National Government Agency's Compliance on Data Privacy Act of 2012 a Case Study

V Pitogo¹,²

¹ College of Computing and Information Sciences, Caraga State University, Butuan City, 8600 Philippines
² De La Salle University, Taft Avenue, Manila, 1004 Philippines

Abstract. The Republic Act (RA) No. 10173 of the Philippines, or also known as "Data Privacy Act of 2012" (DPA of 2012) was established to protect and to safeguard the individual personal data in an information and communications systems within the government and the private sector while keeping the fundamental human right to privacy of communication. The creation of the National Privacy Commission (NPC) as an independent body mandated to administer the DPA of 2012; to monitor and to ensure compliance with privacy, and to provide proper data protection procedures. This empirical qualitative research using case study approach aims to discover and describe why and how the country’s frontline agency (Agency A) complies with DPA of 2012. This paper also seeks to determine the challenges and better practices encountered by the agency relative to compliance and how far the level of commitment does Agency A has taken on. Results further showed that Agency A is Partially Compliant with the Act. It also encountered some challenges such as (a) lack of awareness, (b) wait-and-see attitude, and (c) time and resource constraints. Determinants of compliance like: (i) general deterrence, (ii) legitimacy of regulations, and (iii) reputation and publication had a compelling casual factor why it has conformed to the law. It is further recommended to conduct a follow-up study once the recent Information Systems Strategic Plan (ISSP) is available, vis-à-vis to March 8, 2018, extended deadline.

1. Introduction

Most of the government agencies and national institutions promote good democratic governance by providing transparent and accountable civic information based on the collected data from its citizens [1]. Thus, collection, provision, and sharing of such information must be appropriately taken to safeguard and protect the privacy of each. Data protection and privacy have been in decades of great concern [2] as to how security and data proliferation must be appropriately shared, accessed and mostly, protected. Said matter will have an increasing impact especially in this present digital society wherein the onslaught of information technology has rapidly change civilization [3].

At random across the global arena, countries, and organizations tries to create provisions, laws, and even amendments for the protection of personal information [4]. In the European Union (EU), Data Protection Authorities (DPAs) is an independent body with a principal role about data privacy and protection [5] which legally enforces a binding commitment on data privacy and security. While the General Data Protection Regulation (GDPR), also a regulating body that monitors and enforces action with matters to data protection amongst organizations including private institutions [6] on which, on the other hand, plays a vanguard of the data privacy regulation, and recognizes compliant entities [7].

The Philippines is also an adopting country in safeguarding the citizens’ personal information by establishing the Republic Act (RA) No. 10173 or also knows as “Data Privacy Act of 2012” (DPA
of 2012). Creating the National Privacy Commission (NPC) to promote, regulate, and monitor data privacy compliance of both government agencies and private institutions [8] benchmarked with international standards set for data protection [9] which patterned in the EU’s GDPR. With the existence of the said law, most of the government agencies and other private entities have not given utmost importance on the necessities of complying while others still on the process of crafting the essential measures as mandated in the act. And, only a handful of government agencies already fulfilled, such as the Commission on Higher Education (CHED) [8], the Bureau of Internal Revenue (BIR) [10] and partly, the infamous Commission on Election (COMELEC) [8], [10] viewed as an example of data breached that made the NPC more prudent in enforcing the regulation.

The country’s frontline agency (Agency A) in the provision of employment, labor workforce information, and services; protecting and promoting the welfare and interest of every citizen to work locally and globally [11] has harnessed its full potential in ICT infrastructure to ensure broader public access to information. Moreover, provide comfortable, convenient and efficient processes and further seeks to realize a system of governance that will lead to faster and better delivery of goods and services and providing proactive participation of citizens in management. It has numerous services offered to the Filipinos and collects and stores personal information. Thus, this paper assesses and provides empirical results on why and how does Agency A comply with the NPC requirements to DPA of 2012 amidst the March 8, 2018 deadline using qualitative research in a case study technique [12] and imploring outcomes pattern matching method in analyzing the extent of such compliance.

2. Literature Review

Internet, one of the technological breakthroughs changed the way businesses are conducted [13], it has also influenced human life significantly [14]; hence, information must be safeguarded to ensure privacy among individual and the organization. Regulatory authorities should be established to monitor and protect information and provide enforceable penalties for the offenders. In EU, they amended the General Data Protection Regulation (GDPR) and intended to address the pitfalls of the previous body and provide a way for companies to use certifications as part of their compliance framework [7]; and to harmonize the data protection across European Union. The Philippine has benchmarked its data privacy and security by drafting a provision and promulgate into a law.

