feature

An Ethical Approach to Data Privacy Protection

Wanbil W. Lee, DBA, FBCS, FHKCS, FHKIE, FIMA
Is principal director of Wanbil & Associates, founder and president of The Computer Ethics Society, and cofounder and Life Fellow of the Hong Kong Computer Society. He serves on committees of several professional bodies, editorial boards and government advisory committees. He has held professorial and adjunct appointments in a number of universities. His expertise is in information systems, and he has a strong interest in information security management, information systems audit and ethical computing.

Wolfgang Zankl, Ph.D.
Is a professor of private and comparative law at the University of Vienna (Austria) and associate lecturer for social media law at the Quadriga University (Berlin, Germany). He founded and runs the European Center for E-commerce and Internet Law *(e-center.eu)* and is a board member of The Computer Ethics Society.

Henry Chang, CISM, CIPT, CISSP, DBA, FBCS
Is an adjunct associate professor at the Law and Technology Centre, the University of Hong Kong. Chang is an appointed expert to the Identity Management and Privacy Technologies Working Group (SC27 WG5) of the International Organization for Standardization (ISO). His research interests are in technological impact on privacy, accountability and Asia privacy laws.

Privacy, trust and security are closely intertwined, as are law and ethics. Privacy preservation and security provisions rely on trust (e.g., one will allow only those whom one trusts to enter one's zone of inaccessibility; one will not feel secure unless one trusts the security provider). Violation of privacy constitutes a risk, thus, a threat to security. Law provides a resolution when ethics cannot (e.g., ethics knows that stealing is wrong; the law punishes thieves); ethics can provide context to law (e.g., law allows trading for the purpose of making a profit, but ethics provides input into ensuring trade is conducted fairly). Privacy breaches disturb trust and run the risk of diluting or losing security; it is a show of disrespect to the law and a violation of ethical principles.

Data privacy (or information privacy or data protection) is about access, use and collection of data, and the data subject's legal right to the data. This refers to:

- Freedom from unauthorized access to private data
- Inappropriate use of data
- Accuracy and completeness when collecting data about a person or persons (corporations included) by technology
- Availability of data content, and the data subject's legal right to access; ownership
- The rights to inspect, update or correct these data

Data privacy is also concerned with the costs if data privacy is breached, and such costs include the so-called hard costs (e.g., financial penalties imposed by regulators, compensation payments in lawsuits such as noncompliance with contractual principles) and the soft costs (e.g., reputational damage, loss of client trust).

Though different cultures put different values on privacy or make it impossible to define a stable, universal value, there is broad consensus that privacy does have an intrinsic, core and social value. Hence, a privacy approach that embraces the law, ethical principles, and societal and environmental concerns is possible despite the complexity of and difficulty in upholding data privacy.

Data Privacy Protection

Indeed, protecting data privacy is urgent and complex. This protection is necessary because of the ubiquity of the technology-driven and information-intensive environment. Technology-driven and information-intensive business operations are typical in contemporary corporations. The benefits of this trend are that, among other things, the marketplace is more transparent, consumers are better informed and trade practices are more fair. The downsides include socio-techno risk, which originates with technology and human users (e.g., identity theft, information warfare, phishing scams, cyberterrorism, extortion), and the creation of more opportunities for organized and sophisticated cybercriminals to exploit. This risk results in information protection being propelled to the top of the corporate management agenda.

The need for data privacy protection is also urgent due to multidirectional demand. Information protection becomes an essential information security

function to help develop and implement strategies to ensure that data privacy policies, standards, guidelines and processes are appropriately enhanced, communicated and complied with, and effective mitigation measures are implemented. The policies or standards need to be technically efficient, economically/financially sound, legally justifiable, ethically consistent and socially acceptable since many of the problems commonly found after implementation and contract signing are of a technical and ethical nature, and information security decisions become more complex and difficult.

Data privacy protection is complex due to socio-techno risk, a new security concern. This risk occurs with the abuse of technology that is used to store and process data. For example, taking a company universal serial bus (USB) device home for personal convenience runs the risk of breaching a company regulation that no company property shall leave company premises without permission. That risk becomes a data risk if the USB contains confidential corporate data (e.g., data about the marketing strategy, personnel performance records) or employee data (e.g., employee addresses, dates of birth). The risk of taking the USB also includes theft or loss.

