A Systematic Approach of Impact of GDPR in PII and Privacy

Xiaohua Feng
School of Computer Science&Technolog.
University of Bedfordshire, Luton, UK
Xiaohua.feng@beds.ac.uk
Tel. +441234400400

Yunzhong Feng
Hebei Normal University
Shijiazhuang, Hebei,
P.R. China
fyz02817@sina.com

A. 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 2018 laws brings people's attention, how to cope with data privacy, especially in the current pandemic.

Conventional personal privacy breach crimes have been boosted with the rapid development of ICT technology. The Internet has brought rise in cybercrimes even though it has changed the stages of activities, communications, socialisation and way of access to information. The Internet has now been used as a tool by many cyber criminals hunt PII and personal privacy in order to performing their malicious activities. One of the reason behind the Internet being frequently used by most cyber criminals has been that the Internet is a low-cost, relative easy approach for interaction [Shimizu 2013]. Although there were different strategies have been developed and approved to control these cybercrimes potentialy, since people in the society realised handling of these crimes are seriously significant. Attacks carried online by offenders or perpetrates are considered to have important impact, which could be severe when compared to attacks carried out offline and in the physical domain [Lipton 2011].

KEYWORDS

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

1 INTRODUCTION

Personally identifiable information (PII) is defined as "any data that could potentially identify a specific individual". Any information that can be used to distinguish one person from another and can be used for de-anonymizing previously anonymous data can be considered 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, such as passport information, that can identify a person uniquely or quasi-identifiers, such as race, that can be combined with other quasi-identifiers, like date of birth, to successfully recognize an individual then affect their privacy. 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].

2 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 is launched, PII focused more scientific researchers' attention. [ICO, 2016; EU, 2018].

Personally Identifiable Information (PII) includes: "any information that can be used to distinguish or trace an individual's identity, such as 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." Such as, from social science function point of view, a name is an individual symbol, is a personal identification for verification. For instance, a name is used to distinguish from other individuals. So, a name belong to PII.

Examples of PII include, such as: Name: 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 information social life pattern information and so on. [Pittsburth, nd; Pennsylvania 2005a and Pennsylvania, 2005b]

While personal privacy is defined as "the right of people, associations or organisations to decide for themselves where, how and to what degree knowledge about them is transmitted to others". Also privacy is "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 is "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 [UK Legislation, 1984]. These rules and rights were revised and superseded by the Data Protection Act 1998 and Data Protection Act 2018 [UK Legislation, 2018], The later came into force on 20th century in United Kingdom. DPA 2018 quote all the key point of GDPR smoothly collaborate with EU GDPR and pay more attention on privacy [Swinhoe, 2019; EU, 2018].

The CIAA (Confidentiality, Integrity, Availability and Audit) security concept is 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].

3 THE DPA CHANLLENGES OVERVIEW

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

3.1 Technical Challenges

In research on PII, personal privacy and safety has been published in the past. [Feng, 2015; Hawthorn, 2015]. Furthermore, GDPR needs to be enforced for European Union (EU) residence and the organisations, the management need also to follow the trends to think their users' requirements as the top priority. One of the technical challenge is to detect personal privacy and PII breach. An in-depth discussion has been illustrated in later section.

NIST (National Institute of Standards and Technology) has published some standard, guidelines, and so on. [NIST, 2016] Some of them are quite appropriate to smart city scenarios, which could be used. NIST launched a Framework for Online Privacy in 2018, [Lefkovitz, 2018] and updated version 1.0 this year. However, there are many complicated issues under the Covid-19 pandemic crisis. One of the technical challenge is to detect personal privacy and PII breach. An in-depth discussion has been illustrated in later section.

To overview about PII under the current Covid-19 situation, Since the Covid-19 pandemic crisis, scientists in the world make use of AI technology to monitor and predict the trends of the pandemic. Naudé [2020] also use AI as a method for monitoring and prediction. AI is a good way of support diagnosis and forecast. AI for medications and vaccination, and social regulation in the battle against the Covid-19 and recognize constrains and threats. The result shown the data are fundamental evidence for short and long term future strategy making and planning for fight the pandemic. In cyber space, Phishing is one of the most frequently happened malicious cybercrime attack in order to obtain personal PII and privacy information. Such as, mobile phishing, spear phishing, whaling, smishing and vishing and so on. Phishing detection have to be in place to prevent.