2.1 Republic Act No. 8792 of the Philippines

R.A. 8792 also known as “e-Commerce Act of 2000” aims to facilitate domestic and international dealings, business transactions, arrangements, agreements, contracts, and exchanges and storage of information through the utilization of electronic, optical, and technology medium [15] to recognize the authenticity and reliability of the electronic documents, thus promoting the universal use of electronic transaction in the government and general public [10]. This law plays a very vital role in compliance with the DPA of 2012. Hence, data processing has been at the forefront of every government institutions, and thus, protection of information is a must.

2.2 Republic Act No. 10173 of the Philippines

The R.A. No. 10173 of the Philippines or also known as 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 enacted on August 15, 2012 [16]. More so, its Implementing Rules and Regulations (IRR) promulgated on August 24, 2016 [9].

2.3 The National Privacy Commission

The National Privacy Commission is Philippine's privacy watchdog; an independent body, mandated to administer the Data Privacy Act of 2012. It also monitor and ensure compliance of the country with international standards set for data protection; a regulatory and enforcement agency upholding the right to privacy and data protection while providing the free flow of information, committed to excellence, driven by a workforce that is highly competent, future-oriented, and ethical, towards a competitive, knowledge-based, and innovative nation[17]. Within this commission, the Data Privacy Accountability and Compliance Framework is born and summed up into five critical pillars: (1)
Appoint a Data Privacy Officer (DPO); (2) Conduct a Privacy Impact Assessment (PIA); (3) Develop a Privacy Management Program and Privacy Manual (PMP/PM); (4) Implement Privacy and Data Protection Measures (PDPM); and (5) Develop Breach Reporting Procedures (BRP) [17]. As detailed from the 2017 NPC Toolkit [17], the appointed DPO will be accountable in ensuring the compliance of the Personal Information Controller (PIC) and the Personal Information Processor (PIP). The PIA is a systematic description of a personal data flow and processing activities of the PIC and PIP [17]. While the PMP as "a holistic approach to privacy and data protection, important for all agencies, companies or other organization involved in the processing of personal data", and the Privacy Manual "serves as a guide or handbook for ensuring the compliance of an organization or entity with DPA of 2012" [17]. And lastly, the Breach Management includes the personal data breach notification and annual report on breaches and security incidents [17].

3. Research Question and Objectives of the Study
The primary objective of this research study is to assess the extent of compliance and level of commitment of Agency A to the Data Privacy Act of 2012. In relation, the main research question is how and why will the said frontline agency comply with the DPA of 2012?

To further answer and provide empirical results, specific research questions addressed:
1. What information systems processes which are in place that deals with personal data?
2. How does the agency align its business processes in conformance with e-Commerce Act of 2000?
3. What are the challenges and better practices that the agency had encountered in keeping abreast with DPA of 2012?
4. What are the determinants of compliance? Also, how these constructs affect the performance compliance of Agency A to DPA of 2012?

4. Methodology
The methodology used in this study is a qualitative case study research, that empirically investigates the bind or boundaries between a contemporary phenomenon and its real-world context [8], [18] or intensively studying phenomenon over time within its natural setting in one or a few sites [19]. Figure 1 represents the fullness of the case study.

![Case Study Model](image)

**Figure 1.** This case study model adapted from the work of Robert Yin's methodology use throughout this study.

4.1 Exploratory & Explanatory
This empirical study started at the planning phase, in which crafting of research questions are planned and designed. Thus, reflected in the primary research question, possesses the ‘how’ and ‘why’ questions, and focuses on contemporary events - makes it an *Explanatory* approach [20], while specific research inquiries with "what" questions are *Exploratory* - that is a justifiable rationale for exploratory study, hence, it is to describe the prevalence of a phenomenon [12].
4.2 Design  
In designing this paper, the unit of analysis was determined, thus, Agency A, as a single organization is the subject of inquiry and investigation. Since, there is only one (1) agency that is subject for the study (case), the researcher employed the single-case holistic design with common rationale, which is more fitting to the context of this work.

4.3 Preparation  
Part and parcel of this research paper are to provide the necessary authorization and protocol in conducting such case. All the needed tools, documents, records and other information that would assist in the proliferation of result and outcome are in-place. Crucial select personnel to be interviewed and checklist preparation also drafted.

