DATA PRIVACY COMPLIANCE AT THE DEPARTMENT OF EDUCATION DIVISION OF MABALACAT CITY

Alexis S. de Rama

College of Public Administration and Governance,
Tarlac State University

Abstract: This study determined the data privacy compliance at the Department of Education Division of Mabalacat City with focused on transparency, collection, technical security, organizational security, proportionality, physical security, data security, and legitimate purpose. Significant difference was also assessed. Problems and best practices with compliance to DPA were identified based on the assessment of the respondents. It involved the 26 Administrative Officers (AO) and 35 Administrative Assistants (ADAS). This study employed quantitative descriptive research design.

The study employed a quantitative descriptive research design. A total enumeration was utilized. The researcher used and adopted the Privacy Impact Assessment. The survey questionnaire is tailored from the National Data Privacy Commission Toolkit (2018). Data were obtained physically after approval from the proper authorities.

The results of assessment as to compliance of the respondents with the Data Privacy Act (DPA) of 2012 across all aspects of DPA revealed compliant levels. Moreover, assessment showed no significant difference. Problems encountered are: insufficient data, privacy plans, insidious issues in the digital sphere, purging older data and materials, presence of hackers, dangers of additional devices, bolster data privacy plans, insufficient Standard Operating Procedures, data hoarding, duplicate files, and disable location tracking. Best Practices

identified are: perform data discovery, control access, encrypt data, install anti-malware software, perform assessment and audits, have a data usage policy, physically safeguard data, create strong password, eliminate data, and educate on the sign of phishing.

Recommendations to monitoring systems and processes should be established to make it standardize and dissemination is effective. Seminar/Trainings and other similar activities should be conducted among the Administrative Officers and Administrative Assistants to combat the problems thru online activities and record keeping. Identified best practices should be maintained and enhanced more for efficiently serving clienteles and stakeholders. The proposed action plan may be religiously implemented, note the progress or development of Administrative Officers and Administrative Assistants' compliance. Seek technical assistance among experts in the field like the Chiefs of the Units and veteran employees of equal rank.

I. INTRODUCTION

Increasing globalization, coupled this year with the impact of the COVID-19 pandemic, has driven a significant focus on existing data privacy rules across the Asia Pacific region. For businesses operating in the Asia Pacific region, it is imperative to know how to navigate a diverse set of privacy and data protection regulatory and legislative requirements (The Asia Pacific Privacy Guide 2021).

Data privacy was a normal thing in the past. However, it has become a very critical issue with time. Data Privacy is now given attention at the global, national, and local levels. Relatively, every country has enacted some sort of data privacy laws to regulate how information is collected, how data subjects are informed, and what control a data subject has over his information once it is transferred.

Data is growing faster than ever. More than 1.7 megabytes of new data is created every second. Organizations must keep up with protecting not only their customer's personal information but also sensitive personal information. Breach Level Index, a public tracking site for data breaches, reports nearly 9,198,580,293 data records are now lost or stolen since 2013.

Data has grown exponentially over the last decade, yet poor security practices continue to put organizations at risk of a data breach. Personal Identifiable Information (PII) is one of the biggest concerns in data privacy. Because of the veracity and volume of data in our technology-driven world, it becomes overwhelming to handle millions and possibly even billions of data records.

A data breach can cost organizations millions of dollars in lost revenue. In fact, the Ponemon Institute found that the total average cost of a breach cost in 2017 was $3.62 million. What's more is that there is a 30% chance for an organization to experience a data breach over the next two years. If an organization is breached, they face intense regulatory penalties from an array of entities. For example, companies operating in or with customer data in the European Union that experience a sizable breach from a lack of security controls could face up to 4% of Adjusted Gross Revenue or €20 Million (whichever is greater).

Data privacy is a global issue. Gartner predicts the worldwide information security market will reach $170.4 billion in 2022 as companies globally respond to increasing threats. Some countries are more affected than others though, and the United States is among the worst hit. Internet-connected computers are attacked every 39 seconds in the US and 45 per cent of Americans have had their personal information compromised by a data breach in the last five years. In 2019, the US had the highest average cost per data breach in the world, at $8.64 million, and healthcare data breaches alone affected 40 million people—a number that's growing with the ongoing COVID-19 pandemic. The US still does not have a national consumer privacy law, despite ongoing efforts to enact one, particularly in light of trailblazing regulatory advances in California.

The picture is similar in the United Kingdom where the cost per data breach is slightly lower than the global average but 88 percent of companies have been caught up in a breach, mostly phishing attacks. High levels of data breach are also reported in nearby Germany (92 percent), France (94 percent), and Italy (90 percent). Small UK businesses suffer an attempted hacking attack every 19 seconds, and nearly 40 percent of UK companies reported a data breach in the 12 months to May 2020.

