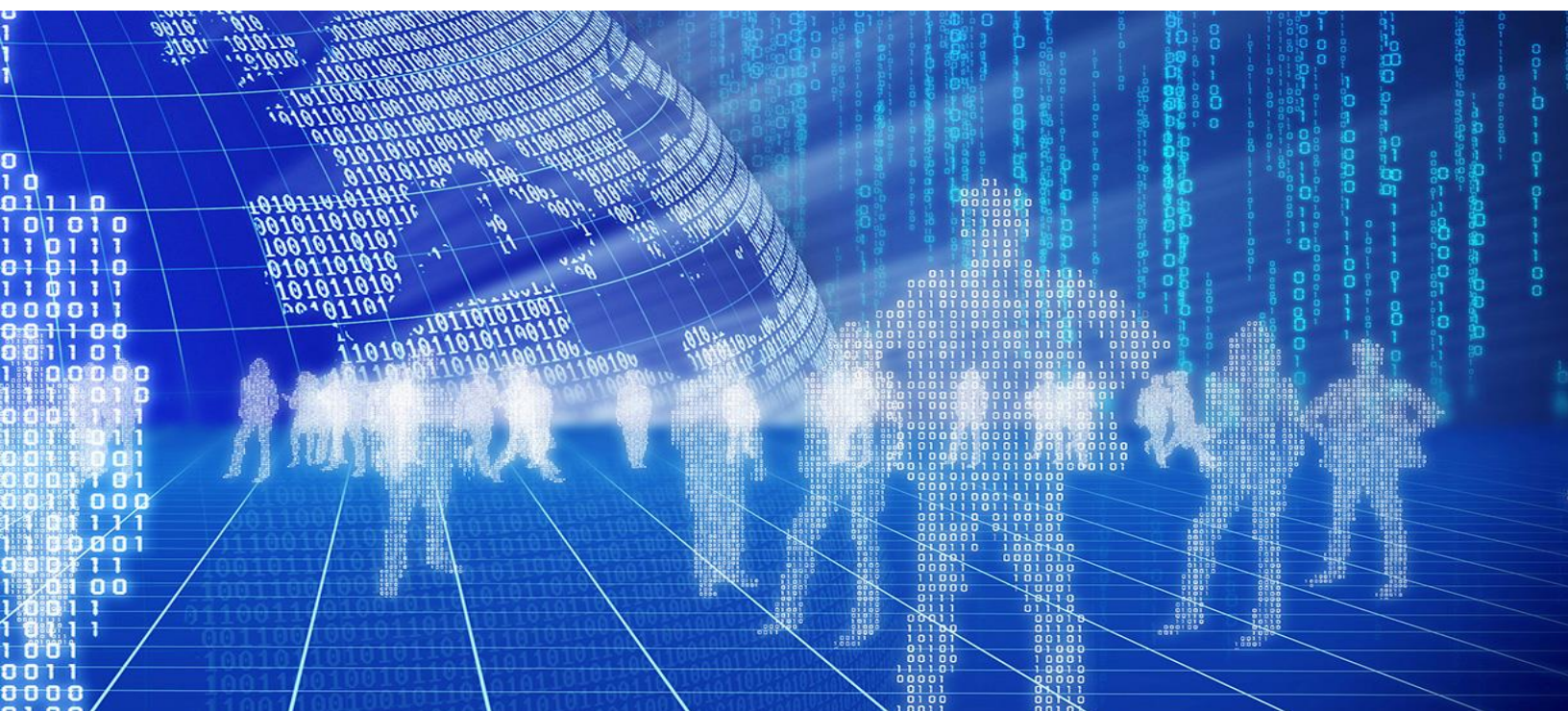


# Ethical Accountability Framework for Hong Kong China

A Report prepared for the Office of the Privacy  
Commissioner for Personal Data

*Analysis and Model Assessment Framework*





## **Foreword for the Research Report of the Legitimacy of Data Processing Project**

Undoubtedly, we are witnessing the digital revolution and the evolution of the data ecosystem. Innovations in information and communications technology such as big data, artificial intelligence and machine learning (smart technologies) have transformed the world we live in: Data, in particular personal data, is collected and generated on a massive scale and at an unprecedented speed by the use of these smart technologies and related devices; data from various sources is aggregated to form big data, which is then processed and analysed by algorithms to formulate patterns, predictions and insights to create value; a wide range of new services such as natural language processing, translation, image recognition, virtual assistants, profiling, credit scoring and automated decisions have been created. Indeed, as set out in the Smart City Blueprint released in December 2017 by the Government of Hong Kong, Hong Kong strives to become a world-renowned smart city by adopting measures such as electronic identity, an intelligent transport system and big-data analytics platform, the functioning of which requires the smart technologies and more importantly, data (including personal data).

Such technological developments do, however, bring about privacy issues. Extensive and ubiquitous collection of personal data, both online and offline, together with the unpredictability in the use and transfer of the data, have challenged the data privacy frameworks around the globe which are largely notification or consent-based. Individuals may not even be aware that their personal data has been collected or shared, not to mention exercising control over their data. Sophisticated data mining, analytics and profiling techniques may, either inadvertently or purposefully, expose one's innermost secrets, or intimate space. Depending on the source and quality of the data and the algorithms, the results of data analytics may be biased or discriminatory.

Like many other data-protection laws, the Personal Data (Privacy) Ordinance of Hong Kong (Cap. 486 of the laws of Hong Kong) is principle-based and technology neutral. The benefit of a piece of principle-based and technology neutral legislation is that it has the ability to be nimble and responds to the changing privacy landscape to protect privacy; however, the advancement of technology and the proliferation of advanced data-processing activities are stretching the limits of the underlying data protection principles enshrined in the Ordinance such as “notice and consent”, “use limitation,” and “transparency.”

For instance, pursuant to the Ordinance, data users (organisations) are not allowed to use personal data for a new purpose unless with the prescribed consent of the individuals (the “use limitation” principle). Prescribed consent, as defined in the Ordinance, is express and voluntary consent. For consent to be meaningful, data subjects (individuals) should also be adequately informed. This means that the individuals concerned should understand well about what the



new purpose is, who the potential data transferees are, and what the risks are, among other things. Nevertheless, assuming the unpredictability of big data analytics and artificial intelligence, it will be difficult to provide these pieces of specific information to the individuals before their personal data is collected, processed, or used.

In view of these challenges to personal data protection and the data economy, I am duty bound to find the way out for both data users and data subjects in the digital age. I believe that data ethics would be the long-term solution. As Mr Giovanni Buttarelli, the European Data Protection Supervisor, has rightly pointed out: “*Massive digitisation and machine learning are demanding new and smarter policy responses: stronger enforcement but also empowerment through tools like meaningful consent; **ethics and accountability and a fairer allocation of the digital dividend***”.<sup>1</sup> (Emphasis added)

Businesses or organisations in general that amass and derive benefits from personal data cannot have the mindset to conduct their operations to meet the minimum regulatory requirements only, as a recent incident involving a social media platform shows that there is a big gap between stakeholders’ expectations and the social media platform’s data practices. They should be held to a higher ethical standard that meets the stakeholders’ expectations alongside the laws and regulations. Data ethics can therefore bridge the gap between legal requirements and the stakeholders’ expectations.

Ethical values and principles typically centre around fairness, respect, and mutual benefits. In practice, it may involve genuine choices, meaningful consent, and fair exchange among organisations and individuals, as well as others. These ethical values and principles also tend to have more enduring applicability and higher flexibility, in particular when dealing with matters that require delicate balancing.

It is against this background that my office commissioned the Information Accountability Foundation (IAF) to conduct this consultancy study—the Legitimacy of Data Processing Project, with a view to exploring the core values to guide advanced data processing activities that are ethical and fair to all stakeholders, including individuals and businesses. The consultancy study also aims to provide a tool in the form of model assessment frameworks to assist organisations that conduct advanced data processing activities to put the core ethical values into practice. By conducting the consultancy study, we aim at finding answers to the following questions:

- What does it mean by “ethical” or “fair” processing of data?
- What would an ethical data impact assessment consist of and what are the standards for ethical data stewardship?
- What is the direct or indirect linkage between ethical or fair processing of data and the relevant legal requirements? What aspects of ethical data stewardship go beyond the law?

---

1. “*Accept and Continue: Billions are Clocking into Digital Sweat Factories without Realising it*” (30 April, 2018), Giovanni Buttarelli. [https://edps.europa.eu/press-publications/press-news/blog/accept-and-continue-billions-are-clocking-digital-sweat-factories\\_en](https://edps.europa.eu/press-publications/press-news/blog/accept-and-continue-billions-are-clocking-digital-sweat-factories_en)



- What are the motivators for business to adopt ethical data stewardship and utilise ethical data impact assessments?