4.4 Evidence Collection  
In relative to preparation, in this stage, the pieces of evidence collected were Documentation, Archived Records and Interview. The Information Systems Strategic Plan (ISSP) of the agency is the primary document for assessment in connection to the set standards of the DPA of 2012 compliance. Archived records aid in the evaluation of how the agency is conformance to e-Commerce Act of 2000 which is a must in complying with DPA of 2012. Interviewed some personnel of the agency that has director has a possible impact of the case study analysis; and analogous to their documents for data triangulation that helped strengthen the construct validity of the case [18].

4.5 Analysis  
In determining the constructs of compliance, the researcher used the work of Kagan [21] to validate the determinants of compliance towards DPA of 2012 as shown in Figure 2.

![Figure 2. Depicts the determinants of compliance from Kagan, this paper only utilizes a handful constructs for such case.](image)

Based on the evidence collected, just a handful constructs from the determinants of compliance model has compelling casual factors affecting the behavior of compliance of said agency, to list: (a) General Deterrence, (b) Legitimacy of Regulation, and (c) Reputation and Publicity.
Figure 3. Operational framework. From the determinants of compliance, a functional model is designed to capture the entire phase of the study.

Deterrence construct defined as a strategy that enforces punishment surpassing any economic gain from failing to comply with the required rules to promote industry compliance [22]. The legitimacy of Regulation is defined as the recognition and acceptance to a governing body, and are expected to comply regardless of its dictates [8], while Reputation and Publicity is a stigma associated with non-compliance and the damage that adverse publicity might have for the agency's reputation. The E-Commerce Act of 2000 of the Philippines would serve as a moderating variable towards DPA of 2012 compliance.

For analytic triangulations, an outcomes pattern matching model was used to match predicted patterns from empirical patterns [23] thus, presented the outcome as the level of compliance in Figure 4.

Figure 4. Empirical patterns draw from different sources of information, such as the ISSP, archived documents, from interviews and direct observation. As defined by Trochim and Yin, it is a technique wherein the predicted patterns compared with the empirical models [12], [23]. A set of patterns adapted from the works of Ching [8] in determining the level of compliance of the Agency A with DPA of 2012 presented in Table 1.
Table 1. There are four (4) expected outcome patterns, from Pattern A to Pattern D. The rightmost column depicts the possible outcome based on the triangulation coming from ISSP and the Five (5) Pillars of NPC as Fully Compliant, Partially Compliant, Low Compliant and Not Compliant. To get a Pattern A outcome, results of data triangulation from ISSP and Five Pillars of NPC must be both high while Pattern B ranges from medium-high compliance, if both sources are low level of agreement, then the outcome would be Pattern C. Pattern D results when there are no available or no applicable data to be assessed for compliance.

| Pattern   | ISSP  | Five (5) Pillars of NPC   | Outcome          |
|-----------|------|---------------------------|------------------|
| Pattern A | High | High                      | Fully Compliant  |
| Pattern B | High | Medium                    | Partially Compliant |
| Pattern C | Low  | Low                       | Low Compliant    |
| Pattern D | n/a  | n/a                       | Not Compliant    |

5. Results and Discussion

To answer the research question posed in number one (RQ1) asking for the information systems currently in use by the agency that deals with personal information, Table 2 provides the information.

Table 2. There are thirteen (13) significant systems of which some of these have sub-systems. All rows with a label of ‘Y’ deals with personal data. Additional information such as process owners or lead agency, internal and external users were also provided to reflect ownership and possible origin of personal information. Majority of the information systems of AGENCY A have the presence of personal data, this is due to the fact, that the agency is handling matters to labor, employment, or job assistance to most of the citizens.

| Information Systems (IS) | Presence of Personal Data |
|--------------------------|---------------------------|
| ISSP for 2012 - 2016     | Yes/ No                   |
| 1 Employment and Manpower Development IS | Y |
| 2 Labor Standards and Social Protection IS | Y |
| 3 Labor Relations IS | Y |
| 4 Policy and Operational Support IS | N |
| 5 Virtual Integrated IS | N |
| 6 Enhanced Phil-JobNet | Y |
| 7 SPES Information System | N |
| 8 Integrated Philippine Occupation on Demand and Supply | N |
| 9 Private Recruitment & Placement | Y |
| Lead Agency              | Internal Processor        |
| Bureau of Local Employment (BLE) | BLE |
| Bureau of Workers with Special Concerns (BWSC) | BWSC |
| Bureau of Labor Relations (BLR) | BLR |
| Office of the Secretary Planning Service, HRDS, BLES | |
| Planning Services (PS) | PS |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |
| Bureau of Local Employment (BLE) | ROs, POs, PESO |

| External Processor        | |
| PESO, JobNet              | |
| Employers’ Job Seekers, PWDs | |
| Employers, Aliens, Employees | |
| Employers, Job Seekers, PWDs | |
In with e-Commerce Act of 2000 that requires authentication, security, and reliability of documents sent in electronic format as stated in research question number 2 (RQ2), Agency A had already streamlined their processes and overhaul some of the existing information systems that are running on a cross-agency platform and web infrastructure.