In Australia, seven in 10 respondents to the Australian Community Attitudes to Privacy Survey 2020 by the Office of the Australian Information Commission (OAIC), nominated privacy as a major concern for them, while 87 per cent wanted more control and choice over the collection and use of their personal information.

Data Privacy or Information privacy is a part of the data protection area that deals with properly handling data, focusing on compliance with data protection regulations. Data Privacy is centered around how data should be collected, stored, managed, and shared with any third parties and in compliance with the applicable privacy laws.

While the public may be concerned with maintaining their digital identity, businesses especially small and medium businesses and other organizations, need to consider data privacy as a priority to determine their success moving forward.

Any organization that wants to work effectively needs to ensure the safety of its information by implementing a data protection plan. Ultimately, data protection's fundamental principle and importance are safeguarding and protecting data from different threats and under different circumstances.

According to the National Law Review, 65 percent of the world's population will have its data covered under modern privacy regulations by 2023. This is a massive jump up from 10 percent in 2021, indicating the priority governments worldwide place on data privacy.

Privacy International (2017) defined privacy as a fundamental right, essential to autonomy and the protection of human dignity, and serves as the foundation upon which many other human rights are built. Finn et. al (2013) proposed that there are different types of privacy which include privacy of the person, privacy of behavior and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association. From the proposed types of privacy, it can be gleaned that one important aspect of it is relevant to data protection.

In the case of the United States of America, despite numerous proposals over the years, there is no one comprehensive federal law that governs data privacy in the U.S., yet they have a new proposed federal privacy law, the American Data Privacy Protection Act (ADPPA), that has made it further than any of its predecessors.

According to the Transformation of the Privacy Landscape in Asia (2021), the data privacy landscape in Asia (East, Central, and South) and the Pacific has undergone a dramatic transformation in the past decade and all indications are that the region's privacy rules will continue to change at an equally rapid pace into 2021 and

beyond.

In 2021, China's Personal Information Protection Law (PIPL), is the first comprehensive law on personal information protection. Private personal information is protected as a right of privacy under the Civil Code, and individual rights in personal information, private or public, are protected under the PIPL. Data security, including data that are not personal information, and cybersecurity are regulated under the Data Security Law and Cybersecurity Law, which along with the PIPL form China's data privacy and security legal regime ("A comparison of data protection laws," 2022).

India is no exception – and is also making efforts on this front. Currently, this space is regulated by the Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Section 43A of the IT act entitles a data principal to seek compensation for unauthorized disclosure of sensitive personal information. Section 72A is the penal provision under which a person, including an intermediary who discloses sensitive personal information without consent, can be punished with imprisonment or a fine.

The Deloitte Asia Pacific Privacy Guide, now in its third edition (2020-2021), identifies specific privacy and data protection laws, regulations, and amendments in each of the Asia Pacific locations we cover, including the Philippines, and outlines six important privacy and data security trends.

These instruments stipulate a more specific right to the protection of personal data. Data privacy is a citizen's right to control how their personal information is collected and used. Data protection is a subset of privacy.

Through these instruments, privacy enables people to create barriers and manage boundaries to protect themselves from unwarranted interference in their lives, allowing them to negotiate who they are and how they want to interact with the world. Privacy helps people establish boundaries to limit who has access to not just their bodies, places and things, but their communications and their information (Privacy International, 2017).

In 2012 the Philippines passed the Data Privacy Act of 2012 which is described as a comprehensive and strict privacy legislation to "protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth." (Republic Act. No. 10173, Ch. 1, Sec. 2). The Implementing Rules and Regulations of the law is also in force and it serves as basis of both public and private institutions on how they manage the data that they are handling from their stakeholders. The main goal of having this law and its IRR is to protect people's privacy.

The Philippine data protection law imposes a series of requirements and compliance designed to protect individuals against the risks resulting from processing personal data.

The Republic Act No. 10173 of the Philippines or the Data Privacy Act of 2012 is a law that aims to protect individual's personal information in information and communications systems in both the government and private sectors that was approved on August 15, 2012, which is composed of nine chapters and 45 sections 12. Moreover, its Implementing Rules and Regulations (IRR) was promulgated on August 24, 2016. The Implementing Rules and Regulations (IRR) shall cover all the mandated functions and duties of the Philippine Competition Commission to facilitate the

implementation of the provisions of Republic Act 10667, otherwise known as the Philippine Competition Act.