Using technology in a manner that is not consistent with ethical principles creates ethical risk, another new type of risk. In the previous example, not every staff member would take the company USB home, and those who decide to exploit the risk of taking the USB may do so based on their own sense of morality and understanding of ethical principles. The ethical risk (in addition to technical risk and financial risk) arises when considering the potential breach of corporate and personal confidentiality. This risk is related partly to technology (the USB) and partly to people (both the perpetrator and the victims) and is, therefore, a risk of a technological-cum-social nature—a socio-techno risk. Hence, taking home a USB is a vulnerability that may lead to a violation of data privacy.

However, the problem of data privacy is not unsolvable. The composite approach alluded to earlier that takes into consideration the tangible physical and financial conditions and intangible measures against logical loopholes, ethical violations, and social desirability is feasible, and the method suggested in this article, which is built on a six-factor framework, can accomplish this objective.

Methods for Data Privacy Protection

The method is modeled on a framework originally perceived and developed to provide a fresh view to decision makers and is based on the following three major instruments:

- The International Data Privacy Principles (IDPPs)[1] for establishing and maintaining data privacy policies, operating standards and mitigation measures
- Hong Kong's Data Protection Principles of personal data (DPPs)[2] for reinforcing those policies, standards and guidelines
- The hexa-dimension metric operationalization framework[3] for executing policies, standards and guidelines

> **"Data privacy can be achieved through technical and social solutions."**

International Data Privacy Principles

Data privacy can be achieved through technical and social solutions. Technical solutions include safeguarding data from unauthorized or accidental access or loss. Social solutions include creating acceptability and awareness among customers about whether and how their data are being used, and doing so in a transparent and confidential way. Employees must commit to complying with corporate privacy rules, and organizations should instruct them in how to actively avoid activities that may compromise privacy.

Next to technical and social solutions, the third element of achieving privacy is complying with data protection laws and regulations, which involves two issues. The first concern is that legal regulation is slow and, thus, unable to keep

up with the rapid developments of information technology. Legal solutions are usually at least one step behind technological developments. Data privacy by electronic means should, therefore, be based not only on traditional jurisdiction, but also on soft law, i.e., self-binding policies such as the existing data privacy principles. Soft law may be more effective than hard law. The reactions of disappointed customers, especially when those reactions are spread by social media, and the fact that noncompliance with corporate governance may result in unfair competition and/or liability toward affected customers (unfair competition by not complying with self-binding policies/liability toward customers by breach of contract) will often be more effective than mere fines or penalties.

The second problem of data protection has to do with the fact that these regulations are not internationally harmonized, causing severe complications (especially between the United States and the European Union) on a cross-border basis, which is the rule rather than the exception in modern business. To make data privacy rules work in a global environment, the principles outlined in this article consider US standards (e.g., the US Federal Trade Commission's Fair Information Practices), European standards (e.g., Data Protection Directive 95/46/EC and the General Data Protection Regulation [GDPR]), Asian regulations (e.g., Hong Kong Personal Data Privacy Ordinance [PDPO]) and international benchmarks (e.g., the Organization for Economic Co-operation and Development [OECD] Privacy Framework Basic Principles).

This article also considers the fact that common data privacy regulations, especially in Europe, tend to focus on a traditional human rights approach, neglecting the fact that nowadays, data are usually given away voluntarily upon contractual agreement. When using sites such as Google, Baidu, Amazon, Alibaba or Facebook, users agree with the terms and conditions of these companies. Data privacy should consider not only mere data protection, but also contractual principles, among which one of the oldest and most fundamental is *do ut des*, meaning a contract in which there is a certain balance between what is given and what is received. That philosophy explains why companies such as Google or Facebook, for whose services the customer does not pay, have the right to use personal data. In other words, that tradeoff—data for services—is the balance.[4]

The consumer being less protected when receiving free services is a basic element of the European E-Commerce Directive, which does not apply to services that are offered free of charge. But this consideration is only a first step. Applied to a modern data environment, a balance also has to be struck in relation to other parameters relevant to contractual aspects of data privacy. Since data are a contract matter, it is important to consider what kind of personal data are in consideration (e.g., sensitive and nonsensitive data have to be distinguished and treated differently), and since contracts are concluded by mutual consent, the extent of such consent also has to be taken into account. For example, does consent have to be declared explicitly or is accepting the terms of use sufficient?

"Common data privacy regulations, especially in Europe, tend to focus on a traditional human rights approach, neglecting the fact that nowadays, data are usually given away voluntarily."