Moreover, DEA (Data Envelopment Analysis) [Emrouznejad, 2016] and AI (Artificial Intelligence) technology [2020] could be applied to the pandemic data analysis, prediction and data management. Based on the monitored data statistics, carry out a significant analysis, properly data governance and data management. Then working out a strategy, such as a five years prediction or a ten years trends forecast and planning.

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

A technical challenge example is about Zoom security issue, Zoom is not secure. This basically 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 really 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. (there is the English saying, that once three people know a secret, it's not a secret.) To be fair, Webex have been doing this for years, but no one "bombed" them. Not to mention every conference call you have attended. When considering privacy security–evaluation depends on who you think your potential adversary is. Probably not the state, or not organised crime. More likely an obsessive with a grudge did the breach.

In this situation, they could put time into hacking you. If that is the case, it is not a problem. If people names are all in the public domain anyway as in the case of trustees, Zoom is only one more platform to target. Also, poor implementation is not a problem. Although Zoom are sloppy. Amateurs will not break their system directly.

As for the lack of user specific credentials by default is one to watch out for though. Using a paid for account, you can 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 take advantage of it, making Zoom-boming attempt to cause public disorder. Some user found fault with confidentiality. Zoom service reputation is affected. Zoom admit, to this expanding trend during the pandemic, Zoom is not fully prepared to solve the social needs of community resonance, especially in terms of personal PII and privacy and security concerns. Zoom has put their resources and energy taken personal PII security and privacy issues into account, to improve from now on.

Schneier Bruce [2019] is one of authority panel on this. He has 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 are not properly tools, at this moment, we do not have much choice to maintain business.

3.2 Social Challenges

Although the COVID-19 pandemic crisis is the current top priority of Government, liberty and well-being are still in the strategy making list. In order to solve the current pandemic, test and trace or contact and trace are 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 use 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 a factor to one of the challenges.

The global COVID-19 pandemic have made each of the government in the world have to make their own strategy from time to time, according to the pandemic develops. However, there are a number of challenges will influence the governments' decisions based on AI scientific result [NewScientist, 2017].

AI assistant security strategy should be on one of the top priority to influence governments in the world. AI security will help governments' strategy makers to work reasonably balancing between technologies, socially and politics. Feng et al. [2020] has indicated, strategy should related to challenges of AI and Security. The paper pointed out, AI security and governments' politics have to have a better trade-off from an initial planning to the near future development. Nevertheless, the current scientific research output gave 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 face tough questions over Internet Law. There were several cases of personal PII and privacy revealed from social media. These companies have gaps about Internet Law in their platforms, remedy needed to patch holes, or other solutions. (BBC, 2020a)

Although GDPR and its UK version DPA 2018 have been in position, there are still many incidences, which have not been imagined taken place. After 2018, for instance, Web form with personal Information, due to the data that organisation hold on their customers should be adequate for the purpose of record file holding the information. Nevertheless, organisation should avoid holding more information than necessary for their customers. The best practice is to calculate the information organisation need in order to achieve 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. So, GDPR on PII still apply. Even for law enforcement, the case document could be hold for less than ten years.

The legal changes under GDPR since 2018, PII and privacy notices on "how organisations use customers' information" guide now need to be clearer than before. This means that mere consent is not enough; the individual must be informed of exactly what their data is being used for. Furthermore, organisations must inform the customer of their right to withdraw consent at any time. That effectively protected customer from organisation abuse their PII and privacy data.

For example, under GDPR, in our University of Bedfordshire student union (SU), they already have student data by virtue of a data sharing agreement with the university for representational purposes; this simply allows 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 Student Union for the purpose of running the academic representatives system only and for no other purpose. SU can confirm the students understands that the Union will hold this information for 18 months maximum and there is an email address: be.heard@beds.ac.uk to trigger its deletion.