Through its data privacy policy at the national and regional levels, Department of Education aims to comply with the requirements of Data Privacy. Relatively, the researcher is a present Administrative Officer II in one of the elementary schools in Mabalacat City Schools Division. One of the duties and responsibilities of an Administrative Officer is to secure data and comply with the existing laws with regards to data privacy act compliance. In view of these contentions, this study assessed the compliance with the Data Privacy Act of Mabalacat City Schools Division in terms of transparency, collection, technical support, organizational structure, proportionality, physical security, data security, and legitimate purpose. Moreover, problems encountered and best practices in relation to the study were identified. From the results of the study, action plan is proposed and implications were drawn.

STATEMENT OF THE OBJECTIVES

Generally, the study assessed the compliance, problems encountered and best practices with the Data Privacy Act of 2012 of the Mabalacat City Schools Division.

Specifically, it answered the following questions:

1. How is Data Privacy be described and evaluated based on assessment of the Administrative Officers and Administrative Assistants in terms of:
   1.1 Transparency;
   1.2 Collection;
   1.3 Technical Security;
   1.4 Organizational Security;
   1.5 Proportionality;
   1.6 Physical Security;
   1.7 Data Security; and
   1.8 Legitimate Purpose?
2. Is there a significant difference between Administrative Officers and Administrative Assistants' assessment relative to the extent of compliance with the Data Privacy Act of 2012?
3. What are the problems encountered by the Administrative Officers and Administrative Assistants relative to compliance with Data Privacy Act?
4. What are the best practices of the Administrative Officers and Administrative Assistants to keep abreast with the Data Privacy Law?
5. What action plan may be proposed based on the findings?
6. What are the implications of the study to Public Administration?

SCOPE AND DELIMITATION

Generally, the study aims to assess the extent of compliance with the Data Privacy Act of 2012 of the Mabalacat City Schools Division. The study's respondents comprised of Administrative Officers and Administrative Assistants from the Mabalacat City Schools Division. This study was conducted for the School Year 2022-2023 in Mabalacat City Schools Division.

It was further delimited to the following: the compliance with the Data Privacy Act of the Division of Mabalacat City along with the following key items: Transparency; Collection, Technical Security, Organizational Security, Proportionality, Physical Security, Data Security, and Legitimate Purpose. The difference between the Administrative Officers' and Administrative Assistants' assessment relative to the extent of compliance with the data privacy act of 2012. Moreover, the challenges or problems encountered by the Administrative Officers and Administrative Assistants in relation to compliance with the data privacy act and the best practices of the school personnel to keep abreast with the data privacy law. Finally, the outcome of this paper is a proposed action plan to further improve the implementation
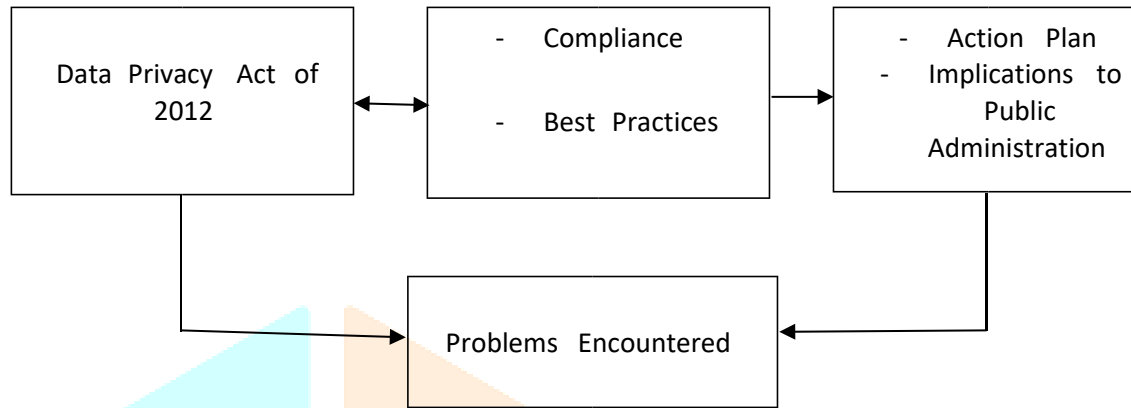
of the data privacy act in the Division Office and implications were also drawn from the results of the study.

CONCEPTUAL FRAMEWORK

Data Privacy in general is very subjective and means different things to different people. Common among all interpretations is the perspective that it is a human right but is context and environmentally dependent.