Twenty-three organisations in Hong Kong from various sectors (e.g., banking, insurance, telecommunications, healthcare services, transportation) have participated in the project by providing comments and feedback on the draft project deliverables, so as to ensure that the recommendations of the project are relevant and practicable in the business environment and day-to-day operations. I am truly grateful for the invaluable contribution made by these organisations.

The theme of the 40th International Conference of Data Protection and Privacy Commissioners, an annual world conference in the privacy/data protection arena, to be held in Brussels in October 2018 is “*Debating Ethics: Respect and Dignity in Data-Driven Life.*” It is an opportune time for IAF and my office to publish the findings of this project with a view to picking the wisdom of privacy professionals, business leaders, civil societies and other stakeholders from around the world.

The three data-stewardship values proposed in this research report, namely being respectful, beneficial and fair, are easy to understand, flexible, and realistic. The two model frameworks are also sensible, comprehensive, and practicable. We sincerely hope that these project deliverables will become wieldy, helpful and effective tools that assist organisations in Hong Kong and beyond to implement data ethics in their daily operations, and to fully reap the benefits of the data-driven economy while protecting and respecting the fundamental rights (including the right to privacy), interests and freedoms of individuals.

The publication of the project findings will mark the beginning of my office’s strengthened initiative for a cultural change in data privacy protection. Through continuous incentives and engagement efforts, I hope that in the not-too-distant future, ethical data stewardship will become a well-received norm among organisations in Hong Kong.

I would also like to extend my sincere appreciation for IAF’s admirable professionalism and acclaimed expertise in accomplishing this project. Special thanks must go to Martin Abrams, Peter Cullen, Lynn Goldstein and Julianne Seaman for their most inspirational thoughts, advice, and dedication.

Stephen Kai-yi WONG  
Privacy Commissioner for Personal Data, Hong Kong, China  
October 2018



## I. Executive Summary

Bringing the physical world together with the cyber world – the fourth industrial revolution—has the potential to revolutionize the way we work, learn, and manage our health and every other facet of human life. It will not happen if individuals lack trust and do not participate. Smart cars will not be smart and personalized medicine will not be personal. An ethical accountability framework, consisting of updated accountability elements, supported by a model ethical data impact assessment and by a process oversight model, can fill that trust deficit facilitating real innovation.

“The First Industrial Revolution used water and steam power to mechanize production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.

“There are three reasons why today’s transformations represent not merely a prolongation of the Third Industrial Revolution but rather the arrival of a Fourth and distinct one: velocity, scope, and systems impact. ... The possibilities of billions of people connected by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge are unlimited. And these possibilities will be multiplied by emerging technology breakthroughs in fields such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing.”<sup>2</sup>

Since data and analytics technologies generate great return on investment, companies increasingly see the goal to be the transformation of data into information and information into insight. Artificial intelligence (AI) and machine learning (ML) assist in transforming data. Privacy and data protection legislation are ill-equipped to keep up with, let alone anticipate, technological changes such as advanced data-processing activities and, therefore, to address the questions of trust raised by the complexities of advanced technology and data intensive activities.

To enhance the protection of personal data privacy rights of individuals, the Hong Kong Privacy Commissioner for Personal Data (PCPD) has commissioned a study, the purpose of which is to achieve the ethical and fair processing of data about an individual by fostering a culture of ethical data governance and addressing the personal-data privacy risks brought by ICT (the Study).<sup>3</sup> The PCPD commissioned the Information Accountability Foundation (IAF) to conduct the Study and to compile this Report.

---

2. Klaus Schwab, “The Fourth Industrial Revolution: What It Means, How to Respond,” *World Economic Forum*, January 14, 2016. <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.

3. This is not the first time the need to review the Personal Data (Privacy) Ordinance (PDPO) has been recognized. In August 2009, the Constitutional and Mainland Affairs Bureau of the Hong Kong Government, with the support of the PCPD, published the “Consultation Document on Review of the Personal Data (Privacy) Ordinance” [hereinafter



As part of the Study, this Report asks: How can data-intensive activities and technologies that have an impact on individuals be conducted in a fair and ethical manner while achieving the desired benefits? Recent privacy legislation such as the General Data Protection Regulation (GDPR) has elevated accountability from check-box compliance to a risk-based approach, but enhanced data stewardship accountability elements are needed to address the challenges raised by advanced data processing activities.

Working with approximately twenty-three Hong Kong organizations, the “Enhanced Data Stewardship Accountability Elements for Data Processing Activities, such as AI and ML, that Directly Impacts People (Enhanced Elements) and Data Stewardship Values” (Values) were drafted. The Enhanced Elements update the accountability elements to incorporate the data stewardship necessary for more trusted, advanced data-processing activities. The Enhanced Elements underpin three behavioral values – Respectful, Beneficial and Fair – and are supported by a [Model Ethical Data Impact Assessment \(EDIA\)](#) and a Process Oversight Model. Together these documents constitute a practicable framework that is interoperable with other privacy and data protection regimes.

An EDIA is a process that looks at the full range of rights and interests of all parties in a data-processing activity to achieve an outcome when advanced data analytics may impact people in a significant manner and/or when data-enabled decisions are being made without the intervention of people. An EDIA assists an organization in looking at the rights and interests impacted by the data collection, use and disclosure in data-driven activities.

The Process Oversight Model looks at how an organization has translated organizational ethical values into principles and policies and into an “ethics by design” program. It considers how well established internal review processes, such as EDIAs and effective individual accountability systems, have been implemented.

Use of the Enhanced Elements, the EDIA and Oversight Process and adoption of ethical values by organizations will give individuals more confidence that their interests are being protected. Undertaking these governance activities will allow organizations to continue to use data during the Fourth Industrial Revolution in a trusted manner while also making the most of technology and data-driven insights

---

Consultation Document]. [https://www.cmab.gov.hk/doc/issues/PDPO\\_Consultation\\_Document\\_en.pdf](https://www.cmab.gov.hk/doc/issues/PDPO_Consultation_Document_en.pdf). The purpose of the Consultation Document was to “examine whether the existing provisions of the Ordinance still afford adequate protection to personal data having regard to developments, including advancement in technology in the last decade.” (Consultation Document at 1.05 .) It was expressly stated that the review was conducted regarding “the privacy impact of technological advancements in this electronic age which facilitate the collection, holding, processing and transmission of massive personal data almost instantaneously.” Id.

## II. Introduction

The proliferation of information and communication technologies (ICT), like the Internet of Things, big-data analytics and AI, in recent years has brought significant changes to the scale and ways personal data is collected, processed and used. ICT is bound to drive economic growth in the data economy of the 21<sup>st</sup> century and to bring tremendous benefits to both organizations and society by improving, for example, communications, resource allocation, productivity, and customer/client satisfaction. Data, primarily personal data, is the key element that fuels this growth engine. However, ICT poses challenges to privacy and data protection laws that rely heavily on the notions of “transparency” and “notice and consent” to protect the individual’s right to fair processing. There is growing agreement that “consent” is not fully effective in governing complex information systems and that achieving transparency is challenging. Governments around the world are confronted, on the one hand, by the ethical implications and the appropriate accountability mechanisms linked to the many risks of AI, and, on the other hand, with promoting data-intensive innovation such as AI as an economic driver. We “cannot allow the rights of individuals to be disregarded in [the development of technological solutions] . . . , nor can we allow new technologies to continue to be designed so to collect as much personal data as possible with so little transparency and control by the users. Technology must serve humankind.”<sup>4</sup>

To enhance the protection of personal data privacy rights, the Hong Kong Privacy Commissioner for Personal Data (PCPD) has commissioned a study, the purpose of which is to achieve the ethical and fair processing of data pertaining to an individual by fostering a culture of ethical data governance and addressing the personal-data privacy risks brought by ICT (the Study). The PCPD commissioned the Information Accountability Foundation (IAF) to conduct the Study and to compile this Report.

This Report is accompanied by the Enhanced Elements, the Data Stewardship Values, the Model EDIA and the Model Oversight Process. Altogether the documents accompanying this report provide a workable framework encompassing data-privacy values and ethics along with fairness suitable for flexible adoption for the whole life cycle in processing personal data. It also accommodates Hong Kong’s legal framework, the business, economic and cultural environment, and balances the interests of multiple parties. When organizations rely on this framework, individuals will have more confidence their interests are being protected, enabling organizations to continue to use data to drive the ICT economy.

---

4. Giovanni Butarelli, “A Crucial Moment for Communications Privacy,” *European Data Protection Supervisor*, 27 September, 2017. [https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy\\_en](https://edps.europa.eu/press-publications/press-news/blog/crucial-moment-communications-privacy_en).