This is to ensure that communications with representatives can be facilitated throughout the academic year. The students understands that one can access PII and these information data on what data the SU holds, how the personal PII and privacy data is managed, ones rights and how to make a complaint through referring to the SU privacy policy online at www.bedssu.co.uk/dataprotection has been confirmed.

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

The emerging threat themes are:

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

4 PII DATA PROTECTION BREACH CASE STUDY

4.1 Cybercrime on PII Consequence Statistics

The methodology of this investigation research, a systematic approach, combine both 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 United Kingdom we carried out Personal PII and privacy breach cybercrime analysis [Feng, 2019; 2020].

When NCCR investigate personal PII and privacy were compromised cases, the consequence impact on victims' daily life are show 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 have been illustrated as follows in Figure 4.1.

Consequently, the data have 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 needs to be understood comprehensively.
- Revenge porn used in course of conduct.
- Links identified in escalation to violence.
- Dispelling myth of the evil, in fact genius– most attacks are quite mundane.
- Necessity to increase skills and confidence in cyber field is in demand.

These shown there are plenty work to be done to maintain GDPR and DPA2018 for us in the future [Short, 2018].

4.3 Personal Privacy and PII Risk

There are increasing personal PII and privacy breach threat with Internet technology growth rapidly worldwide. These crimes could even be multi states cases. These risk could be such as phishing, spear phishing, whaling, smishing and vishing or in other words, identity theft cyber crimes [Feng, 2017].

To have people's credentials controlled.

To have somebody's online accounts (user name and password) being taken over.

To have people's contact address details obtained and used.

To locating and tracking of someone by GPS on laptop, mobile phones, tracker devices or spyware on phones.

Make up a false profile posted on social networking and other sites.

To have malicious websites, blogs and social networking sites misleading about a person.

To impersonation of a person being used to bullying or stalk others, positioning people as the guilty party.

Making someone discredited in social media and other online communities.

Making a person discredited in people's place of work or receiving direct threats through email or instant messaging.

To bullying, stalking or harassment of somebody's family, 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, like the criminal taking over victim's online accounts, verification and so on; the list is endless [Feng, 2018].

4.4 Possible PII and Privacy Cyber Criminals

For years, computer scientist and IT professionals are engaged on how to reduce the increasingly cybercrime. In Figure 4.1, it illustrated an analysis of possible 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 represent 76.4% of the group.

A classification of personal PII and Privacy cybercrime breach record shown in Figure 4.1. These resulted in a challenge emerging for scientist: how are the remaining 68% risk could possibly being assessed reasonably in a professional manner [Short, 2018].

4.5 PII & Privacy Closely Related to Digital Forensics

Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is prepared in order to present evidence in a court of law when required. Digital forensics is an investigation and analysis science to gather and preserve evidence from a particular computing or digital device compromised, in a suitable way and in legally standard for presentation in court of law. The goal of computer forensics is to perform a structured investigation with chain of custody to find out what happened and who was responsible for the digital attack. [Feng, 2019]

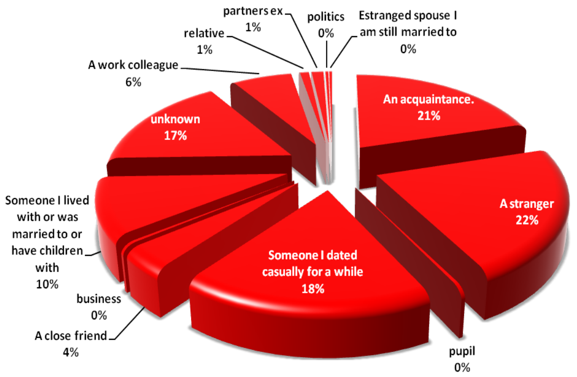

Figure 4.1 Source analysis [Short, 2018]

We can extract evidences from digital device. Forensics is track down the evidence with the aid of AI technology, report to law enforcement, and pin down the identity of the stalker and cyber criminals. And 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 behaviours in which an individual, group of individuals or organisation uses information technology to harass one or more individuals. Such the behaviour may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring and the solicitation of minors for sexual purposes. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress."

