A Summary of the Study conducted by the Technology Law and Policy Program of the University of the Philippines Law Center[1] entitled "Enforcing the DPA through Administrative Fines: Some Economic Considerations"

The scope of the Study focuses on the imposition of administrative fines to deter certain violations of the Data Privacy Act of 2012 (DPA) involving various forms and degrees of negligence. This excludes criminal violations penalized under the DPA.

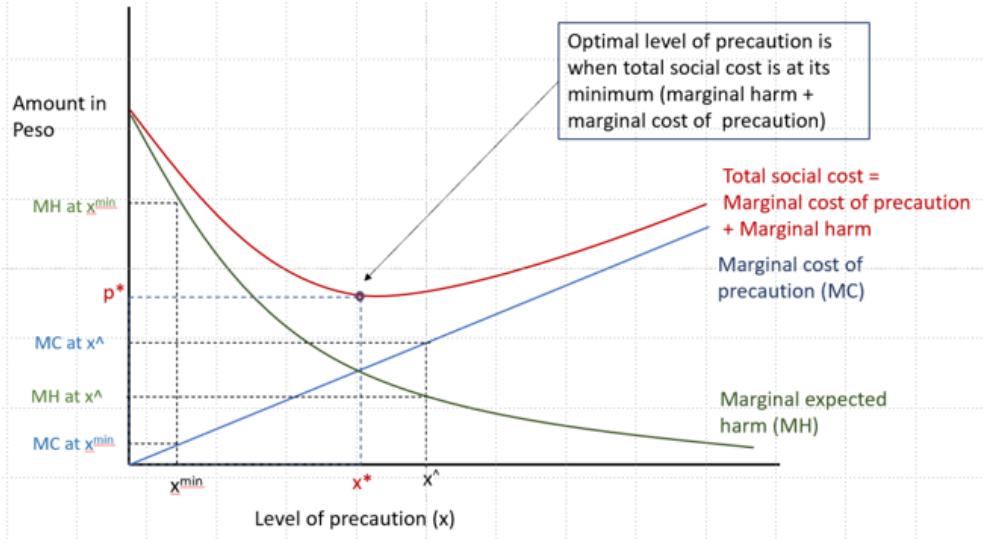
Personal information is now considered as a resource by most industries, and is increasingly developed for monetization. Personal data can be shared or used multiple number of times once disclosed. Further, consumers reap benefits of disclosing their personal data through lower costs of goods and services, or its wider availability and customization. At the same time, processing of personal data became more intensive due to the prospect of higher profits. This leads to the likelihood of abuse, theft, and violation of privacy rights.

The unauthorized access or use of personal data may be prevented or mitigated by the appropriate security measures. However, the adoption of measures requires corresponding costs for firms. Such additional cost gives little to no incentive for the firm to adopt sufficient measures to protect consumer's data.

The Study, based on existing literature that has guided other jurisdictions in optimal fine-setting, notes that as the level of precaution adopted by the firm increases, the marginal expected damage suffered by the consumer decreases. On the other hand, additional levels of precaution would require additional cost for companies. Ideally, from the point of view of society, the standard should be set such that the total social cost from consumer harm and precaution are minimized. The ideal is to set the fine and the standard optimally such that the total social cost from harm and precaution are minimized. The setting of the fines above the firm's cost of precaution is to incentivize them by internalizing the harm externalized to consumers. However, if a firm is risk-averse, they may overinvest in precaution, which would take away funding for other important resources of the company.

In order to analyze whether the administrative fines are "effective, proportionate, and dissuasive," the Study provided the graphical illustration and discussion points below:

[1]The Study Team includes members of the respective faculties of the University of the Philippines College of Law and the University of the Philippines School of Economics.



a. Data as a separate commodity has some characteristics of a public good: nonrival but excludable. Unauthorized access and use of data may be excluded using an appropriate technology, but it has an additional cost. The horizontal axis denotes the level of precaution, and the blue curve represents the firm's marginal cost of precaution, which is increasing with the level of precaution.

b. The harm from data breach is suffered by the consumers and is denoted by the green line. Without regulation or fines, there is no incentive for firms to incur the additional cost of taking precaution and the expected damage suffered by consumers from data breach is at its highest. Adopting the minimum level of precaution (x^{min}) would greatly reduce the marginal expected harm from data breach.

c. As the level of precaution adopted by the firm increases, the marginal expected damage suffered by the consumer decreases. On the other hand, the cost of additional level of precaution which correspond to the adoption of more sophisticated and more expensive technologies increases.

d. The optimal level of precaution is given by the lowest point in the total social cost curve, x*. At levels below it (x^{min}), the expected marginal damage can still be avoided at a lower additional cost to society. On the other hand, levels of precaution in excess of x* such as at x^ implies that the marginal cost society pays to avoid the expected marginal harm is now even higher.