Figure 1 shows the paradigm of the study.

```
┌─────────────────┐      ┌──────────────────┐      ┌──────────────────┐
│                 │      │  -  Compliance   │      │  -  Action Plan  │
│ Data Privacy Act│◄────►│                  │─────►│  -  Implications │
│    of 2012      │      │  -  Best         │      │     to Public    │
│                 │      │     Practices    │      │   Administration │
└─────────────────┘      └──────────────────┘      └──────────────────┘
         │                                                    │
         │               ┌──────────────────┐                │
         └──────────────►│    Problems      │◄───────────────┘
                         │   Encountered    │
                         └──────────────────┘
```

II. RESEARCH METHODOLOGY

RESEARCH DESIGN

This study on the level of compliance with data privacy act of Mabalacat City SDO utilized quantitative descriptive research design. Quantitative descriptive research is a quantitative research method that attempts to collect quantifiable information for statistical analysis of the population sample. It is a popular market research tool that allows us to collect and describe the demographic segment's nature. It is quantitative in nature as it attempts to collect information and statistically analyze it. This research type is a powerful research tool that permits a researcher to collect data and describe the demographics of the same with the help of statistical analysis. Thus, it is a quantitative research method.

Quantitative descriptive research refers to the methods that describe the characteristics of the variables under study. This methodology focuses on answering questions relating to the "what" than the "why" of the research subject. The primary focus of this research is to simply describe the nature of the demographics understudy instead of focusing on the "why". It is called an observational research method as none of the variables in the study are influenced during the process of the research.

LOCALE OF THE STUDY

The study was conducted in the Division of Mabalacat City. Mabalacat, officially known as the City of Mabalacat (Kapampangan: Lakanbalen ning Mabalacat; Tagalog: Lungsod ng Mabalacat), is a 3rd class component city in the province of Pampanga, Philippines. According to the 2020 census, it has a population of 293,244 people (Census of Population, 2020).

Mabalacat has a land area of 83.18 square kilometres (32.12 sq mi). It is 93 kilometres (58 mi) from Manila, 10 kilometres (6.2 mi) from Angeles, and 27 kilometres (17 mi) from the provincial capital, San Fernando. It politically subdivided into 27 barangays.

Figure 2 shows the geographical location of the study.

Figure 2. Mabalacat City Map

RESEARCH INSTRUMENT

With anobjective to gather the needed data on the compliance of Administrative Officers and Administrative Assistants with the Data Privacy Act, the researcher used and adopted the Privacy Impact Assessment. The survey questionnaire is tailored from the National Data Privacy Commission Toolkit (2018).

Part one of the questionnaire includes the extent of compliance with the Data Privacy Act of 2012 in terms of the eight key items referring to Transparency, Collection, Technical Security, Organizational Security, Proportionality, Physical Security, Security of Personal Data, and Legitimate Purpose.

Part two of the instrument is dedicated to explore the problems encountered in implementing the data privacy law and the best practices to keep abreast of the provisions of the said policy.

DATA GATHERING PROCEDURE

The researcher asked permission to conduct the study from the Office of the Schools Division Superintendent of Mabalacat City. After that, the researcher built and provided a plan of action for the actual data collection procedure using various social media online and offline platforms. Personal communications from the researcher were sent to the respondent via various social media outlets. The respondents were able to discuss the tools with the researchers via the internet. The respondents' time and effort were much appreciated. The online survey was sent using Google Forms.

The researcher conducted face-to-face interview while adhering to ethical guidelines during the qualitative research process. The researcher provided informed consent before engaging in an interview. The researcher contacted the key informants regarding the purpose and intention of the interview.

Data Analysis

The gathered data were treated statistically using the following statistical techniques:

Weighted Mean. This was used to determine the extent of compliance with the data privacy act of the   division office. Further, the following scales will be used for interpretation.

T-test for Independent Samples. This tool was used to describe the difference in the assessments between the administrative officers and administrative assistants concerning the extent of compliance with the data privacy act of 2012.

Likert Scale. In describing the extent of compliance with the data privacy act with the following parameters.

Scale	Interval	Adjectival Rating
4	3.50 - 4.00	Fully Compliant (FC)
3	2.50 - 3.49	Compliant (C)
2	1.50 - 2.49	Moderately Compliant (MC)
1	1.00 - 1.49	Not Compliant (NC)

III. RESULT AND DISCUSSION

Table 1

Transparency as Assessed by the Administrative Officers and Assistants

Indicators	AO Mean	Adjectival Rating	ADAS Mean	Adjectival Rating	Weighted Mean	Adjectival Rating
Data subjects aware of the nature, purpose, and extent of the processing of his or her personal data.	3.04	C	3.06	C	3.05	C
Data subjects aware of the risks and safeguards involved in the processing of his or her personal data.	2.93	C	2.54	C	2.74	C
Data subjects aware of his or her rights as a data subject and how these can be exercised.	3.07	C	2.76	C	2.92	C

There is a document available for public review that sets out the policies for the management of personal data.	2.50	*C*	2.51	*C*	2.51	*C*
The steps in place to allow an individual to know what personal data it holds about them and its purpose of collection, usage, and disclosure.	2.52	*C*	2.33	*MC*	2.42	*C*
The data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data.	2.25	*MC*	2.49	*MC*	2.37	*C*
The data subjects provided information about how to contact the organization's Data Protection Officer (DPO)	2.21	*MC*	2.69	*C*	2.45	*C*
Grand Mean	2.65	*C*	2.63	*C*	2.64	*C*

Fully Compliant (FC), Compliant (C), Moderately Compliant (MC), Not Compliant (NC)

The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principle of transparency.