### III. The Value of Data and Advanced Data-Processing Activities and the Role of Technology

Organizations now see data as a valuable resource. “The world’s most valuable resource is no longer oil, but data.”<sup>5</sup> Smartphones and the internet have made data abundant, ubiquitous and far more valuable. AI techniques such as ML extract more value from data.<sup>6</sup> Organizations increasingly are seeing data as a driver of value-creating innovation. In fact, 68 percent of Chief

Executive Officers see data and analytics technologies as generating the greatest return for stakeholder engagement.<sup>7</sup> Indeed, in 2010, it was estimated that the median Fortune 1000 company could increase its revenue by \$2.01 billion a year just by marginally improving the usability of the data already at its disposal.<sup>8</sup> Global business value derived from AI is projected to total \$1.2 trillion in 2018, an increase of 70 percent from 2017, and is forecast to reach \$3.9 trillion in 2022.<sup>9</sup>

The “data is oil” analogy is an imperfect one because data itself is not a commodity. Data, like oil, goes through many refinements and iterations as it becomes useful in multiple ways. The same data can be hosted or processed by many entities—with the consent of the user. For example, a consumer may want his/her health data shared with several hospitals for medical reasons or may have financial data hosted in financial tracking software with more than one company (e.g. Intuit’s Mint, You Need a Budget, Banktivity, Every Dollar, Simple) as well as with the financial institutions themselves.

However, the “data is oil” analogy does demonstrate that data-intensive activities involving, for example, AI need data to run. AI takes in raw data and converts it into useful information for decision-making. The organization relies on data it has accumulated over time as input to train an algorithm and then uses the algorithm to generate predictions to inform actions. The ongoing value of data usually comes from the actions the organization takes in its day-to-day business—the new data it accrues each day. New data allows operation of the AI model after it is trained, and ongoing operational data enables improvements of the AI model through learning.<sup>10</sup>

---

5. “The World’s Most Valuable Resource is No Longer Oil, But Data,” *The Economist*, May 6, 2017.

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

6. Id.

7. “Redefining business success in a changing world,” *PwC 19th Annual Global CEO Survey*, January 2016.

<https://www.pwc.com/gx/en/ceo-survey/2016/landing-page/pwc-19th-annual-global-ceo-survey.pdf>.

8. Anitesh Barua, Deepa Mani, & Rajiv Mukherjee. “Measuring the Business Impacts of Effective Data,” University of Texas McCombs School of Business, September 1, 2010, p. 3.

<http://middleman.heltenkelt.se/anvandbart.se/images/drupalbilder/blogsource/div/EffectiveDataStudyPt1-MeasuringtheBusinessImpactsofEffectiveData-WP.pdf>.

8. “Gartner says Global Artificial Intelligence Business Value to Reach \$1.2 Trillion in 2018,” *Gartner*, April 25, 2018.

<https://www.gartner.com/newsroom/id/3872933>.

10. Ajay Agrawal, Joshua Gans & Avi Goldfarb, “Is Your Company’s Data Actually Valuable in the AI Era?” *Harvard Business Review*, January 17, 2018. <https://hbr.org/2018/01/is-your-companys-data-actually-valuable-in-the-ai-era>.





Again, the “data is oil” analogy is an imperfect one because data changes over time but stays in its original structure while oil is derived from petroleum. However, the “data is oil” analogy is useful to demonstrate the need for quality as well. In their raw forms, the uses of oil and data are limited. It is through refining that oil becomes useful as kerosene, gasoline and other goods, and similarly it is through the refining process of cleansing, validating, deduplicating and auditing that data can become useful in these kinds of analytics. The role data plays in enabling technologies such as AI is critical, but it is one that will be undermined if businesses do not make data quality a priority.<sup>11</sup> By extension, the decision to use data and the decision-making process relating to data use becomes key in the data refining analogy.

There are three major sources of data-driven business value that will be enabled by technologies such as AI and their use of quality data: customer experience, new revenue, and cost reduction.<sup>12</sup> In the early years of AI, customer experience is the primary source of derived business value, as organizations see value in using AI techniques to improve every customer interaction, with the goal of increasing customer growth and retention.<sup>13</sup> Customer experience is followed closely by cost reduction, as organizations look for ways to use AI to increase process efficiency to improve decision-making and automate more tasks.<sup>14</sup> However, in 2021, new revenue will become the dominant source as companies uncover business value in using data-driven AI to increase sales of existing products and services as well as to discover opportunities for new products and services.<sup>15</sup>

---

11. “The Data Differentiator: How Improving Data Quality Improves Business,” *Forbes*, May 2017. [https://www.forbes.com/forbesinsights/pitney\\_bowes\\_data\\_quality/index.html](https://www.forbes.com/forbesinsights/pitney_bowes_data_quality/index.html).

12. Gartner.

13. Some examples of customer experience implementations of AI are: North Face using a chatbot, an app of voice and messaging platforms that helps people converse with a digital business, to help customers refine product selections based on their answers to a series of questions (e.g. if customer likes to hike in the winter, the program asks questions about location and preferences to recommend a jacket) and avoid sorting through hundreds of products; 1-800-FLOWERS using a Facebook Messenger chatbot to help customers order flowers by picking up on conversational cues to suggest arrangements (e.g. if a customer wants something quickly, the bot makes brisk suggestions to win the customer over); Domino’s Pizza using a Facebook Messenger chatbot named Dom that allows customers to place an order by sending a message that says “pizza” (the order is completed faster than a customer could call the store or drive to place an order); Black Diamond Equipment, an e-commerce ski equipment retailer, using browsing history, past purchases and weather conditions to predict customers’ needs and actively making product recommendations (purchases have increased, and abandoned carts have decreased); Spotify storing customer data, accessing it to find trends and predicting what music each customer will like, and delivering each user a personalized “Discover Weekly” playlist with music handpicked for them. Blake Morgan, “10 Customer Experience Implementations of Artificial Intelligence,” *Forbes*, February 8, 2018. <https://www.forbes.com/sites/blakemorgan/2018/02/08/10-customer-experience-implementations-of-artificial-intelligence/-11ee06e82721>.

14. Gartner; Tripps Reddy. “How chatbots can help reduce customer service costs by 30%,” *IBM*, October 17, 2017. <https://www.ibm.com/blogs/watson/2017/10/how-chatbots-reduce-customer-service-costs-by-30-percent/> (Chatbots and virtual agents are being used to reduce customer service costs by up to 30 percent, an estimated \$20 million for 2017. Autodesk’s customer service chatbot, AVA, responds to queries like address changes, login issues, payment issues and other frequently asked questions, any time of day, any day of the year.)

15. Gartner.



While consumers provide much of the data to make “smart” technologies, such as the Internet of Things, sensors, big data analytics, AI and ML, work,<sup>16</sup> many data driven activities involving algorithms and AI models do not use much or any personal data.<sup>17</sup> Indeed, synthetic data, computer generated data that mimics real data, is increasing for data driven activities, such as AI and ML.<sup>18</sup> These “smart” technologies are the innovation and technology forces fueling the engine of the digital economy.<sup>19</sup> “I&T (innovation and technology) is undoubtedly an economic driver in the new era.’ I&T can introduce new industries and can create wealth, drive economic transformation, bring quality jobs for young people and improve people’s quality of life.”<sup>20</sup>

Privacy law generally differentiates between personal data, which is covered, and nonpersonal data that pertains to people, which is not. Between personal data and nonpersonal or anonymized data, however, the boundary between nonpersonal data and personal data may become increasingly blurred when AI is capable of learning underlying relationships between datasets. While these innovative applications of technology may not use personal data, the data they do use can have an impact on individuals (e.g. personalized advertisements and targeted sales activities). These ramifications suggest that an evolved approach to data protection is needed to balance the benefits and the risks to individuals of more data intensive impacting activities.

#### IV. The Focus Should be not only on Technology but also on Information

By focusing on the value of the data to the technology, one may lose sight of the fact that the data also has value when it is converted into information. About 15 years ago, Carly Fiorina, then Chief Executive Officer of Hewlett-Packard, gave a speech on “Information: The currency of the Digital Age.” In that speech, she said: “The agenda is not as much today about technology as it is about information. ... [I]t’s clear that more and more people want access to more and more information, and they don’t want to be limited by technology, by location, by time of day. ... [W]e are entering a world now where every process and all content are being transformed from physical and analog, to digital, mobile, virtual and personal. And by personal, I am not just talking about personalization of content and services, although of course I mean them as well, but what I’m really talking about in this context is the ability of individuals, consumers, citizens,

---

16. Stephen Wong. “Engineering Privacy Through Accountability,” *Office of the Hong Kong Privacy Commissioner for Personal Data*, April 11, 2018, p. 21.