4.6 PII and Privacy Data Identification & Detection and Legal Consideration

Although Adegoroy, et al. [2020] have carried 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 are still lack of research on personal PII and privacy crimes that occur at physical locations [Reyns, Henson et al. 2011]. There is also lack of accurate data about the prevalence of cybercrime cases. Furthermore, these updated data management. Nevertheless, NCCR (National Centre of Cybercrime Research) has worked out many data classification and analysis with real cases, by collaboration with Bedfordshire Police. Later section gave details which shown in Figure 4.2 [Short, 2018].

Personal PII and privacy data breaches have also been discussed in terms of DPA Laws previously [Feng, 2015; 2018]. Further development is in progress at NCCR, IRAC (Institute of Research Application Computing), University of Bedfordshire, UK.

In Cyber Law aspect, from legal theory of cyber science [Bainbridge, 2004] to a practical design application [Holt, 2011], GDPR, Network Security Act, E-Commerce Act and so on need 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, we could use these data to use DEA method [Emrouznejad, 2016; 2014] to analyses and using AI technology to process for us.

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 some experiment.

The proposed system will 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 University of Bedfordshire. This system is based on the 2015 reported [Ghasem, 2015]. It demonstrated proposed architecture of the detection framework in Figure 4.2.

As Figure 4.2 demonstrated, this cybercrime detection framework adopted for detecting cyberstalking is based on machine learning methodology, text and 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 will help understand how messages or information can be filtered, analysed and stored as evidence.

The system is 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 which are normal evidence and encrypted evidence are collected. Contacts, trained examples data and profiles database will support the detection process. Testing have been on going with this framework [Feng, 2017].

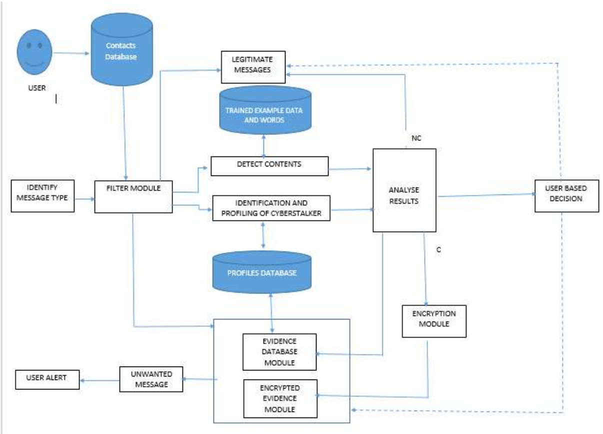

Figure 4.2 A PII Breach Detection Framework

5 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 need safety and security protection solutions considered, as earlier as PII and privacy data being considered before GDPR [Hawthorn, 2015; Feng, 2015] and cyber security.

For a COVID-19 pandemic crisis development period, PII and personal privacy security involved of every stage and aspect of human daily life. The framework testing have been carried out successfully, and that also shown data protection is very important, in order to ensure the society life quality.

One of the challenges in biometrics security of PII privacy remains outstanding. There were people lack of fingerprints. When recognize special individuals, there were still have no any solution yet.

Up to today, we have to admit, there is still without a thoroughly perfect/appropriate solution in the outstanding cyber security issues to protect the online application and services for personal PII and privacy. Professionals and scientists are all try their best to achieve a good trade-off between better online services and cyber security in order to improve personal PII and privacy in our society life.

To summarise personal PII and privacy under the current Covid-19 pandemic situation, AI technology indicate/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 selection/solution.