Transparency means the data subject must be aware of the nature, purpose, and extent of the processing of personal data, including the risks and safeguards involved, the identity of personal information controller, rights as a data subject, and how these can be exercised.

From the table above, it can be noted that out of seven indicators under transparency there are two indicators with means of 2.25 and 2.21, respectively interpreted as moderately compliant stating that the data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data and data subjects provided information about

how to contact the organization's Data Protection Officer (DPO). The first indicator of compliance with the Data Privacy Act of 2012 obtained a mean of 2.65 (compliant).

Moreover, data on the transparency as assessed by the Administrative Assistants. It can be noted that a weighted mean of 2.63 (compliant) satisfied the transparency of data among the Administrative Assistants. Differences, however, are shown or observed when compared to the assessment of compliance among Administrative Officers. Indicators five and six had 2.33 and 2.49 means interpreted as moderately compliant.

Wilbert, D (2018) explained data transparency affords readers access to the evidence or data used to support empirical research claims. This permits readers to appreciate the richness and nuance of what sources actually say, assess precisely how they relate to broader claims, and evaluate whether they have been interpreted or analyzed correctly.

According to the law, personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.

It can be noted that the first indicator stating that the collection of personal data for declared, specified, and legitimate purpose had a mean of 2.81 (compliant). This is followed by indicators stating individual consent is secured prior to collection and processing of personal with a mean 2.96 (compliant); consent time-bound in relation to the declared, specified, and legitimate purpose with a mean of 3.04 (compliant); consent is withdrawn at 3.23 (compliant) mean; ; all the personal data collected necessary for the program with 3.35 mean (sometimes compliant); personal data anonymized or de-identified with a mean of 3.04 (compliant); collection of personal data directly from the individual with 3.0 mean (compliant); necessity to assign or collect a unique identifier to individuals to enable your organization to carry out the program at 2.69 mean (compliant); there is authority for collecting personal data about the individual from other sources with a mean of 3.0 (compliant); and necessity to collect a unique identifier of another agency at 2.81 mean (compliant). A grand mean of 3.00 interpreted as compliant signaled that collection of data following the required protocols are being complied.

Table 2

Collection as Assessed by the Administrative Officers and Assistants

Indicators	AO Mean	Adjectival Rating	ADAS Mean	Adjectival Rating	Weighted Mean	Adjectival Rating
The collection of personal data for a declared, specified, and legitimate purpose.	2.81	C	2.89	C	2.85	C
Individual consent secured prior to the collection and processing of personal data. If no, specify the reason.	2.96	C	3.09	C	3.02	C
Consent time-bound in relation to the declared, specified, and legitimate purpose.	3.04	C	3.14	C	3.09	C
Consent is withdrawn.	3.23	C	3.20	C	3.22	C
All the personal data collected necessary for the program.	3.35	C	3.40	C	3.37	C
Personal data anonymized or de-identified.	3.04	C	3.17	C	3.10	C
The collection of personal data directly from the individual.	3.00	C	2.74	C	2.87	C
There is authority for collecting personal data about the individual from other sources.	3.08	C	3.17	C	3.12	C
Necessity to assign or collect a unique identifier to individuals to enable your organization to carry out the program.	2.69	C	3.20	C	2.95	C

Necessity to collect a unique identifier of another agency. e.g. SSS number, PhilHealth, TIN, Pag-IBIG, etc.,	2.81	*C*	3.00	*C*	2.90	*C*
Grand Mean	3.00	*C*	3.10	*C*	3.05	*C*

Fully Compliant (FC), Compliant (C), Moderately Compliant (MC), Not Compliant (NC)

Table 2 also explicates the data on the collection of data as assessed by the Administrative Assistants. A grand mean of 3.10 (compliant) obtained by the Administrative Assistants is somewhat higher compared to the grand mean of 3.0 (compliant) obtained by the Administrative Officers.