[https://www.pcpd.org.hk/english/news\\_events/speech/files/Engineering\\_Privacy\\_Through\\_Accountability.pdf](https://www.pcpd.org.hk/english/news_events/speech/files/Engineering_Privacy_Through_Accountability.pdf).

17. French Data Protection Authority (CNIL), *How Can Humans Keep the Upper Hand? The Ethical Matters Raised by Algorithms and Artificial Intelligence*, December 2017, p. 4.

[https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_rapport\\_ai\\_gb\\_web.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf). AI often uses data that has been aggregated or anonymized and therefore can be more privacy protective relative to earlier technologies.

18. Seif, George. “Deep learning with synthetic data will make AI accessible to the masses,” Medium, July 10, 2018. <https://towardsdatascience.com/deep-learning-with-synthetic-data-will-make-ai-accessible-to-the-masses-15b99343dd0e>.

19. “LCQ6: Development of smart city,” *Office of the Hong Kong Chief Information Officer*, October 1, 2018.

[https://www.ogcio.gov.hk/en/news/press\\_releases/2018/01/pr\\_20180110.html](https://www.ogcio.gov.hk/en/news/press_releases/2018/01/pr_20180110.html).

20. “Opening Remarks by S for IT at Press Conference on Innovation and Technology Initiatives in 2018-19 Budget,” *Office of the Hong Kong Chief Information Officer*, March 1, 2018 (quoting the Hong Kong Financial Secretary).

[https://www.ogcio.gov.hk/en/news/press\\_releases/2018/03/pr\\_20180301.html](https://www.ogcio.gov.hk/en/news/press_releases/2018/03/pr_20180301.html).



Business professionals—anyone—to control the services and information they get as well as when and where and on what device they get them. ... [T]his of course will add trillions of new devices to the network within the next few years, not to mention the huge volumes of information—data actually first—that must be stored and analyzed and managed and shared, because of course the goal is to transform data into information and information into insight.”

According to Fiorina, the issue “is now all about putting information to work. It is about transforming data from passive to active, from static to dynamic—transforming data into insight. ... [The goal] is to turn data into information, information into knowledge and insight, and knowledge into competitive advantage.”<sup>21</sup>

For the last fifteen years, advances in data processing have made the extraction of useful information from data more effective.<sup>22</sup> “Data processing is simply the conversion of raw data to meaningful information through a process. ... Similar to a production process, it follows a cycle, where inputs (raw data) are fed to a process (computer systems, software, etc.) to produce output (information and insights).”<sup>23</sup>

Potentially the interpretation of data into information is a very complex issue. Humans achieve the transformation of data to information relatively easily and make use of a variety of means: cultural background, unconscious intuitions, concrete memories or similar observation of the past, expectations (depending on context), text book knowledge, and domain-dependent heuristic rules. Computers cannot do such things as easily, although advances have been made in the fields of AI; this level of sophistication is currently beyond the scope of knowledge-based computational systems.<sup>24</sup>

## V. Advanced Data Processing Activities, such as AI and ML

The current wave of progress and enthusiasm for AI began in around 2010, driven by three factors that built upon each other: the availability of big data (from sources including e-commerce, businesses, social media, science, and government) which provided raw material for dramatically improved machine learning approaches and algorithms which in turn relied on the capabilities of more powerful computers.<sup>25</sup>

---

21 Carly Fiorina, “Information: The Currency of the Digital Age,” *HP*, December 6, 2004.

<http://www.hp.com/hpinfo/execteam/speeches/fiorina/04openworld.html>.

22. The EDIA that is proposed to address issues raised by advanced data processing activity, see Section XII *infra*, covers the six important stages in the data-processing cycle: collection, preparation, input, processing, output and interpretation and storage, Paul Rudo, “6 Important Stages in the Data Processing Cycle,”

[www.enterprisefeatures.com](http://www.enterprisefeatures.com), April 24, 2013. <http://www.enterprisefeatures.com/6-important-stages-in-the-data-processing-cycle/>

23. Rudo

24. “Transforming Data Into Knowledge,” *Newcastle Engineering Design Centre*, September 2018.

<http://www.edc.ncl.ac.uk/highlight/rhmarch2007g01.php>.

25. Executive Office of the President of the United States, National Science & Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence* (2016) p. 6



There is no single definition of AI, and the concept of what defines AI has changed over time, but at the core, AI is generally any software which approximates some significant fraction of some aspect of human intelligence.<sup>26</sup> In some cases, a problem is considered as requiring AI before it has been solved, but once a solution is well known, it is considered routine data processing.<sup>27</sup> AI is divided broadly into two stages: narrow AI which uses the principles of pattern recognition to carry out one specific task (e.g. language translation, self-driving vehicles), and general AI which exhibits apparently intelligent behavior at least as advanced as a person across a full range of cognitive tasks.<sup>28</sup> Narrow AI is already providing breakthroughs (e.g. in medicine where it is used to diagnose patients based on genomic data and in industry where it is employed in the financial world for uses ranging from fraud detection to improving customer service by predicting what customers will need.)<sup>29</sup> The current consensus is that full general AI will not be achieved for at least decades.<sup>30</sup>

ML is a statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data. An advantage of ML is that it can be used even in cases where it is infeasible or difficult to write down explicit rules to solve a problem. In a sense, ML is not an algorithm for solving a specific problem but rather a more general approach to finding solutions for many different problems, given data about the problems.<sup>31</sup> ML is about teaching computers to learn in the same way humans do, by interpreting data from the world around humans, classifying the data and learning from the computer's successes and failures.<sup>32</sup> With ML, everything about the decision procedure is known, but there may be too much information to interpret it clearly.<sup>33</sup> ML is a subset of AI.<sup>34</sup>

---

[https://obamawhitehouse.archives.gov/sites/default/files/whitehouse\\_files/microsites/ostp/NSTC/preparing\\_for\\_the\\_future\\_of\\_ai.pdf](https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf); European Commission, European Group on Ethics in Science and New Technologies, *Statement Artificial Intelligence, Robotics and 'Autonomous' Systems*, March 2018, p. 7.

[https://ec.europa.eu/research/ege/pdf/ege\\_ai\\_statement\\_2018.pdf](https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf); House of Lords, Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?* 16 April 2018, 13-14.

<https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>; CNIL Report at 16.

26. U.S. Future of AI Report at 7; Jack Krupansky, "Untangling the Definitions of Artificial Intelligence, Machine intelligence, & Machine Learning," *Medium*, June 13, 2017. <https://medium.com/@jackkrupansky/untangling-the-definitions-of-artificial-intelligence-machine-intelligence-and-machine-learning-7244882f04c7>.

27. *U.S. Future of AI Report* p. 7.

28. *Id.*; *AI in the UK* at 15; CNIL Report at 16.

29. Bernard Marr, "What is Artificial Intelligence and How Will it Change our World?" *Bernard Marr & Co.*

<https://www.bernardmarr.com/default.asp?contentID=963>

30. *U.S. Future of AI Report*, p. 7.

31. *Id.* Pp. 7-9.

32. Bernard Marr, "What is Machine Learning—A Complete Beginner's Guide," *Forbes*, May 4, 2017. <https://www.forbes.com/sites/bernardmarr/2017/05/04/what-is-machine-learning-a-complete-beginners-guide-in-2017/-5129278b578f>; CNIL Report, p. 16.

33. *U.S. Future of AI Report*, p. 9.

34. Marr on ML.



Autonomy in a technology context refers to the ability to work unattended and to make decisions independent of any external intelligent entity over an extended period of time (e.g. an autonomous car driving itself to its destination).<sup>35</sup> Automation occurs when a machine does work that previously might have been done by a person. In some cases, a machine will complement human work (e.g. radiology where both AI and human input are used).<sup>36</sup>

## VI. The Use and Promise of AI/ML Across all Sectors

The CNIL Report, which was the result of public debate organized by the French Data Protection Authority, the CNIL, comprehensively collects, discusses and categorizes the use of AI and ML across sectors and identifies the ethical issues with those uses. The most commonplace uses today are online search engines, road navigation apps, cultural content recommendation on platforms (e.g. Netflix and Amazon), or social media and marketing for targeted advertising purposes or, increasingly, for political campaigns during elections. In healthcare, the uses include health surveillance (detection of epidemics or mental health risks) and precision medicine (personalized therapeutic solutions are developed by cross-linking patient data with datasets obtained from large-scale cohorts). Government uses include providing the legal occupations (e.g. judges) with tools that would enable them, by processing case-law data, to anticipate the outcome of a trial or fine-tune a judicial strategy and providing police forces with tools to channel their resources towards a given area through data analysis. In education, teaching practices are being challenged by ever more advanced strategies to personalize education or the detection of potential early school leavers. Finally, on the job market, various stakeholders are currently working on developing solutions for assisting recruitment (by matching supply with demand in particular) and managing human resources.

