When What Is Lost Is Lost Forever
Data Privacy

The present is an interesting time to be alive. The “Kodak Moment” has been redefined from capturing and immortalizing memories on film to waking up the next day and seeing entire industries disappear. Social media (e.g., Twitter, Facebook, Instagram) allows people to (over)share details of their everyday lives; organizations and industries are built entirely on technology platforms and a “sharing” economy (e.g., AirBnB, Uber, Grab); pervasive electronic commerce allows anything to be bought online and delivered directly (e.g., Lazada, Zalora, Amazon, Food Panda). Technology and the willingness to share personal data makes this all possible. These online platforms collect, process and retain large amounts of personal data. More and more aspects of individuals’ personal lives are in the hands of third parties, anonymous individuals and those working behind corporate veils.

On the dark side, cases of personal information being lost or misused for marketing and even exploited for fraud and cybercrime are increasing. Large amounts of personal data can be exploited to initiate profiling and implement a surveillance economy, which also raises the risk of information leakage, cyberstalking and identify theft. The biggest issue here is that when personal information is lost, it is lost forever. Birthdays cannot be changed and neither can mothers’ maiden names. These are the most common security questions used by online portals.

On 25 July 2012, the Data Privacy Act of 2012 (DPA) was passed in the Philippines. This was the culmination of a long process of crafting legislation aimed at explicitly protecting the rights of data subjects aligned with the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. However, implementation of the rules and regulations and the appointment of the first commissioners of the National Privacy Commission (NPC) were only completed on 24 August 2016. What drove this sudden appointment and activity after nearly four years?

On 27 March 2016, the Philippine Commission on Elections (COMELEC) website was hacked. The COMELEC is the country’s election authority. Unfortunately, the website was connected to a database that contained more information than the website needed to expose over the Internet. It was later discovered that 340 total gigabytes of data were exfiltrated. This included information covering approximately 55 million registered voters. This information included the voter’s personal information (gender, civil status, birthday, birthplace, address, parent information, voting precinct details, biometric information, passport information of overseas voters), firearms registered during elections (make, model, owner details and serial numbers) and even the personal information of COMELEC employees. This was the largest data breach in the Philippines to date. The incident is now known as COMELEAK.

COMELEAK caused a sudden flurry of activity in the Philippines. Initially, data protection was primarily the concern of corporations trying to protect their corporate information and intellectual property. This was particularly true for business process outsourcing companies that protect their customers’ personal information. Since the incident occurred just a few months before the May 2016 election, it was especially disconcerting.

What was once the domain of the chief information officer (CIO) is now the concern of the entire organization. After incidents like this, data privacy is on everyone’s mind.

William Emmanuel Yu, Ph.D., CRISC, CISM, CISSP, CSSLP
Is senior vice president and chief technology officer at MDI (a 29-year-old systems integrator) and Novare Technologies. He is working on various projects involving mobility, web and telecommunications convergence. In his career, he has supported various customers such as Airtel, BPI, Delta, Globe, Shell, Smart, Thomson-West and Verizon. He is an active advocate of shaping Internet and technology policy, working with organizations such as the Internet Society, Philippine Computer Emergency Response Team (PH-CERT), Parish Pastoral Council for Responsible Voting (PPCRV), and the Philippine Department of Information and Communications Technology (DICT). He is a teacher at heart and continues to lecture at the Ateneo de Manila University (Philippines) and the Asian Institute of Management.
There has been a substantial increase in data protection awareness and data privacy issues. The COMELEAK incident received mainstream media coverage and is still relevant today.

The Implementing Rules and Regulation (IRR) of the Data Privacy Act\(^6\) was quickly released post COMELEAK. It was enacted in August 2016, more than four years after the DPA.

The majority of commerce portals and online sites have replaced their security questions since the incident. They now avoid asking for birthdays and mothers’ maiden names. In many cases, these commerce portals and online payment processors have rushed their implementation of multi-factor authentication (MFA) such as Short Message Service (SMS) challenge response, time-based one-time pad (TOTP), public key cryptography and others.

There has also been a surge of data protection officer (DPO) appointments in organizations. Not only is there a large increase in availability for this position, but many organizations also now wonder if the DPO role should be filled by the same person who acts as the chief information officer (CIO). With privacy issues now at C-suite level awareness, organizations are reviewing their data protection postures and contracting data privacy consultants for privacy impact assessments.