An outcomes pattern matching was conducted to further analyze and assess the extent of compliance by triangulating empirical patterns against the predicted or expected trends. Figure 5 presents the results of the pattern matching.

As presented, Before the Enactment of DPA of 2012 and Before NPC Took Action, there were no evidence (n/a as Rating) as to how the agency is safeguarding the personal information used in their daily processes. While the presence of ISSP is Low in rating, this is because the agency has a handful of information that could be considered part of an ISSP resulted in a match of Pattern D with a similar outcome of Not Compliant.

During the Enactment of DPA of 2012 and After NPC Took Action in 2015, Agency A has already an Information Systems Strategic Plan (ISSP) for 2012-2016, this gives the agency a High rating on ISSP, which both present in documents and during the interview. For the NPC’s Pillar 1 – Appointment of a Data Privacy Officer (DPO) got a High rating on papers presented, however, during meeting the concerned personnel designated as the agency is trying to properly in-place human resources to handle matters on data privacy, this assesses a Medium rating.

For NPC’s Pillar 2 – Privacy Impact Assessment (PIA), Pillar 3 – Privacy Management Program and Privacy Manual (PMP and PM) and Pillar 4 – Privacy and Data Protection Measures (PDPM). All got a Medium rating on both sources of shreds of evidence (documents and interviews), this is because the agency had conducted a Privacy Impact Assessment but as not officially
implemented and reported to NPC for filing an action. For the Privacy Management Program and Privacy Manual, this is present, but not followed accordingly, and for the Privacy and Data Protection Measures, also present but no additional evidence as to how it has developed and ruled. For the last pillar, **Pillar 5 – Breach Reporting Procedures** with Low ratings on both sources, this is because, as stated that they perform breach reporting scheme, but no evidence to further support of the claim in case data breach will occur. The overall pattern matching on the latter event resulted in **Pattern B** with the similar outcome of Partially Compliant.

Also, **Agency A** had encountered some challenges and learned best practices along with its compliance with the law. First, the lack of awareness, though the regulation promulgated in 2012, still there is a need to fully inform all concerned agencies and entities on the mandate and its scope of compliance. Second, the wait-and-see attitude made the agency to less prioritize its requirements until one of the government agencies had an incident of data breach[8], [10] that made the NPC more prudent in enforcing the law. Third, time and resource constraints, the agency has limited resources. Hence, it is less priority concerning upgrade, and overhauling and would take much time in doing so, though, **Agency A** conducted a series of workshop and internal assessment of their processes and determined current information systems and applications that need re-engineering and development. Human resource is also a factor on why they were not able to conform to such regulation as earlier hence, there's a need for the agency to rearrange its current ICT organizational structure.

6. Conclusion
Based on the findings and pattern matching results, before enactment of DPA of 2012 and before NPC took action in 2015, **Agency A** is not compliant at all because of following concerns posed by said agency: first, the lack of awareness of said act hampers them in complying, second, they do not have the right people to focus on the matter, resources also forbids, and lastly, projects and programs relative to this is mostly on low priority agenda.

During the enactment of e-Commerce Act of 2000, the agency has already streamlined its services consonance with the law that made them more resilient in producing and complying with the Data Privacy Act of 2012. However, constraints, such as wait-and-see attitude hampers their compliance; the agency just passively feels its surrounding and co-agencies as to whom first submit and wait for the possible outcome, wherein NPC is very much strict with its guidelines and enforcement of the law. Second, time constraints are also a factor; the agency cannot further fast-phased its processes hence it cannot be done overnight and was also overlooked that such imposition of the law will not have a significant impact to the agency, which in return, it was. The identified constructs for the determinants of compliance has a compelling casual factor why **Agency A** comply with DPA of 2012. General deterrence poses possible legal sanctions and provisional penalties if there would be data breach occur in the agency and no proper documentation submitted to NPC before an unexpected event.

To sum, the agency is steadfast and committed to delivering services aligned to the data privacy, including its protection, access control, and security of personal data of its client with an aim to fully comply with the law in near possible time.