The CNIL Report highlights six main ethical issues:

1. While technology may be increasing the way for ever more complex and critical decisions and tasks to be delegated to machines, autonomous machines can also pose a threat to individual autonomy and free will.
2. AI can create bias, discrimination and even exclusion.
3. Personalization is likely to affect not just individuals but also the key collective principles forming the bedrock of societies (filter bubbles—classifying and filtering masses of information could indirectly erode pluralism and cultural diversity).
4. Preventing the collection and retention of personal data while enhancing AI may justify rethinking the balance between the two.
5. The choice of which and how much data should be curated for AI are of paramount importance.
6. Human uniqueness is being challenged by the autonomy of machines on the one hand and the increasing hybridization of humans with machines on the other hand.<sup>37</sup>

---

35. Krupansky.

36. *U.S. Future of AI Report*, pp. 10-11.

37. *CNIL Report*, pp. 19-21, 24-42



Because of the CNIL Report’s focus on the main uses of AI and the ethical issues raised by these uses of AI, the U.S. Future of AI Report, issued by the Executive Office of the President’s National Science and Technology Council Committee on Technology, can be looked at for a discussion of some applications of AI for public good, the potential of AI and ML to improve people’s lives by helping to solve some of the world’s greatest challenges and inefficiencies, that are not mentioned in the CNIL Report.<sup>38</sup> Major benefits for the public have already begun being reaped in fields as diverse as transportation, the environment, and economic inclusion. In transportation, AI-enabled smarter traffic management applications are reducing wait times, energy use, and emissions; cities are beginning to leverage the type of responsive dispatching and routing used by ride-hailing services and linking it with scheduling and tracking software for public transportation to provide just-in time access to public transportation that can often be faster, cheaper and, in many cases, more accessible to the public. AI image classification is being used to analyze tourist photos from public social media sites to improve animal migration tracking; autonomous sailboats and watercraft are patrolling the oceans carrying sophisticated sensor instruments, collecting data on changes in the Arctic ice and sensitive ocean ecosystems in operations that would be too expensive or dangerous for crewed vessels. Several academic institutions have launched initiatives that use AI to tackle economic and social challenges (e.g. unemployment, school dropouts, homelessness, and poverty).<sup>39</sup>

Other positive impacts of AI and ML can be found in FinTech developments in the Insurance Industry. In general, the expected benefits are: competitiveness (increased revenues/lower costs from cost-effective processes linked to the exploitation of data and from access to a wider/more stable client base), consumer choice (better, more innovative processes, products and services as well as more personalized products and services) and conduct of business/consumer protection (improved detection of fraud and other illegal activities).<sup>40</sup>

## VII. AI and ML as Both Risk and Tool for Mitigating Risk

AI/ML also are both a tool for managing risk and a source of significant new risks that must be managed. Some of the ways AI and ML can be used to mitigate risk are:

---

38. Another application of AI for the public good is image recognition to translate sign language into “readable language,” making it easier for the deaf and hearing impaired to communicate. Sarah Griffiths, “Automatic Sign Language Tool Can Translate Gestures into ‘Readable Language,’” *Daily Mail*, June 23, 2014.

<https://www.dailymail.co.uk/sciencetech/article-2666166/Automatic-sign-language-tool-translate-gestures-readable-language.html>

39. *U.S. Future of AI Report*. pp. 13-14.

40. International Association of Insurance Supervisors, “[FinTech Developments in the Insurance Industry](#),” 21 February 2017, § 5.7, ¶ 125.

<https://www.google.com/search?q=fintech+developments+in+the+insurance+industry&og=fintech+developments+&aqs=chrome.1.69i57j0i5.17236j0j7&sourceid=chrome&ie=UTF-8>

- Credit risk and revenue modeling: ML supports more informed predictions about the likelihood of an individual or an organization defaulting on a loan or a payment. It can also be used to build variable revenue-forecasting models.
- Fraud detection: ML has been successfully applied to the detection of credit-card fraud for many years. Banks use systems that have been trained on historical-payments data to monitor payments for potential fraudulent activity and block suspicious transactions.
- Surveillance of conduct and market abuse in trading: Financial institutions use automated systems to monitor traders by linking trading information with other behavioral information relating to traders.<sup>41</sup>
- Anti-money laundering (AML) compliance: AI-based AML systems detect patterns and trends that have not been seen before and inevitably lead to the discovery of more convoluted money-laundering patterns. Through continuous training, a ML-based system can look at its past analyses and use that information to better prepare itself for future money-laundering threats.<sup>42</sup>

Some of the uses of AI/ML to reduce risk can also create risk (e.g. AI/ML can help analyze credit risks but at the same time lead to unfairness and discrimination in profiling). Some of the main risks associated with advanced data-processing activities, such as AI and ML, include:

- The data subject may be unaware of or surprised by massive and ubiquitous data collection from multiple sources, online and offline tracking, the potential for conversation collection by digital virtual assistants, the analysis by organizations of innocuous data to predict intimate and sensitive data, the use by organizations of data to predict correlations (not causality), and the use by researchers of algorithms to analyze “likes” to infer sensitive personal particulars (including religious beliefs, race and sexual orientation);
- Re-identification or the linkage of data sets destroying anonymity<sup>43</sup>;
- Unfairness and discrimination in profiling due to potential of inherent or latent bias in the underlying data and processes because profiling can be used to infer or predict individuals’ preferences, health, work performance, credit worthiness and propensity to commit crime;
- Limits on ability to explain due to self-evolving logic, not following the logic of the engineers, and minimal human input;
- Lacking transparency because: data-collection purposes may not be able to be specified for big data, “black box” algorithms that are opaque and complicated, automated decision-making that does not provide rationales;

---

41. EY, “When Boards Look to AI, What Should They See?” <https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/ey-when-boards-look-to-ai-what-should-they-see>

42. Breana Patel-Bonova, “AI Implementation in AML at HSBC Sees a Considerable Reduction in Compliance Costs,” Finextra, 16 November, 2017. <https://www.finextra.com/blogposting/14748/ai-implementation-in-aml-at-hsbc-sees-a-considerable-reduction-in-compliance-costs>.

43. The PCPD encourages that whenever an organization carries out advanced data processing that the data is anonymized before the processing occurs and that if the data is to be transferred, that it be specified to whom and that it be anonymized before transfer or by the recipient.



- Filter bubble (state of intellectual isolation as a result of personalized searches when a website algorithm selectively guesses what information a user would like to see based on information about the user, such as location, past click-behavior and search history);<sup>44</sup>
- Uncertainty due to speed and scale of change: given the scale and divergence of the new technologies, any historical trends based on extrapolating previous technological innovations are likely to provide little to no meaningful basis on which to predict future impacts.
- Consumer choice issues when consumers experience a reduced comparability of financial services related to limited/unclear information and comprehension about the extent to which the offer/service is tailored to consumers and/or represents a personal recommendation.<sup>45</sup>

Some of these risks are the byproduct of using AI/ML to mitigate other issues. Therefore, the configuration of AI/ML tools require careful planning/design (e.g. use of a diverse data set to train AI without a built-in bias), effective controls and appropriate governance.

#### VIII. Regulatory Response to Advanced Data Processing Activity, such as AI and ML

Regulatory responses to privacy and data protection risks raised by advanced data-processing activities, such as AI and ML, range from nonexistent to specific.

In the EU, the EU General Data Protection Regulation (GDPR)<sup>46</sup> regulates the processing of personal data<sup>47</sup> and prohibits solely<sup>48</sup> automated decision-making,<sup>49</sup> including profiling,<sup>50</sup> unless

---

44. Stephen Wong, Big Data, *Artificial Intelligence and Privacy*, Office of the Hong Kong Privacy Commissioner for Personal Data, April 26, 2017, 9-22. [https://www.pcpd.org.hk/spec\\_event/files/Big\\_Data\\_AI\\_Privacy.pdf](https://www.pcpd.org.hk/spec_event/files/Big_Data_AI_Privacy.pdf); techopedia, “What Does Filter Bubble Mean?” <https://www.techopedia.com/definition/28556/filter-bubble>.

<sup>45</sup> FinTech Developments at ¶¶ 42, 125.

46. General Data Protection Regulation. 2016/679. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

47. GDPR Article 1.


48. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Article 29 Data Protection Working Party Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, WP251 rev. 01, 8 [hereinafter Article 29 Guidelines].