In Data Privacy Act of 2012, general principles in collection, processing and retention is stated. Collection must be for a declared, specified, and legitimate purpose. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

3.2 Issues and Concerns

Table 3.2 Issues and Concerns Involving Information Dissemination

Statements	*F*	R
Lack of service vehicle for District Public Affairs and Information Unit	56	1
Absence of support and assistance from top management for District Public Affairs and Information Unit	45	2
Insufficient budget allocation for District Public Affairs and Information Unit	36	3
Non- active participation of the stakeholders of District offices	29	4
Delayed releasing of information gathered by the District Public Affairs and Information Office	18	5
Non- participation of the District Public Affairs and Information Unit in the information dissemination process	7	6
Non -implementation of policies regarding information dissemination	2	7

It shows in the table that mobilization of District Public Affairs and Information Unit got the highest frequency 56 that ranks 1. Respondents claimed that there is lack of service vehicles for Information Staff. Without service vehicles, it would be impossible for the information staffs to document all the programs and projects of their respective districts to promote transparency among them and their stakeholders. Then followed by the Absence of support and assistance from top management for District Public Affairs and Information Unit got a frequency of 45 ranks number 2. There is insufficient support from top management for the District Public Affairs and

Information Unit of their respective District Offices. These concerns reveal that the top management does not provide ample support for the Information Offices in promoting proper procedure in the information dissemination.

Third in the rank is the statement that there is insufficient budget allocation for District Public Affairs and Information Unit got a frequency of 36 wherein there was no ample budget to cascade and provide the stakeholders the correct information that they ought to have. Then followed by the non-active participation of the stakeholders in the district offices got a frequency of 29 that ranks number 4. Stakeholders' participation with the District's Information Dissemination Process is a part of every agency's development in terms of information cascading process.

Then the fifth in the rank is the delayed release of information gathered by the district public affairs and information unit got a frequency of 18. Another concern of the respondents is the timeliness of the release of the information that was gathered by the information staff for the consumption of the stakeholders of the respective district offices. Then followed   by the non-active participation of District Public Affairs and Information Unit in the information dissemination process got a frequency of 7 ranks number 6. Participation of the information staff also affects the information dissemination process if the district offices. Lastly, the non-implementation of policies regarding information dissemination process got a frequency of 2 ranks number 7.

3.3 Intervention Measures

Table 3.3 Intervention Measures

Statements	*f*	R
Increase support from top management for information dissemination	63	1
Provide sufficient budget allocation for District Public Affairs and Information Unit	56	2
Further improve the process of gathering and dissemination of information	21	3
Coordination with the Regional and Central Office regarding the proper guidelines of Information Dissemination Process	11	4
Coordination with all implementing office regarding the guidelines of information dissemination process	11	4
Information Dissemination Process should be strictly in accordance with the Implementing Guidelines	6	6

It shows in the table that increase support from top management for information dissemination got the highest frequency of 63 that ranks 1. Respondents claimed that the support from top management for the District Public Affairs and Information Unit is needed to further enhance the process of information dissemination. It is essential for the top management to support their respective information unit because the latter is the one in charge of providing credible information to the public.

Then followed by provide sufficient budget allocation for District Public Affairs and Information Unit with a frequency of 56 and ranks 2. It can be gleaned that Information Unit of each district offices need sufficient budget to gather information regarding the programs and projects of the said agency to provide the public with reliable information that they deserve. Such budget allocation for information unit shall be used for gathering, preparing and cascading the information for public consumption. Then the third in the rank with a frequency of 21, stated that further improve the process of gathering and dissemination of information. Respondents thinks that the information unit shall always be develop since there is always an innovation and demand from the public with regards to the information that they need. Information Unit shall always base their process on the demand of their respective stakeholder.

It is then followed by coordination with the implementing office within the district level as well as with the Regional and Central office regarding the proper guidelines vof information dissemination process with a frequency of 11 and rank 4. Respondents also claimed that coordination by the Information Unit with other section within the district office as well as the Regional Public Affairs and Information Office and stakeholders Relation Services at the Central office of DPWH. Information Officers cannot work alone without coordination with other section within the district due to the fact that supporting document or information may be provided by them such

as information or data about the infrastructure projects by the district office. Moreover, upon gathering credible data in the district level, it is necessary for the district public affairs information unit to coordinate with Regional Public Affairs and Information Office as well as the stakeholder's relation services at the Central Office for proper documentation of all the communications being cascaded in the district level. Regional and Central Offices shall also have a record of the information being dissemination in the district level. Lastly, with a frequency of 6 and rank 6 state that information dissemination process should be strictly in accordance with the implementing guidelines.