The IDPPs approach takes into consideration the Asian, European, US and international data protection standards and focuses on personal data, but can apply to corporate data as well. These principles suggest that the three parameters (payment, consent and data category) should be balanced and combined with the previously mentioned, Asian, European, US and international

standards, putting them into a set of privacy rules. Organizations in compliance with international data privacy standards should commit to the following 13 IDPPs:[5]

1. Comply with national data protection or privacy law, national contract law, and other legal requirements or regulations relating to data privacy.
2. Comply with current security standards to protect stored personal data from illegitimate or unauthorized access or from accidental access, processing, erasure, loss or use.
3. Implement an easily perceptible, accessible and comprehensible privacy policy with information on who is in charge of data privacy and how this person can be individually contacted, why and which personal data are collected, how these data are used, who will receive these data, how long these data are stored, and whether and which data will be deleted or rectified upon request.
4. Instruct employees to comply with such privacy policies and avoid activities that enable or facilitate illegitimate or unauthorized access in terms of IDPPs.
5. Do not use or divulge any customer data (except for statistical analysis and when the customer's identity remains anonymous), unless the company is obliged to do so by law or the customer agrees to such use or circulation.
6. Do not collect customer data if such collection is unnecessary or excessive.
7. Use or divulge customer data in a fair way and only for a purpose related to activities of the company.
8. Do not outsource customer data to third parties unless they also comply with standards comparable to these IDPPs.
9. Announce data breaches relating to sensitive data.
10. Do not keep personal data for longer than necessary.
11. Do not transfer personal data to countries with inadequate or unknown data protection standards unless the customer is informed about these standards being inadequate or unknown and agrees to such a transfer.
12. In the case of a contract between the company and the customer in which the customer commits to pay for services or goods:
    - Inform the costumer individually and as soon as reasonably possible in the event of a data breach.
    - Inform the customer upon request about which specific data are stored, and delete such data upon request unless applicable laws or regulations require the company to continue storing such data.
    - Do not use or divulge content-related personal data.
    - Do not use or divulge any other personal data without the customer's explicit, separate and individual consent.
    - Do not store, use or divulge any customer data, unless applicable laws or regulations require the company to continue storing such data.

13. In the absence of a contract between the company and the customer in which the customer commits to pay for services or goods:
   – Inform the customer as soon as reasonably possible in the event of data breaches.
   – Inform the customer upon request what types of sensitive data are stored and delete such data upon request when such data are outdated, unless applicable laws or regulations require the company to continue storing such data.
   – Do not use or divulge sensitive data without the customer's explicit, separate and individual consent.

The Hong Kong Personal Data Privacy Ordinance

The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Privacy Guidelines)[6] are often the standard that data protection laws of many countries reference.[7]

The OECD Privacy Guidelines have eight basic principles:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Being a framework with the aim of providing guidelines to jurisdictions to enact their own privacy laws, the definitions of these principles are at a high level deliberately. When these high-level principles are converted to national laws, many jurisdictions take on the same principles-based approach. For example, the UK's Data Protection Act uses eight DPPs,[8] Australia's Privacy Act has 13 privacy principles,[9] and the Canadian Personal Information Protection and Electronic Documents Act has 10 principles.[10]

For the purpose of illustration, the remaining part of this article will use Hong Kong's PDPO, enacted in 1995 and Asia's first privacy law, to highlight the salient points on how ethical considerations are built within the implementation of privacy legislation that is compatible with the OECD Privacy Guidelines.

The Six Data Protection Principles of PDPO

An explanation of the DPPs is provided by the Hong Kong,[11] Office of the Privacy Commissioner for Personal Data, and can be summarized as:

1. Data Collection and Purpose Principle:
- Personal data must be collected in a lawful and fair way for a purpose directly related to a function/activity of the data user (i.e., those who collect personal data).

- Data subjects (i.e., individuals from whom personal data are collected) must be notified of the purpose and the classes of persons to whom the data may be transferred.
- Data collected should be necessary, but not excessive.

2. **Accuracy and Retention Principle**—Personal data must be accurate and should not be kept for a period longer than is necessary to fulfill the purpose for which they are used.
3. **Data Use Principle**—Personal data must be used for the purpose for which the data are collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.
4. **Data Security Principle**—A data user needs to take reasonably practical steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use, while taking into account the harm that would affect the individual should there be a breach.
5. **Openness Principle**—A data user must make personal data policies and practices known to the public regarding the types of personal data it holds and how the data are used.
6. **Data Access and Correction Principle**—Data subjects must be given access to their personal data and allowed to make corrections if the data are inaccurate.