Reasonable use of AI against the pandemic, while concerning public health issues might overshadow personal data protection issues and that mission maybe arise, with governments maintaining their citizens' unnecessary monitoring long after the pandemic has ended. Kapa [2020] specified "further research is needed as to whether privacy-enabled measures minimise 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 indicates that Spaniard has 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, industry and self-quarantine impact. This result leads to discussion on the usage of apps. such as COVID-19 Exposure Notification System. Sakul-Ung and Smanchat's [2019] Integrated Privacy System study shown a framework includes helpful components for data protection management, development and monitoring mechanisms. This maybe useful in developing privacy-aware AI products services. Nanni et al., [2020] study supports the benefit of a distributed approach where contact and location data are strictly gathered to be separately, selective and voluntarily shared only when the person tested positive while necessity and the individual has full control of the privacy. They suggested: "existing architectures being extended carefully to manage the gathering geographic data locally on user's device, and allow the user to share with health authorities, e.g. as they were fit and for special purposes. Also an effort of create the concept of a Personal PII and Privacy Data Storage that allows 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 is one of the highest sensitive data, which would be one of life-ling identity.

One of the personal PII and privacy issue of the pandemic's implications is working online (from home). Microsoft Teams, Zoom, Hangout Meets, Houseparty are among the top video conferencing software adopted as a basic tool during this period [Sydow, 2020]; even Boris 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 flexibility to acquire or exchange information data. Its instant messages can 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 does not meet the EU GDPR law [EU, 2018; ICO 2016].

6 CONCLUSIONS

In this paper, we have overlooked the current challenges and the impact of the GDPR to personal PII and Privacy in a systematic approach. Investigated every related aspect, we think, although a legacy is inherited from previous research in our NCCR research Centre, the research work being reported here is still only an early stage experience when we face the current Covid-19 pandemic crisis internationally.

To keep PII and personal privacy under GDPR is not easy in this hard time nowadays. The most difficulty is Phishing threat and cybercrime. To against phishing personal security attack needs cyber security education to enhance citizen's security awareness in the technology fast developed society. While to fight against cybercrime technically is a long ongoing battle, demand many resources, including government and senior management of organisation supports.

A case study example of handling cybercrime message to protect personal PII and privacy data has been illustrated in this paper, section 4. [Ghasem, 2015; Feng, 2017 and Short 2018]

A suggested further development is for a more appropriate approach to finalize the planning, dealing with the multiple diversity issues, including GDPR and DPA 2018 incidents, to protect PII and privacy information [ICO, 2016; Hawthorn, 2015].

The plan principle will also need to be applied on the development of cyber security law sets, with security audit for the time being [Feng, 2018]. A well balanced compensation will 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 protection tools could be helpful in this kind of 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 AND BIBLIOGRAPHY

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).

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

BBC (2020a) "*Facebook, Twitter and Google face questions from US senators*" https://www.bbc.co.uk/news/technology-54721023 [Accessed: 28/10/2020]

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

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

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

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]

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

Bainbridge, David (2004) "*Introduction to Computer Law*", 5th Edition, Aston University, Longman/Pearson Edu. UK. ISBN 0-582-47365-9

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.

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

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

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.

DFRWS Technical Committee (2001) “*A Road Map for Digital Forensic Research*” DFRWS Technical Report.

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.

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, Kuala Lumpur, Malaysia, ISBN: 978 1 85449 487 0.

European Parliament and EU Council (2018) “*General Data Protection Regulation (GDPR) – Official Legal Text*”. Available at: https://gdpr-info.eu/

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.

Feng, X. and Zhang X. (2015) “*Personally Identifiable Information Security in Cloud Computing*”, International Conference on Computing and Technology Innovation, UK

Feng, X.; Asante Audrey and Short Emma (2017) “*Cyber-Bullying, Cyber-Stalking and Digital Forensics*”, IEEE Xplore, the 3rd IEEE International Conference on CyberSciTech, FL. USA. November 2017.

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.

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

Feng, X. and Feng Y. et al. (2020) “*Artificial Intelligence and Cyber Security Strategy*”, IEEE 5th International CyberSciTech Conference, Athabasca University, Calgary, Canada.

Forsyth, R. and Rada, R. (1986) “*Machine learning: applications in expert systems and information retrieval*”. Halsted Press.

