. Oliver et al. [2020] conducted a COVID-19 related survey involving 156,614 general adult population via social media posts to assess the Spanish citizens' situation and perception on their social contact behavior during the confinement, their economic impact, their work environment situation and their health status. This research indicated that Spaniard had shown high conformity with all confinement measures, although more than a quarter of the population reports lacking the necessary quarantine.

The investigation result shown gender and age matter regarding social interaction behavior, the economic,industryand self-quarantine impact. This result lead to discussion on the usage of apps, such as COVID-19 Exposure Notification System. Sakul-Ung and Smanchat's [2019] Integrated Privacy System study showna framework includes helpful components for data protection management, development and monitoring mechanisms. This could be useful in developing privacy-aware AI products services. Nanni et al., [2020] study supported the benefit of a distributed approach where contact and location data were strictly gathered to be separately, selective and voluntarily shared only when the person being tested positive while necessity and the individual had full control of the privacy. They suggested "existing architectures being extended carefully to manage the gatheringgeographic data locally on user's device and allow the user to share with health authorities, for example, as they were fit and for specialpurposes. Also an effort of create the concept of a Personal PII and Privacy Data Storage that allowed users to contribute to gathered data as they consent". [Adegoroy, 2020] Corresponding to personal PII and privacy DPA 2018, Welsh government promised, the pandemic contact and tracing data would not release to any one unnecessary. [BBC, 2020b]. In addition, bio-information was one of the highest sensitive data, which would be one of life-long identity.One of the personal PII and privacy issueof the pandemic's implications was working online. Microsoft Teams, Zoom, Google Hangout Meet, Apple Houseparty were among the top video conferencing software adopted as abasic toolkit during this pandemic period [Sydow, 2020]; even UK PM Mr. Johnson also claimed to use Zoom for his cabinet meeting. Reports suggested that while there was no evidence of Zoom selling user information to third parties, the terms of use of the company offer some flexibilityto acquireor exchange information data. Its instant messages could be used to advertising.The hosts could turn on 'attention monitoring' to test if the user paid attention during the call [O'Flaherty, 2020]. While Zoom may meet the US privacy laws, but it did not meet the EU GDPR law [EU, 2018; ICO 2016]. So, the fact were still needed to be aware.

VI. CONCLUSIONS

In this paper, we hadoverlooked the current challengesand the impact of the GDPR to personal PII and Privacy in a systematic approach. Investigated majority of related aspect, although a legacy is inherited from previous research in ourNCCR Research Centre, the research work being reported here werestill only an early stage experience when we face the current Covid-19 pandemiccrisis internationally.To keep PII and personal privacy under GDPR and DPA 2018 were not easy in this hard time nowadays. The most difficulties were Phishing threat and cybercrimes. A strategy of proactively protect PII privacy, to against phishing personal security attack needed cyber security PII education to enhance citizen's security awareness in the technology fast developed society, which was important and necessary.

While to fight against cybercrime technically could be a long ongoing battle, demand many resources, including government and senior management of organization supports.A case study example of handling cybercrime message to protect personal PII and privacy data had been illustrated in this paper, section 4[Ghasem, 2015; Short 2018]. Strategic suggestions reported in this paper, in order to enhance worldwide cyber security awareness on personal PII and Privacy.

A suggested further development was for a more appropriate approach to finalize the planning, dealing with the multiple diversity issues, including GDPR and DPA 2018 incidents, to protect personal PII and privacy information data [ICO, 2016; Hawthorn, 2015]. The plan principle would need to be applied on the development of cyber security law sets, with security audit for the time being [Feng, 2018]. A balanced compensation would be an ongoing process in the near future coming decades, as Figure 4.1 shown perhaps.Moreover, take data of the pandemic prediction into account of planning considerations as Figure 4.1 demonstrated, to work out a good trade-off in every aspects. Furthermore, develop AI privacy app tools could be helpful in the circumstances.

ACKNOWLEDGMENTS

The authors would like to appreciate Dr. E. Short and Prof. J. Barn and NCCR for their support on this research.