With the given context, administrative fines can provide incentive for companies to adopt a reasonable or optimal level of data protection measures to comply with the Data Privacy Act of 2012 (DPA). Requiring a perfect compensation will motivate them to adopt x* rather than pay higher damages.

a. However, this relies on paying the damages *ex post*. When consumers are discouraged to file a suit against the firm for the harm that they suffered, then there

will be no incentives to adopt costly security measures to protect data. This may be due to (1) uncertainties in evidentiary standards required to assign blame and prove causality, (2) high transaction costs incurred when filing a suit, (3) lack of awareness about the extent of the damage, and (4) weak preference for privacy by the consumer.

b. Victims should be perfectly compensated if they cannot protect their data. The problem however is how to evaluate non-pecuniary losses or psychological harm suffered by victims of privacy breach. There are instances when the owners of data can also take precaution to protect themselves at a lower cost.

c. In some cases, owners of data can also take precaution at a lower cost (installing free software for instance). If the objective is to minimize total social cost, then they should also be incentivized to take precaution. Also, if owners of data can take care and they know they will be perfectly compensated and the amount can be very high (including non-pecuniary losses), this may encourage opportunistic behavior and filling of suits that may be extortionary in nature.

Imposing administrative fines can provide the *ex-ante* incentives to adopt the optimal or reasonable level of data protection. In adopting the corresponding threshold of precaution, firms may not be considered liable and avoid paying the fine.

a. Note that to deter, **the fine should at least be equal or larger than the cost of precaution at the optimal or reasonable level**. Otherwise, the firm would just rather pay the fine.

b. To account for the fact that not all violations are detected, then **the fine should be higher than the cost of precaution at the optimal level.** Generally, the lower the probability of detection, the higher should be the fine. Firms consider the expected fine when making decisions, not just the monetary amount of the fine.

c. As long as the legal standard is clearly identified and parties are risk neutral, any expected fine set above the cost of precaution at the optimal level of care would provide the proper incentives for firms to adopt the optimal level of data protection.

d. **However, if firms are risk averse, then they will overinvest in precaution, which from the point of view of society is also not desirable.** (1) The additional investment could have been allocated by the firm to more productive uses in the economy, aside from avoiding a harm that will occur at a greatly reduced probability. (2) It may discourage the firm from pursuing welfare-enhancing innovations that involve the processing of data. (3) For small firms, this may lead to exit (especially during the pandemic).

To summarize the economic considerations to achieve optimal deterrence, the amount of the fine for infringement of the DPA should generally factor the marginal harm to the consumer, a firm's marginal cost to protect the consumer, a firm's marginal gain if it violates the law, private and

social harm, the probability of detection, advantage gained and the risk preferences of the parties concerned. These figures would vary on a case-to-case basis.

Because the DPA covers all types of persons and entities that are engaged in the processing of personal information, monetary fines should consider the heterogenous entities, particularly the differences in the size of firms and entities, the types of data being collected, the processing involved, and the nature and seriousness of the offense.

Considering that adding a fixed or uniform fines that is designed to deter large companies may overly deter/penalize MSMEs. According to the Philippine Statistics Authority (PSA), 99.5% of businesses in the country are comprised of MSMEs, employing 5,510,760 jobs or 62.4% of total employment. The expansive scope means that monetary fines should consider the diverse entities that are covered by law.

From the point of optimal protection and fairness, the study recommends a proportionate or tiered schedule of fines, similar to those being implemented in other jurisdictions. This helps in providing clarity and predictability to guide behavior, and also flexibility to balance protection with fairness. A fine can be determined as a percentage of the firm's annual turnover and can be increased once a threshold value of income or assets is reached. A range of fines may also be calibrated and refined to depend on various key factors such as the number of data subjects affected, the number of violations, the seriousness of the infringement, or repeat offenses. A cap on the fines may also be provided to address overdeterrence.