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.

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

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.

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

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].

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.

Lefkovitz Naomi (2018) “*A Framework for Online Privacy*”. National Institute of Standards and Technology).

Lipton, Jacqueline D. (2011). “*Combating cyber-victimization*”. Berkeley Technology Law Journal, 26, pp. 1104–1126

MacAskill, E., Dance, G., Cage, F., Chen, G. and Popovich, N. (2013) “*NSA files decoded: Edward Snowden's surveillance revelations explained*”. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded [Accessed: 12/10/ 2020].

Margulis, S.T. (2003) “*On the Status and Contribution of Westin's and Altman's Theories of Privacy*”, Journal of Social Issues, 59(2), pp. 411-429. doi: 10.1111/1540-4560.00071.

McFarlane (2003) “*An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers*”. First Monday, 8(9). The University of Illinois at Chicago University Library. ISSN 1396-0466.

Mullen Paul, Pathé Michele and Purcell Rosemary (2009), “*Stalkers and Their Victims*”, Cambridge University Press, ISBN 0521732417, 9780521732413.

Naudé, W. (2020) “*Artificial intelligence vs COVID-19: limitations, constraints and pitfalls*”, AI and SOCIETY. 35(1) doi: 10.1007/s00146-020-00978-0.

New Scientist (2017) “*Machines that Think: Everything you need to know about the coming age of artificial intelligence*”. New Scientist, ScienceDirect.

NIST (2020) “*Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*”, NIST 2020.

O'Flaherty, K. (2020) “*Zoom’s A Lifeline During COVID-19*: *This Is Why It’s Also A Privacy Risk*”. Forbes.

Olivier Antoine, et al (2013) “*ISO/IEC 27018: The Future Standard for Personal Data Protection in Public Cloud*”, EBRC (Cloud, Data Centre & Managed Services, Specialist), ICT solutions, Luxembourg.

Oliver, N., Barber, X., Roomp, K. and Roomp, K. (2020) “*The Covid19 Impact Survey: Assessing the Pulse of the COVID-19 Pandemic in Spain via 24 questions*”. Computers and Society. Cornell University.

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].

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&billTyp=B&billNbr=0601&pn=1791

Piotrowski, Chris; Lathrop, Peter (2012) “*College Student Journal*”, Volume 46, Number 3, 1 September 2012, pp. 533-536(4), Project Innovation Publish.

Razavi Amir H.; Inkpen Diana; Uritsky Sasha and Matwin Stan (2010) “*Offensive Language Detection Using Multi-level Classification*” Publisher: Springer Berlin Heidelberg.

Reyns, Henson et al. (2011) “*Being pursued online applying cyberlifestyle–routine activities theory to cyberstalking victimization*”. Criminal Justice and Behavior, 38(11), pp. 1149-1169.

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

Sakul-Ung, P. and Smanchat, S. (2019) “*Towards Privacy Framework in Software Development Projects and Applications: - An Integrated Framework*”. Faculty of Information Technology King Mongkut’s University of Technology IEEE, pp. 1.

Salimi, E. and MansourabadI, A. (2014) “*The criminology of cyber stalking: investigating the crime, offenders and victims of cyber stalking*”. International journal of criminology and sociological theory, 7(2), pp. e39711- e39711.

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

Shimizu A. (2013) “*Recent development domestic violence in the digital age*”, Berkeley journal of Gender, Law and Justice. 28 (1).

Short Emma and Barnes Jim (2018) “*Cyberstalking*”, National Centre for Cyberstalking Research (NCCR), 2018 Conf. of UoB.

Sydow, L. (2020) “*Video Conferencing Apps Surge from Coronavirus Impact*” | App Annie Blog. https://www.appannie.com/en/insights/market-data/video-conferencing-apps-surge-coronavirus/ [Accessed: 18/10/2020].

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

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]

UK Legislation (1984) “*Data Protection Act 1984–UK*”. The Official Home of UK Legislation. www.legislation.gov.uk [Accessed: 14/10/2020]