On 11 January 2017, another personal information breach befell the COMELEC. A computer at the COMELEC Office of the Election Officer (OEO) in Wao, Lanao del Sur was stolen.\(^7\) This computer, unfortunately, contained the National List of Registered Voters (NLRV) that contained the records of 55 million active registered voters. Fortunately for the COMELEC, these records were encrypted as part of the remedies recommended in the wake of COMELEAK. The National Privacy Commission (NPC) recommended that COMELEC henceforth ensure that full databases are not stored in systems where a full database is not required. However, COMELEAK2 points out another valuable lesson. Many privacy-related data breaches commonly involve personal data loss in portable computing assets such as laptops and mobile devices. There are many documented cases of this occurring, including at Oregon Health,\(^8\) Coca-Cola,\(^9\) Hartford Health,\(^10\) State of Georgia and Salvation Army in the SterlingBackCheck incidents,\(^11\) among many others. Further, many, if not most incidents, are probably not reported and documented. In fact, a study on US health care data breaches showed that 45 percent of breaches are due to lost laptops and other portable devices.\(^12\)

![Quote](https://via.placeholder.com/150)

> THE ENTIRE DATA PROTECTION LIFE CYCLE MUST BE CONSIDERED WHEN CREATING AND ENFORCING APPROPRIATE POLICIES FOR HANDLING ANY FORM OF DATA.

Some straightforward measures can be taken by organizations to mitigate the increasing risk to data protection, which, in turn, affects privacy:

- **Creation and enforcement of proper information governance and audits**—The entire data protection life cycle must be considered when creating and enforcing appropriate policies for handling any form of data. For example, the principle of least privilege must be applied. In the case of COMELEC, the regional or local offices do not need access to all the records in the national database. They only need access to their relevant subset. This could have substantially minimized exposure. With any policy measure, the proper creation and appointment of accountable parties and a review of all existing policies with the lens of data protection is necessary. These are not one-time events. These are constant review cycles.

- **Use of appropriate and proper controls**—There are many information technology solutions that
aid data protection. Some simple measures such as full disk encryption (FDE) are already available on all Android and Apple smartphones and some laptop operating systems. These simply need to be enabled. An often neglected, but equally important control is proper asset disposal. This is a key concern as both corporate and personal data can be harvested from devices that are improperly disposed or sent out for repair. The goal is to use the proper controls depending on the organization’s risk profile and appetite.

- **Perform regular and comprehensive user education**—At the end of the day, a large amount of personal data is handled by end users. A lot of jobs require access to this data and it can easily fall into the wrong hands if proper awareness is not present. The need to provide protection and privacy training is essential as with any information security program. This is an ongoing process and requires that everybody live and breathe information security and data protection.

As the world becomes more mobile and bring your own device (BYOD) becomes the norm,13 data leakage breaches involving stolen, lost or mishandled devices are expected to rise if proper measures are not taken. Addressing this is the first and most accessible step for most organizations.

Data privacy is a relatively new phenomenon. Previously, it was not as necessary since information was not as widely collected. Information was not shared as often and the ability to store and process information in today’s capacity did not exist. Today, personal information is widely distributed. Data for service is the new business model.

Additionally, data are no longer easily protected by the safety of a filing cabinet or vault. In the past, it was possible to keep information safe by physically securing it with padlocks and moats. Security professionals built a physical castle around the information. As technology progressed, data moved into the digital space. However, data continued to be protected with firewalls, intrusion prevention systems, and security solutions without data centers and premises. A digital castle was built around the information. Today, information is in cloud services, third-party service providers and other locations outside an enterprise’s own premises. Data are all over the Internet.

A key goal of data privacy is to ensure that personal information is protected and data subjects’ rights are respected. This is the key goal of data privacy legislation. COMELEAK caused the Philippines to rethink its data protection posture and has increased data privacy compliance measures. The country will never be the same. Do not wait for a COMELEAK-like incident to create the necessary awareness. Data security and data privacy are two sides of the same coin.

**Endnotes**

10 Ribiero, J; “EMC and Hospital to Pay $90,000 Over Stolen Laptop With Medical Data,” PC World, 9 November 2015, www.pcworld.com/article/3003052/emc-hospital-to-pay-90-000-over-stolen-laptop-with-medical-data.html
12 Santamaria, M; “45% of Healthcare Breaches Occur on Stolen Laptops,” digicert, 13 April 2016, https://www.digicert.com/blog/45-percent-healthcare-breaches-occur-on-laptops/