[http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)

49. Automated individual decision-making has a different scope and may partially overlap with or result from profiling, Article 29 Guidelines p. 8, and means decisions which produce legal effects concerning an individual or similarly significantly affects an individual, GDPR Article 22(1).

50. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Id. Article 4(4). Profiling is composed of three elements: (1) it has to be an automated form of processing; (2) it has to be carried out on personal data; and (3) the objective of the profiling must be to evaluate personal aspects about an individual. Article 29 Guidelines at 6-7.





the decision is necessary for the performance of a contract, is authorized by law, or is based on explicit consent.<sup>51</sup> Also the EU Statement on AI calls for a common, internationally recognized ethical and legal framework and proposes a set of fundamental ethical principles based on the values laid down in the EU treaties and the EU Charter of Fundamental Rights:

- a. Human dignity,
- b. Autonomy,
- c. Responsibility,
- d. Justice, equity, and solidarity,
- e. Democracy,
- f. Rule of law and accountability,
- g. Security, safety, bodily and mental integrity,
- h. Data protection and privacy, and
- i. Sustainability.<sup>52</sup>

In AI in the UK and the CNIL Report, blanket AI-specific regulation is considered inappropriate or unnecessary, partly because the GDPR appears to address many of the concerns regarding the handling of personal data.<sup>53</sup> Instead, AI in the UK, after a review of the benefits and risks of AI, recommends consistent and widely-recognized ethical guidance, in the form of an AI code of conduct,<sup>54</sup> and the CNIL Report, which discussed the use and promise of AI across sectors and identified ethical concerns raised by algorithms and AI, recommends two founding principles for the development of algorithms and AI: fairness and continued attention and vigilance, and six practical policy recommendations:

1. Fostering education of all players involved in the “algorithmic chain” (designers, professionals, citizens) in the subject of ethics;
2. Making algorithmic systems understandable by strengthening existing rights and organizing mediation with users;
3. Improving the design of algorithmic systems in the interests of human freedom;
4. Setting up a national platform for auditing algorithms;
5. Increasing incentives for research on ethical AI and launching a participatory national worthy cause on a general interest research project; and
6. Strengthening ethics within businesses.<sup>55</sup>

In the United States, the U.S. Future of AI Report recommends that the approach to regulation of AI-enabled products should be informed by assessment of the risk that the addition of AI may reduce alongside the assessment of the risk that it may increase. If the risk falls within the bounds of an existing regulatory regime, the policy discussion should start by considering whether the existing regulations already adequately address the risk or whether they need to be adapted to the addition of AI. Also, where regulatory responses to the addition of AI threaten to

---


51. GDPR Article 22(2).

52. EU Statement on AI p. 5.

53. AI in the UK at 116 ¶ 386; CNIL Report at 45.

54. AI in the UK at 125 ¶¶ 419-420.

55. CNIL Report, pp. 48-50, 53-60.



increase the cost of compliance or slow the development or adoption of beneficial innovation, policymakers should consider how those responses could be adjusted to lower costs and barriers to innovation without adversely impacting safety or market fairness.

Because the use of AI to make consequential decisions about people, often replacing decisions made by human-driven bureaucratic processes, leads to concerns about how to ensure justice, fairness and accountability, the U.S. Future of AI Report also recommends ethical training for AI practitioners and students, augmented with technical tools and methods for putting good intentions into practice by doing the technical work needed to prevent unacceptable outcomes.<sup>56</sup>

The privacy and data protection risks raised by advanced data processing activities may not be adequately addressed by existing regulatory regimes.<sup>57</sup> For example, the Hong Kong Personal Data (Privacy) Ordinance (PDPO),<sup>58</sup> which regulates the collection, retention, and use of personal data, provides the legal framework necessary for the development of Internet-based business, in particular ICT applications, creative media and content.<sup>59</sup> However, big data analytics, AI and other digital platforms and tools in the modern ICT age also challenge the existing notification and consent based privacy legal framework.<sup>60</sup> Indeed, history has shown that generally privacy and data protection law has lagged behind technological advances.<sup>61</sup>

There are several historical examples of this lag. Mainframe computers were invented during the 1940s, but it was not until 1976 that the United Nations recognized the basic right to privacy in Article 17 of the International Covenant on Civil and Political Rights (UN International Covenant)<sup>62</sup> which proclaimed that no one should “be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.” Relational databases were invented during the 1970s, but it was not until 1980 that the Organization for Economic Cooperation and Development (OECD) created a set of eight fair-information principles (collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability) and codified them in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines).<sup>63</sup> The first web browser was invented in 1990 and

---

56. *U.S. Future of AI Report*, pp. 1-3.

57. According to the House of Lords Select Committee on Artificial Intelligence, many of the concerns regarding the handling of personal data appear to be addressed by the GDPR. *AI in the UK* at 116 ¶ 386.

58. Cap. 486 of the Laws of Hong Kong, <https://www.elegislation.gov.hk/hk/cap486>.

59. Office of the Hong Kong Chief Information Officer, “ICT Fact Sheet,” July 2018. [https://www.ogcio.gov.hk/en/about\\_us/facts/doc/Fact\\_Sheet-OGCIO-EN.pdf](https://www.ogcio.gov.hk/en/about_us/facts/doc/Fact_Sheet-OGCIO-EN.pdf)

60. Stephen Wong, “Engineering Privacy through Accountability,” *Office of the Hong Kong Privacy Commissioner for Personal Data*, April 11, 2018, p. 3.

[https://www.pcpd.org.hk/english/news\\_events/speech/files/Engineering\\_Privacy\\_Through\\_Accountability.pdf](https://www.pcpd.org.hk/english/news_events/speech/files/Engineering_Privacy_Through_Accountability.pdf).

61. This lag is true in Asia as well as other parts of the world.

62. UN International Covenant, <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

63. OECD Privacy Guidelines.

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>. The Hong Kong Bill of Rights Ordinance, Cap. 383 of the Laws of Hong Kong,

<https://www.elegislation.gov.hk/hk/cap383>, adopted the UN International Covenant into law in 1991, and the PDPO enacted six of the eight OECD fair information principles (data collection, accuracy and retention, data use,



released in 1991, and the use of virtual computers became popular in the 1990s leading to the development of the modern cloud computing infrastructure; however, the EU Data Protection Directive (EU Directive)<sup>64</sup>, the EU's version of the OECD Privacy Guidelines, was not adopted until 1995.<sup>65</sup> Advanced analytics (big data) began in 2006, the first smart phones were released in 2007, when Watson won Jeopardy in 2011, AI broke through, and the Internet of Things started in approximately 2013. The GDPR, which replaces the EU Directive and is the most notable change to data protection legislation in well over two decades, began being drafted in 2012, was not adopted until 2016, and did not go into effect until 2018.<sup>66</sup> Despite its recency and despite its goal of dealing with advanced data-driven technologies, when the GDPR was finalized, AI and ML were not in wide use. As evidenced by the GDPR, changes to privacy and data protection laws require lead time, funding and resources due to the complex nature of the subject and the rapid change of the technology. As this chronology shows, privacy and data protection legislation are ill-equipped to keep up with, let alone anticipate, technological changes such as advanced data processing activities.

Revolutionary and innovative developments in advanced data processing activities, like AI and ML, present challenges to the regulatory strengths and effectiveness of existing personal data and consent-based data protection laws.<sup>67</sup> On or before collection of an individual's personal data, data users must notify the individual of the purpose for which the individual's data is to be collected and used.<sup>68</sup> Express and voluntary consent is required if the personal data will be used or transferred in a manner that is not covered by the original collection purpose (as communicated to the individual at the time of collection) or a directly related purpose, unless an exemption applies.<sup>69</sup> Prior and specific consent is required before personal data can be used or transferred for direct marketing purposes.<sup>70</sup> These laws have remained largely unchanged since

---

data security, openness, and data access and correction) in 1995, well after creation of distributed processing and personal computers during the 1980s.

64. EU Directive 95/46/ec, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> .

65. The APEC Privacy Principles contained in the APEC Privacy Framework, <https://www.google.com/search?q=apec+privacy+principles&oq=apec&aqs=chrome.1.69i57j69i59j0l4.4518j0j7&sourceid=chrome&ie=UTF-8> (preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability), were not adopted until 2005. Consistent with the accountability principle in the APEC Privacy Principles, the Hong Kong Privacy Management Programme guidance was issued in 2014 and reissued in 2018. [https://www.pcpd.org.hk/pmp/files/pmp\\_guide2018.pdf](https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf) , and the Hong Kong Privacy Impact Assessment information leaflet was issued in 2015.