IV. ACKNOWLEDGEMENT

V. BIBLIOGRAPHY

Adaja, T.A and F.A, Ayodele (2013), ", vol. 21, no. 5, pp. 65-75.
https://files.eric.ed.gov/fulltext/EJ1269016.pdf

Akporhonor and Olise (2015) https://www.projectreserve.com/2020/01/professional-librarians-perception-of-social-media-as-tools-for-information-dissemination-in-selected-universities-in-edo-state.html\

Amerjaphil Louie A. Vidal, Elsie Valdes (2018).https://www.researchgate.net/publication/329780888_Factors_Affecting_Effective_Dissemination_of_Peace_and_Order_Ordinances_to_Punong_Barangays_in_Maria

Andrianaivo & Kpodar (2011); Delponte, et al., (2015).   https://core.ac.uk/download/pdf/188127383.pdf

Aral and Walker (2014) Bakshy et al. (2012)
https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1993&context=gscis_etd

Arthur, (2018).https://www.ijser.org/researchpaper/Implementation-of-Information-Dissemination-Policy-in-Central-Java-Province.pdf

Benkler et al., 2018; Madrigal, 2017). Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press*.

Black et al., 2017. https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-   la-communication-2019-2-page-103.htm

Boateng and Quan Liu (2014)
https://libres.uncg.edu/ir/uncg/f/H_Moorefield_Lang_Delivering_2017.pdf

Bradley, P. (2012). *Why librarians must use social media.* Retrieved fromhttp://www.slideshare.net/Philbradley/why-librarians-must-use-social-media

Cathy Mae D. Toquero,Karen Joy B. Talidong, (2020)https://onlinelibrary.wiley.com/doi/full/10.1002/hbe2.214

(Center,2016)..https://amity.edu/UserFiles/asco/journal/ISSUE45_6.%20Sushobhan.pdf

(Cheng, 2022). https://www.hindawi.com/journals/cin/2022/1746472/

Correia et al., (2014). The studies of Bakshy et al. (2012) and Steeg and Galstyan (2012)https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1993&context=gscis_etd

Cui Jiangning (2015).https://gvpress.com/journals/IJMUE/vol10_no3/33.pdf

De Angelis, Gino; Davies, Barbara; King, Judy; McEwan, Jessica; Cavallo, Sabrina; Loew, Laurianne; Wells, George A; Brosseau, Lucie (2016-11-30)https://worldwidescience.org/topicpages/t/technology+information+dissemination.html

Educational,Technology. http://erepository.uonbi.ac.ke/bitstream/handle/11295/75594/Manyeki_Information%20and%20communication%20technology%20as%20a%20strategic%20approach%20in%20information%20dissemination%20at%20the%20Kenya%20forest%20research%20institute.pdf?sequence=3

Education in Kenya. Eldoret: University of Eldoret.http://erepository.uonbi.ac.ke/bitstream/handle/11295/75594/Manyeki_Information%20and%20communication%20technology%20as%20a%20strategic%20approach%20in%20information%20dissemination%20at%20the%20Kenya%20forest%20research%20institute.pdf?sequence=3

Edward K. Morris (2017). https://link.springer.com/article/10.1007/BF03391916

Fang, B., Jia, Y., Han, Y. et al. A survey of social network and information dissemination analysis. Chin. Sci. Bull. 59, 4163–4172 (2014). https://doi.org/10.1007/s11434-014-0368-5

(Gabriel Bazimaziki 2020). http://journal-repository.com/index.php/ijels/article/view/1971

Gray, E. (2013). ICT and Research Dissemination in African Universities. Centre for Guanghui Wang, Yufei Wang, Kaidi Liu and Jimei Li (2019) .https://doi.org/10.1142/S0217979219503752

Haiyan Wang1a, Liying Cao, *Research on Information Dissemination of Colleges and Universities based on PDCA algorithm* (2015)

Huang H,Zhao J, Zhang B. (2014). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098649 Higgins, K. (2016). Post-truth: A guide for the perplexed. Nature News, 540(7631), 9. https://doi.org/10.1038/540009a.

Ilaria Montagni, Will Stahl-Timmins, Lise Monneraud, Tobias Kurth (2019) https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2019 2-page-103.htm

Jude William Genilo (2017). https://link.springer.com/chapter/10.1007/978-981-10-7104-1_9

(Kwon, Angelo, & Mcleod, (2013), pp. 35–43) https://amity.edu/UserFiles/asco/journal/ISSUE45_6.%20Sushobhan.pdf

(Kellough & Hill, 2014; Larkin, (2013).