7. Future Works
Hence, during the conduct of this study, the available document reviewed and assessed covers only from 2012 – 2016 based on the agency's record. For this, the author further recommends conducting a follow-up study once the new and approved Information System Strategic Plan (ISSP) is available on how far the level of compliance does **Agency A** committed to achieving with Data Privacy Act of 2012 after the National Privacy Commission's set deadline on March 8, 2018.

8. References
[1] Altman M Wood A O 'brien DR Vadhan S and Gasser U 2015 Towards a Modern Approach To Privacy-Aware Government Data Releases *Berkeley Technol. Law J.* vol 30 no 3 pp 1967–2072.
9

[2] Bertot JC Jäger PT and Grimes JM 2010 Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies Gov. Inf. Q. vol 27 no 3 pp. 264–271

[3] Belanger F and Crossler R 2011 Privacy in Digital Age: A Review of Information Privacy Research in Information Systems MIS Q. vol 35 no 4 pp. 1017–1041

[4] Mansfield-Devine S 2017 Data governance: going beyond compliance Comput. Fraud Secur. vol 2017 no 6 pp. 12–15

[5] Barnard-Wills D Pauner Chulvi C and De Hert P 2016 Data protection authority perspectives on the impact of data protection reform on cooperation in the EU Comput. Law Secur. Rev. vol 32 no. 4 pp. 587–598

[6] Lachaud E 2016 Why the certification process defined in the General Data Protection Regulation cannot be successful,” Comput. Law Secur. Rev., vol. 32, no. 6, pp. 814–826, 2016.

[7] Lachaud E 2017 The General Data Protection Regulation and the rise of certification as a regulatory instrument Comput. Law Secur. Rev., no. August 2017

[8] Ching MRD Fabito BS and Celis NJ 2017 Data Privacy Act of 2012: A Case Study Approach to Philippine Government Agencies Compliance Soshum 2017

[9] NPC 2017 National Privacy Commission Toolkit: A Guide for Management and Data Protection Officers

[10] Celis NJ 2018 Compliance Theory: A Case Study Approach in Understanding Organizational Commitment DLSU Bus. Econ. Rev. vol 27 no 2 pp 88–118

[11] DOLE 2013 The Department of Labor and Employment [Online] Available: https://www.dole.gov.ph/pages/view/7.

[12] Yin R 2011 Case Study Research Design and Methods

[13] Biagi F and Falk M 2017 The impact of ICT and e-commerce on employment in Europe J. Policy Model vol 39 no 1 pp. 1–18

[14] Sohrabi Safa N Von Solms R and Furnell S 2016 Information security policy compliance model in organizations Comput. Secur. vol 56 pp 1–13

[15] Congress of the Philippines 2000 Republic Act No . 8792 AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC

[16] Congress of the Philippines 2012 RA 10173: Data Privacy Act of 2012

[17] NPC 2015 The National Privacy Commission [Online] Available: https://privacy.gov.ph/about-us/#visionmission [Accessed: 02-Mar-2018].

[18] Runfola A Perna A Baraldi E and Gregori GL 2017 The use of qualitative case studies in top business and management journals: A quantitative analysis of recent patterns Eur. Manag. J. vol 35 pp 116–127

[19] Bhattacherjee A 2012 Social Science Research: principles, methods, and practices vol 9

[20] Pitogo VA and Ching MRD 2018 Understanding Philippine National Agency’s Commitment on Data Privacy Act of 2012: A Case Study Perspective in Proceedings of the 2Nd International Conference on E-commerce, E-Business and E-Government pp 64–68

[21] Gunningham N Thorton D and Kagan RA 2005 Motivating Management: Corporate Compliance in Environment Protection Law Policy vol 27 no 2 pp 289–316

[22] Sutinen JG and Kuperan K 1999 A socio-economic theory of regulatory compliance Int. J. Soc. Econ. vol 26 no 1/2/3 pp 174–193

[23] Trochim W 1989 Outcome Pattern Matching and Program Theory.pdf Eval. Program Plann. vol 12 pp 355–366

Acknowledgments

VA Pitogo would like to acknowledge few individuals who had a significant contribution in conducting this study: to Prof. Michelle Renee D. Ching, for her delightful insight and extensive knowledge on the matter including tools and materials preparation necessary for this work. To the organization’s administration understry for allowing me to conduct evaluations and assessments of their documents and processes, and interview critical persons. Also, to the Almighty Father for always showers blessings, guidance, and aspirations to the researcher. Thank you everyone.