[https://www.pcpd.org.hk/english/resources\\_centre/publications/files/InfoLeaflet\\_PIA\\_ENG\\_web.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf) .

66. According to the House of Lords Select Committee on Artificial Intelligence, the GDPR addresses the privacy and data protection risks by prohibiting solely automated decision-making. AI in the UK at 116 ¶ 386.

67. Stephen Wong, "Protecting Consumers & Competition—International Emerging Technologies," *66th ABA Section of Antitrust Law Spring Meeting*, April 11, 2018, p. 22.

[https://www.pcpd.org.hk/english/news\\_events/media\\_statements/files/PCPDABA2018.pdf](https://www.pcpd.org.hk/english/news_events/media_statements/files/PCPDABA2018.pdf) .

68. PDPO, Data Protection Principle 1.

69. Id. Data Protection Principle 3.

70. Id. Part 6A.



the creation of the OECD Privacy Guidelines in 1980. For AI and ML, the performance of human intelligence processes by machines (especially computer systems), which may include harvesting of data from multiple sources, a consent-based approach to privacy is not fully effective because often there is no human involvement.

As a result, while the consent-based approach is the foundation upon which future governance approaches will be built, given the significant impact nonpersonal data can have on individuals, a broader view of governance is needed. Rather than trying to change the definition of personal data to keep up with the technological developments, for example, it is more workable to develop governance mechanisms that help organizations determine that data is not being used in an inappropriate fashion.

## IX. Enhanced Data Stewardship

Against this backdrop, the question is: how can data intensive activities and technologies that have an impact on individuals be conducted in a fair and ethical manner while achieving the desired benefits? Uses of data that do not easily enable meaningful consent, uses that may not be within the individual's expectation, and uses that cannot be explained effectively through transparency alone, can raise issues about trustworthiness of advanced data processing activities. How can the individual trust the organization is not using the data in a way that adversely impacts his or her rights or interests? Privacy and data-protection laws do not effectively or fully address these issues.<sup>71</sup> Yet, much innovation, much transformation of data into information and information into insight, depend on the organization's use of data that the individual may not anticipate but might benefit from (e.g. collision avoidance systems on cars).<sup>72</sup>

In order to encourage innovation in their regions, digital information strategies are being adopted which recognize that the internet and digital technologies are transforming the world, that the needs of business, government and the general public impact the competitiveness of their country's economy, and that the protection of personal data and fair data processing are needed for the development of Internet-based economies.<sup>73</sup> If individuals do not trust how organizations are using their data and how organizations are transforming data into information and information into knowledge, and the law is not keeping up with the technology, organizations need guidance on how to act ethically and apply equitable principles.<sup>74</sup> This guidance is needed

---

71. To some extent, the legitimate-interest basis for processing under the EU Directive and the GDPR attempts to address this issue but only for personal data.

72. IAF, "Artificial Intelligence, Ethics and Enhanced Data Stewardship," September 20, 2017, pp. 5-7. <http://informationaccountability.org/wp-content/uploads/Artificial-Intelligence-Ethics-and-Enhanced-Data-Stewardship.pdf>.

73. E.g. Hong Kong Government's ICT Strategy & Initiatives, *Hong Kong Digital 21 Strategy*, March 2018. <https://www.gov.hk/en/residents/communication/government/governmentpolicy.htm>, and EU Digital Single Market Strategy, [https://ec.europa.eu/commission/priorities/digital-single-market\\_en](https://ec.europa.eu/commission/priorities/digital-single-market_en).

74. PDPO s 8(1)(c) charges the Privacy Commissioner with promoting awareness and understanding of, and compliance with, the provisions of the PDPO, particularly the Data Protection Principles. The Data Protection Principles can be construed widely to include some principles of equity at law, i.e., an "equitable" right of privacy protection. *W v. Registrar of Marriages* [2010] HKEC 1518 at para128 ("The absence of any relevant definitions in the Ordinance itself or elsewhere would also support the view that the relevant provisions should be construed in

particularly with respect to advanced data-processing activities, such as AI and ML, and to the application of knowledge that enables data-driven innovation to reach its full potential.<sup>75</sup>

Acting ethically means organizations need to understand and evaluate advanced data processing activities and their positive and negative impacts on all parties. This approach means organizations will need to be effective data stewards and not just data custodians. Data stewards consider the interests of all parties and use data in ways that create maximum benefits while minimizing risks to those involved. They ask whether the outcomes of their advanced data-processing activities are legal, fair, and just.<sup>76</sup> Legal, fair, and just is another way to state that organizations will behave ethically with regard for the individual when maximizing the benefits of data insight.<sup>77</sup> In order to determine whether advanced data-processing activities, such as AI and ML, that may impact people significantly, are ethical or fair, organizations should define values that are reduced to core or guiding principles and then are translated into organizational policies and processes. In other words, the stated ethics must be turned into demonstrable action.

This approach is similar to corporate social responsibility that encompasses the economic, legal and ethical expectations that society has of organizations at any given time.<sup>78</sup> Like corporate social responsibility, organizations have a corporate data responsibility that should guide their economic, legal and ethical responsibilities with respect to the data they collect, create, transfer, and disclose. These responsibilities form the basis for data stewardship.

---

the light of moral, ethical and societal values as they are now rather than as they were at the date of first enactment or subsequent amendment and that Parliament intended some judicial licence”) (citing Thorpe LJ in *Bellinger (CA)*, para 148); *LKW v. DD* [2010] 6 HKC 528 at para 56.

<http://www.hklii.hk/eng/hk/cases/hkcfa/2010/70.html> (implicit objective of an exercise under section 7 of Matrimonial Proceedings and Property Ordinance, which requires the court to “have regard to the conduct of the parties and all the circumstances of the case” in ordering financial provision and other ancillary relief, is to arrive at a distribution of assets which is fair as between the parties); Consultation Document at 1.06 (The review of the PDPO was guided by (amongst other guiding principles) the principle that “... the rights of individuals to privacy ... must be balanced against other rights, as well as certain public and social interests and with reference to the particular circumstances in which they arise” and “the need to balance the interests of different sectors/stakeholders. For instance, a suitable balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology.”)

75. PDPO s 8(1)(c). Guidance issued pursuant to PDPO s 8(1)(c) in connection with the Report consists of the Enhanced Elements, Data Stewardship Values, the Model EDIA, and the Process Oversight Model.

76. IAF Paper pp. 6-7.

77. *In re Estate of Chan Lai Fong* [2004] HKEC 654 (common law principles of statutory interpretation entail looking at “the basics of ethics, common sense, fairness and justice.”). <https://www.hongkongcaselaw.com/re-chan-lai-fong/>.

78. Mark S. Schwartz & Archie B. Carroll, “Corporate Social Responsibility: A Three-Domain Approach”, *Business Ethics Quarterly*, 13, Number 4: 2003, 503, 509.

[https://www.researchgate.net/profile/Archie\\_Carroll/publication/261827186\\_Corporate\\_Social\\_Responsibility\\_A\\_Three-Domain\\_Approach/links/54a17ab80cf267bdb902c00f/Corporate-Social-Responsibility-A-Three-Domain-Approach.pdf](https://www.researchgate.net/profile/Archie_Carroll/publication/261827186_Corporate_Social_Responsibility_A_Three-Domain_Approach/links/54a17ab80cf267bdb902c00f/Corporate-Social-Responsibility-A-Three-Domain-Approach.pdf).



Similar to corporate social responsibility, ultimately, data stewardship is predominantly driven by organizational policies, culture and conduct and not technological controls. Thus, the core question is: what does an appropriate trustworthy accountability framework look like for a data steward?

#### X. Enhanced Data Stewardship Accountability Elements

In 2009, the accountability principle in the OECD Privacy Principles formed the basis for the Essential Elements of Accountability (Essential Elements).<sup>79</sup> In 2010, the EU Article 29 Data Protection Working Party issued opinion 3/2010 on the principle of accountability.<sup>80</sup> The Office of the Privacy Commissioner of Canada and provincial commissioners in Alberta and British Columbia adopted accountability guidance in 2012.<sup>81</sup> Hong Kong issued accountability guidance in 2014 and updated it in August 2018,<sup>82</sup> and Colombia issued accountability guidance in 2015.<sup>83</sup> Now, accountability is the foundation of the GDPR.<sup>84</sup> The guidance and the adoption of the GDPR has elevated accountability from check-box compliance to a risk-based approach but has not kept up with the advanced data-processing activities, such as AI and ML, that may impact people in a significant manner. In order to be able to transform data into information, information into knowledge, and insight and knowledge into competitive advantage, and in order for individuals to be able to trust data processing activities, enhanced data stewardship accountability (Enhanced Accountability) is needed.<sup>85</sup>

Working with approximately 20 Hong Kong organizations,<sup>86</sup> the Enhanced Elements<sup>87</sup> were drafted. The Enhanced Elements call for organizations to:

---

79. Essential Elements, <http://www.informationaccountability.org>.

80. Article 29 Data Protection Working Party, Opinion 3/2010 on the Principle of Accountability, WP 173, 13 July 2010.

[https://www.researchgate.net/profile/Archie\\_Carroll/publication/261827186\\_Corporate\\_Social\\_Responsibility\\_A\\_Three-Domain\\_Approach/links/54a17ab80cf267bdb902c00f/Corporate-Social-Responsibility-A-Three-Domain-Approach.pdf](https://www.researchgate.net/profile/Archie_Carroll/publication/261827186_Corporate_Social_Responsibility_A_Three-Domain_Approach/links/54a17ab80cf267bdb902c00f/Corporate-Social-Responsibility-A-Three-Domain-Approach.pdf).