Larkin (2013), https://files.eric.ed.gov/fulltext/EJ1269016.pdf Liah Shonhe;   A Literature Review of Information Dissemination Techniques in the 21st Century Era

Li, Boying (2019). http://eprints.nottingham.ac.uk/59141/

Lorenzo, L (2012, July 7). The Evolution of Information Dissemination and its Consequences: The Mobile Learner. http://themobilelearner.wordpress.com/2012/07/07/the-evolution-of-informationdissemination-and-its consequences/http://erepository.uonbi.ac.ke/bitstream/handle/11295/75594/Manyeki_Information%20and%20communication%20technology%20as%20a%20strategic%20approach%20in%20information%20dissemination%20at%20the%20Kenya%20forest%20research%20institute.pdf?sequence=3https://files.eric.ed.gov/fulltext/EJ1269016.pdf

Lory Jean L. Canillo, Bryan G. Dadiz (2020). https://link.springer.com/chapter/10.1007/978-981-15-4409-5_73

Madrigal, A. C. (2017). What Facebook did to American democracy. The Atlantic. http://www.cs.yale.edu/homes/jf/MadrigalFeb2018-2.pdf

McQuail, (2011). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4039515/

Mcluban (2013) file:///C:/Users/DPWH/Downloads/1415-1-3925-1-10-   20220406.pdf

Moorefield-Lang (2017) https://www.ijlis.org/articles/awareness-and-use-of-social-media-platforms-for-information-dissemination-by-librarians-in-benue-state-schools-of-nursing.pdf. https://libres.uncg.edu/ir/uncg/f/H_Moorefield_Lang_Delivering_2017.pdf

Nalini Ratnasiri, (2015). https://files.eric.ed.gov/fulltext/EJ1269016.pdf

Nwachi & Igbokwe, (2019). https://www.ijlis.org/articles/awareness-and-use-of-social-media-platforms-for-information-dissemination-by-librarians-in-benue-state-schools-of-nursin.pdf

Omogor (2013) file:///C:/Users/DPWH/Downloads/1415-1-3925-1-10-20220406.pdf

Pickard, V. (2016). *Media failures in the age of Trump. The Political Economy ofCommunication*,4(2).http://polecom.org/index.php/polecom/article/viewFile/74/264.

Pin-Yu Chen; Shin-Ming Cheng; Kwang-Cheng Chen, (2014) https://ieeexplore.ieee.org/abstract/document/6755465

Pitkanen, S. (2013). Strengthening ICT-supported Community-Engaged Forestry

Pol&Lim,(2013).https://dspace.uii.ac.id/bitstream/handle/123456789/12613/05.%202%20Chapter%20 2.pdf? Sequence=7&isAllowed=y#

Rachit Agarwal, (2013). https://tel.archives-ouvertes.fr/tel-00919417/file/AGARWAL_Rachit-2.pd.

S. Panichpapiboon and W. Pattara-atikom, (2011). "A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks," I n IEEE Communications Surveys & Tutorials, vol. 14, no. 3, pp. 784-798, Third Quarter 2012, doi: 10.1109/SURV.2011.070711.00131.

Sahu, (2013). https://www.projectreserve.com/2020/01/professional-librarians-perception-of-social-media-as-tools-for-information-dissemination-in-selected-universities-in-edo-state.html\

Selwyn, N. (2012). Face working: exploring students' education-related use of Facebook." Learning, Media and Technology, vol. 34, no. 2, pp.157-174. https://files.eric.ed.gov/fulltext/EJ1269016.pdf

(Shonhe, 2017). https://digitalcommons.unl.edu/libphilprac/1731/

Shuai XuEmail authorYucheng Dong, (2013). https://link.springer.com/chapter/10.1007%2F978-3-642-40078-0_19   (Statista Inc, 2016). https://amity.edu/UserFiles/asco/journal/ISSUE45_6.%20Sushobhan.pdf

Tofi, S.T., Tondo, R.I., Ugba, T. &Akaaimo, G.T. (2019). Perceived benefits of marketing library and information resources and services using social media platforms. Benue Journal of Library, Management and Information Science (BJLMIS), 9(1): 91-107.

(World Bank, 2012). http://erepository.uonbi.ac.ke/bitstream/handle/11295/75594/Manyeki_Information%20and%20 communication%20technology%20as%20a%20strategic%20approach%20in%20information% 20dissemination%20at%20the%20Kenya%20forest%20research%20institute.pdf?sequence=3

Writing for Success (2015). *Strategies for gathering reliable information*. http://open.lib.umn.edu/writingforsuccess/chapter/11-4-strategies-for-gathering-reliable-information/

Wylie (2014) https://files.eric.ed.gov/fulltext/EJ1269016.pdf

Xie, I. & Stevenson, J. (2013). Social media application in digital libraries. OnlineInformation Review, 38(4): 502-23. DOI.10.1108/OIR-11-2013.

Zhang, N.; Huang, H.; Su, Boni (2016-11-01) https://worldwidescience.org/topicpages/t/technology+information+dissemination.html