The PDPO is principle-based and is not a piece of prescriptive law. Knowing the underlying ethical considerations for each principle will help an organization to better understand the spirit and the letter of the law when developing a compliance program. In particular, ethical relevance is clearly evident in the implications of PDPO privacy protection principles:

- DPP1 explains that the collection of personal data must be fair and that personal data collected should not be excessive. Whether the collection is fair and excessive will have to be assessed under the circumstance. Given that fairness and excessiveness for one person may not be the same for another person, there is, inevitably, a judgment involved in the assessment. That relativistic judgement will, in turn, be influenced by the society's acceptable behavior and value, i.e., its collective ethical belief.
- DPP2 states that collected personal data are not to be kept for longer than is necessary. As there is also an element of judgment on necessity, it can be argued on utilitarian grounds that there could be an ethical dilemma in deciding on a short retention period that is protective of the individuals or a longer period that is protective of the interests (commercial or otherwise) of the organization that collects the personal data.
- DPP3 states that data use that is not directly related to the original purpose may be carried out only with the consent of the individual. This may be translated as respecting the wishes of the individuals. Even if the organization thinks that the changed use would be beneficial to individuals, the organization has no right to take away the individual's free will and choice.

"Knowing the underlying ethical considerations for each principle will help an organization to better understand the spirit and the letter of the law."

- DPP4 states that organizations should implement reasonable security protection on the collected personal data to prevent data leakage. While leaving aside the decision on how many resources and how much effort an organization should use to protect the personal data collected, DPP4 asks organizations to balance the resources and effort against the likely harm to individuals.

In 2010, ethical considerations related to data protection played a major role in testing existing laws. The Octopus card is an "electronic wallet" that many Hong Kong residents use for daily transportation and everyday purchases. In 2010, it was discovered that Octopus Cards Limited, the company that owned the cards, was selling card owners' loyalty membership to insurance companies for direct marketing purposes. As a result of public outcry, the privacy commissioner investigated and concluded that while the sales of customer records was not prohibited by the law at the time, the company failed to make a meaningful effort to seek consent from customers when it informed them of this data use in a privacy policy statement.

The company denied contravening the law, but accepted that its actions felt short of customer expectations. Two major officers of the company stepped down during the investigation.[12, 13]

The heightened public awareness of personal data rights that arose in the wake of the incident changed expectations of organizational behavior. No longer will people accept companies doing only the bare minimum required by law; they must also act ethically. The chief executive officer (CEO) who took over Octopus Cards Limited after the incident captured the new expectations succinctly: "We need to do not just [what is] legal, but what is right."[14]

The Hexa-dimension Code of Conduct

A code of conduct serves a variety of functions, one of the most important of which is to serve as a guide for stakeholders based on a set of rules and standards. Despite official adoption, company policies and standards, which tend to be difficult for stakeholders, including employees to absorb, are not easy to enforce effectively and are probably ignored in the end. A code of conduct, if formulated and articulated well, should serve to communicate the policies and standards to stakeholders in a relatable way. While such codes may serve to deter potential offensive actions, they are limited in enforcing those rules or standards; they rely purely on the moral obligation of the stakeholders concerned, because violation by itself does not, in general, attract any criminal charges in the legal sense. However, despite the good intention and official adoption, the code by itself cannot guarantee more ethical behavior, and auxiliary measures must be in force to operationalize the rules and standards effectively.

Organizations of all varieties might have some kind of code of practice in place. However, the extant codes invariably tend to focus on technical, financial and legal issues and are insufficient when considering the ethical, social and ecological concerns that rapidly emerge and ascend to the top of corporate and IT management agendas. Different organizations have their own unique policies and a unique code of conduct; there can be no universal recipe, only a general guideline. As a general guideline for designing a code of conduct, the hexa-dimension framework is recommended. This framework comprises two major components: the theoretical hexa-dimension metric for measuring legal validity, social desirability, ecological sustainability, ethical acceptability, technical effectiveness and financial

viability (the six requirements/factors) and a scheme for operationalizing the framework. The operationalization scheme is carried out in three major steps including:

- Identify the relevant critical factors depending on the target end users (corporatewide or a functional unit or nature of operation). For example, environmental impact is critical for a mining company or a factory, but could probably be skipped for an information security unit.
- Secure the support of the board of directors with respect to corporate policy aspects and the supporting infrastructures that include the organization's human resources (HR) management, legal, finance, and information and communications technology functional units with respect to technical support and reference. An appraisal of ethical consistency in conduct should be included during annual performance reviews (by HR).
- Determine a schedule for quantifying the elements of each factor for measuring, prioritizing and balancing the factors. The attributes/factors with help determine the steps to be taken to measure the effectiveness.