KEY REFERENCES ANDBIBLIOGRAPHY

[1]. Adewale Adegoroy et al. (2020) "*A new perspective on the issue of privacy: Covid-19 pandemic vs. privacy*". IADC (International Association of Drilling Contractors). The 19th International Conference of Internet (ICWI 2020).

[2]. Antoine Olivier, et al (2013) "*ISO/IEC 27018: The Future Standard for Personal Data Protection in Public Cloud*", EBRC (European Business Reliance Centre). 2013.

[3]. BBC(2020a) "*Facebook, Twitter and Google face questions from US senators*" https://www.bbc.co.uk/news/technology-54721023

[4]. BBC(2020b)*BBCTechnology*BBCClick,https://www.bbc.co.uk/programmes/m000nzn3 [Accessed: 24/10/2020]

[5]. BBC (2018a)"*Smart home gadgets in domestic abuse warning*" BBC Technology, http://www.bbc.co.uk/news/technology-44765830 [Accessed: 19/10/2020]

[6]. BBC (2018b) "*Is your computer safe from the cryptojackers*?" BBC Click. https://www.youtube.com/watch?v=aSMVgoaHA50 [Accessed: 18/09/2018]

[7]. BBC (2012a) "*Keeping your personal information safe online*" BBC On Top of the Digital World. https://www.bbc.co.uk/programmes/p0110jl9 [Accessed: 18/09/2019]

[8]. BBC (2012b) "*Cyberbullying - impact and prevention*". BBC On TopoftheDigitalWorld programme.https://www.bbc.co.uk/programmes/p0110jl9 [Accessed: 19/11/2019]

[9]. Bainbridge, David (2004) "*Introduction to ComputerLaw*", 5th Ed. Aston University, Longman/Pearson Edu.ISBN 0-582-47365-9

[10]. Beebe, N.L. and Clark, J.G. (2005) *"A hierarchical, objectives-based framework for the digital investigations process"*, Digital Investigation, 2 (2), pp.147-167.

[11]. Belot, H. (2018) "*Security leak about spy agency referred to AFP*". https://www.abc.net.au/news/2018-04-29/labor-blames-government-for-security-leak/9708594

[12]. Brown C.S. (2015) "*Investigating and Prosecuting Cyber Crime: Forensic Dependencies and barriers to Justice*" International Journal of Cyber Criminology, 9(1) pp55.

[13]. Coyne, H. (2019) "*The Untold Story of Edward Snowden's Impact on the GDPR*", The Cyber Defense Review, 4(2), pp. 65-80. Doi: 10.2307/26843893.

[14]. DFRWS Technical Committee (2001) "*A Road Map for Digital Forensic Research*" DFRWS Technical Report.

[15]. Emrouznejad Ali (2016) "*Big Data Optimization: Recent Developments and Challenges. In the series of "Studies in Big Data*", Springer-Verlag, ISBN: 978-3-319-30263-8.

[16]. Emrouznejad, A.; R. Banker; Munisamy, S. and Arabi B. (2014), "*Theory and Applications of Data Envelopment Analysis*", Proceedings of the 12th International Conference of DEA, April 2014, University of Malaya, Malaysia, ISBN: 978 1 85449 487 0.

[17]. Fair, P. (2020) "*Privacy vs pandemic: government tracking of mobile phones could be a potent weapon against COVID-19*", The Conversation Science and Technology, March 2020.

[18]. Feng, X. and Zhang X. (2015) "*Personally Identifiable Information Security in Cloud Computing*", International Conference on Computing and Technology Innovation, UK

[19]. Feng, X.; Asante Audrey and Short Emma (2017) "*Cyber-Bullying, Cyber-Stalking and Digital Forensics*", IEEE Xplore, the 3rdIEEE International Conference on CyberSciTech, FL. USA. November 2017.