If properly and appropriately formulated and articulated, the code can be useful in disseminating the policies and standards throughout the organization and beyond, thus cultivating corporatewide ethical, professional conduct. While a code may deter potential offensive actions, it is limited in enforcing the rules or standards. The limitation exists because the code can rely only on the stakeholders' sense of morality because violation of the code does not entail any criminal charges. Auxiliary measures must be put in place to arrive at desirable results, such as executive actions that provide rewards and impose punishment (e.g., discussing the hexa-dimensional code of conduct during an annual performance appraisal when those being appraised are asked to exemplify that their assigned duties were carried out in a manner consistent with data privacy protection policies, i.e., not breaking the law; not harmful to individuals and society at large; not wasteful of the resources available including the computer facilities, the workforce, the budget; and not harming the environment).

"While a code may deter potential offensive actions, it is limited in enforcing the rules or standards."

Conclusion

Information security professionals are in urgent need of effective and pragmatic guidance for developing data privacy protection standards for two major reasons. The first is that the information security function in a technology-driven information-intensive environment becomes more complicated due to new risk (e.g., socio-techno risk); the second is that data privacy protection becomes a primary concern to information security management as privacy infringement occurs frequently and attracts wide coverage in the media. Viewing privacy from the perspective of ethics can help enterprises establish and improve their code of conduct. Considering privacy from an ethical point of view and establishing a code of conduct makes all individuals in an organization, not just security personnel, accountable for protecting valuable data.

Endnotes

1 Zankl, W.; The International Data Privacy Principles, presented at Harvard University, Cambridge, Massachusetts, USA, October 2014, *www.e-center.eu/static/files/moscow-dataprivacy-handout-russian.pdf*

2 The Personal Data (Privacy) Ordinance, Chapter 486 , *https://www.pcpd.org.hk/english/files/pdpo.pdf* and *https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html*

3 Lee, W. W.; "A Hexa-dimension Metric for Designing Code of Ethical Practice," *Encyclopedia of Information Science and Technology, 4th Edition*, July 2017

4 It has been argued that companies using, for instance, their Internet platforms for advertising purposes are already being paid by the advertisers so there is no need for further payment with data. This point of view neglects the fact that *do ut des* refers to a balance between *quid pro quo* of the contracting parties and not between these parties and third parties. That is why readers have to pay for magazines despite the publisher receiving payments from third parties (advertisers).

5 *Op cit*, Zankl

6 Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *www.oecd.org/sti/ieconomy/cdguidelinesonthe protectionofprivacyandtransborderflowsof personaldata.htm*

7 Greenleaf, G; "Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority," *133 Privacy Laws & Business International Report*, February 2015, p. 14-17

8 Information Commissioner's Office, Data Protection Principles, United Kingdom, *https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/*

9 Office of the Austrailian Information Commissioner, Australian Privacy Principles, *https://oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles*

10 Office of the Privacy Commissioner of Canada, PIPEDA Fair Information Principles, September 2011, *https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/*

11 Office of the Privacy Commissioner for Personal Data, Six Data Protection Principles, Hong Kong, *https://www.pcpd.org.hk/english/data-privacy_lau/6_data_protection/principles.html*

12 Ng, J.; "Octopus CEO Resigns Over Data Sale," *The Wall Street Journal*, 4 August 2010, *https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html*

13 Chong, D.; "Second Octopus Boss Quits Amid Scandal," *The Standard*, 20 October 2010, *www.thestandard.com.hk/news_detail.asp?pp_cat=30&art_id=104016&sid=29979255&con_type=1&d_str=20101020&sear_year=2010*

14 Cheung, S.; "The Challenges of Personal Data Privacy in A New Era," International Conference on Privacy Protection in Corporate Governance, 11 February 2014, *https://www.pcpd.org.hk/privacyconference2014/programme.html*