[20]. Feng Xiaohua, Short Emma and Barnes Jim (2018) "*Cyber-Bullying and Online Safety for Children*" BCS Seminar, National Centre for Cyberstalking Research (NCCR), School of Computer Sciences and Technology, Faculty of Creative Arts, & BCS, UK.

[21]. Feng X. et al. (2019) "*Computer Laws Consideration on Smart City Data Planning of Chongli* 2022" IEEE proceeding of ACE-2019 International Workshop. UK.

[22]. Feng, X. and Feng Y. et al. (2020) "*Artificial Intelligenceand Cyber Security Strategy*", IEEE 5th International CyberSciTech Conference, Athabasca University, Calgary, Canada.

[23]. Forsyth, R. and Rada, R. (1986) "*Machine learning: applications in expert systems and information retrieval*". Halsted Press.

[24]. Gangavane, H., Nikose, M. and Chavan, P. (2015). "*A novel approach for document clustering to criminal identification by using abk-means algorithm*" IEEE Computer Communication and Control (IC4) 2015, pp. 1-6.

[25]. Ghasem A. et al. (2015)"*A Machine Learning Framework to Detect and Document Text-based Cyberstalking*", NCCR, University of Bedfordshire.

[26]. Hawthorn, N. et al. (2015)"*White paper: How European Union data protection affects your data in the cloud, the new EU data protection regulations*", Skyhigh and DMH Stallard LLP, Euro Cloud Expo 2015.

[27]. Holt Jeremy et al. (2011) "*A Managers Guide to IT Law*", British Computer Society, 2nd Ed. ISBN 10: 1906124752, ISBN 13: 9781906124755

[28]. ICO (2016) "*Overview of the General Data Protection Regulation (GDPR)*". https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ [Accessed 14/3/2017].

[29]. Kapa Suraj, Halamka, John and Raskar Ramesh (2020) "*Contact Tracing to Manage COVID-19 Spread—Balancing Personal Privacy and Public Health*", Mayo Clinic. Cardiovascular Medicine.

[30]. Lefkovitz Naomi (2018) "*A Framework for Online Privacy*". National Institute of Standards and Technology).

[31]. Lipton, Jacqueline D. (2011). "*Combating cyber-victimization*". Berkeley Technology Law Journal, 26, pp. 1104–1126.

[32]. NIST (2020) "*Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*", NIST 2020.

[33]. Pennsylvania State (2005a) "*Pennsylvania Breach of Personal Information Notification Act*". Pennsylvania State.http://www.palrb.us/pamphletlaws/20002099/2005/0/act/0094.pdf. [Accessed 19/10/2020].

[34]. Pennsylvania (2005b) "*Pennsylvania Privacy of Social Security Numbers Act*". Pennsylvania State. http://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=HTM&sessYr=2005&sessInd=0&billBody=S&billType=B&billNbr=0601&pn=1791

[35]. Rouse Margaret and Bernstein Corinne (nd) "*Personally-identifiable-information*". TechTarget. https://searchsecurity.techtarget.com/definition/personally-identifiable-information-PII [Accessed: 16/10/2020]

[36]. Schneier Bruce (2019) "*We Have Root: Even More Advice from Schneier on Security*" 1st Ed. Kindle Edition. ISBN-13: 978-1119643012, ISBN-10: 1119643015.

[37]. Short Emma and Barnes Jim (2018) "*Cyberstalking*", National Centre for Cyberstalking Research (NCCR), 2018 Conf. of UoB.

[38]. Vinciworks (2018) "*The Eight Principles of Data Protection*" https://vinciworks.com/blog/8-principles-data-protection-act-gdpr-guide/ [Accessed: 18/10/2020].

[39]. University of Pittsburth (nd) "*Guide to Identifying Personally Identifiable Information (PII)*" University of Pittsburth. https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii[Accessed: 16/10/2020].

Xiaohua Feng, et. al. "A Systematic Approach of Impact of GDPR in PII and Privacy."*International Journal of Engineering Science Invention (IJESI)*, Vol. 10(01), 2021, PP 05-14. Journal DOI- 10.35629/6734