81. The Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, “Getting Accountability Right with a Privacy Management Program,” April 17, 2012. [https://www.priv.gc.ca/media/2102/gl\\_acc\\_201204\\_e.pdf](https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf).

82. Hong Kong Accountability Guidance.

83. Columbia Superintendence of Industry and Commerce, “Guidelines for the Implementation of the Accountability Principle,” May 2015.

[https://iapp.org/media/pdf/resource\\_center/Colombian\\_Accountability\\_Guidelines.pdf](https://iapp.org/media/pdf/resource_center/Colombian_Accountability_Guidelines.pdf).

84. GDPR Article 5(2).

85. Wong Article at 20 (“[A]ccountability represents a perfect balance between seemingly irreconcilable interests of personal data protection and innovative use of data in data-driven economies. It helps data protection regulators realise abstract privacy principles and allows businesses to make innovative uses of data so long as they use data responsibly, minimize risks and prevent harms to data subjects.”)

86. A list of the businesses is attached as Appendix A.

87. The Enhanced Elements are [published separately and accompany the Report](#). The five Enhanced Elements are set forth in the text of this section of the Report, and the subparagraphs of the Enhanced Elements are set forth in notes 88-92 *infra*.



1. Define data-stewardship values that are condensed to guiding principles and then translated into organizational policies and processes for ethical data processing.<sup>88</sup>
2. Use an “ethics by design” process to translate their data-stewardship values into their data analytics and data-use design processes so that society, groups of individuals, or individuals themselves, and not just the organization, gain value from the advanced data processing activities, and require EDIAs when advanced data analytics may impact people in a significant manner or when data-enabled decisions are being made without the intervention of people.<sup>89</sup>
3. Use an internal review process that assesses whether EDIAs have been conducted with integrity and competency, if the issues raised as part of the EDIA have been resolved and if the advanced data processing activities are conducted as planned.<sup>90</sup>
4. Be transparent about processes and where possible enhance societal, groups of individual or individual interests; communicate the data stewardship values that govern the advanced data processing activities, such as AI or ML systems developed, and that underpin decisions widely; address and document all societal and individual concerns as part of the EDIA process and design individual accountability systems that provide appropriate opportunities for feedback, relevant explanations and appeal options for impacted individuals.<sup>91</sup>

---

88. The values and principles should be organizationally derived and should not restate laws or regulations, may go beyond what the law requires, but at a minimum, should be aligned with and not be inconsistent with existing law, regulation, and formal codes of conduct. Organizations should be open about their values and principles. Organizational policies and procedures derived from these values should be anchored to clearly defined accountable individuals within the organization and be overseen by designated senior executives. The guiding principles should be easily understood by all staff, especially technical staff, and should be capable of being programmed into activity objectives. Enhanced Elements 1a-c.

89. Advanced data-processing activities that affect individuals should have beneficial impacts accruing to individuals and communities of individuals, particularly those to whom the underlying data pertains. Where an analytical data driven use has potential impact at the individual level, or at a higher level, such as groups of individuals and society, the risks and benefits should be explicitly defined, and the risks should be proportional to the benefits and should be mitigated to the extent possible. The systems, and the data that feeds those systems, should be assessed for appropriateness based on the decision the data is being used for and should be protected proportional to the risks. Where appropriate, organizations should follow codes of conduct that standardize processes to industry norms. All staff involved in data impacting processing should receive training so that they may competently participate in an “ethics by design” process. Enhanced Elements 2a-d, f.

90. Where data processes begin with analytic insights, those insights should be tested for accuracy, predictability, and consistency with organizational values. Intensive data impacting systems should be reviewed so that outcomes are as intended with the objectives of the activity, risks are mitigated as planned, harms are reduced, and unintended consequences are understood. Where internal reviewers need external expertise, that expertise should be sought. The review of the EDIA process should be separate and independent from the EDIA process itself. Enhanced Elements 3a-d.

91. Organizations should be able to explain how data is used, how the benefits and risks to society, groups of individuals, or individuals themselves are associated with the processing, and how society, groups of individuals, and individuals themselves may participate and object where appropriate. Organizations should be open about how analytical data use and advanced data processing activities, such as AI and ML systems, have been developed. Individual and societal concerns should be part of the data system evaluation lifecycle. Enhanced Elements 4a-c.



- Stand ready to demonstrate the soundness of internal processes to the regulatory agencies that have authority over advanced data processing activities, including AI or ML processes, as well as certifying bodies to which they are subject, when data processing is or may be impactful on people in a significant manner.<sup>92</sup>

The Enhanced Elements are supported by the Data Stewardship Values and a Model EDIA.



This connected framework is also supported by a Process Oversight Model to enhance the EDIA’s trustworthiness and effectiveness.<sup>93</sup> Where the oversight of the assessment and accountability process is done by the organization itself (versus the accountability or regulatory agency), then the oversight should be conducted pursuant to a commonized approach.<sup>94</sup> Until

92. Organizations should be open about core values in regulator-facing disclosures. Organizations should stand ready to demonstrate the soundness of the policies and processes they use and how data and data use systems are consistent with their data stewardship values and guiding principles. Depending on how data is used and what type of data is used, soundness of internal processes may be established by privacy impact assessments (PIAs) or EDIAs. Enhanced Elements 5a-b.

93. The Model EDIA and the Process Oversight Model are published as part of the Enhanced Elements, which accompany the Report.

94. See IAF, Report for Comprehensive Assessment Oversight Dialog: Canadian Ethical Data Review Boards Project, March 31, 2018, [18-24](http://informationaccountability.org/wp-content/uploads/Report-for-the-Comprehensive-Assessment-Oversight-Dialog-Canadian-Ethical-Data-Review-Boards-Project.pdf). [IAF Oversight Report]. <http://informationaccountability.org/wp-content/uploads/Report-for-the-Comprehensive-Assessment-Oversight-Dialog-Canadian-Ethical-Data-Review-Boards-Project.pdf>. A “commonized” approach is one that has been agreed upon after going through a process where the views and interests of a wide variety of stakeholders have been heard and considered before an agreed upon process is





such an approach is established, the Process Oversight Model looks at how an organization has translated organizational ethical values into principles and policies and into an “ethics by design” program. It considers how EDIAs and effective individual accountability systems have been implemented. The oversight process is independent from the assessment process.

The Enhanced Elements and the supporting framework consisting of the Values, the Model EDIA, and the Process Oversight Model are consistent with, and expand upon, the actions other regulators have proposed. The EU Statement on AI proposes a set of fundamental ethical principles based on the values laid down in the EU treaties and the EU Charter of Fundamental Rights; the Values are consistent with the Data Protection Principles.<sup>95</sup> AI in the UK recommends ethical guidance in the form of a code of conduct that could provide the basis for statutory regulation if and when this is determined to be necessary. One of the recommendations of the CNIL Report is to strengthen ethics within businesses by, for example, sector-specific ethical frameworks (such as ethical charters, codes of professional conduct or codes of ethics); the supporting framework leaves codes of conduct to be implemented at the organization—instead of the country—level, but under Section 12(1) of the PDPO, the Privacy Commissioner may publish Codes of Practice including a “standard,” a “specification” or written “practical guidance” in respect of any requirement under the PDPO.<sup>96</sup> The U.S. Future of AI Report recommends ethical training augmented with technical tools; the Values, the Model EDIA and the Process Oversight Model are exactly the kind of technical tools contemplated.

## XI. Data Stewardship Values

Working with the approximately 20 Hong Kong organizations, three Hong Kong Values – Respectful, Beneficial and Fair – were proposed. The Values are recommended for organizations, but organizations may change these values to reflect their culture.

### *Respectful*

The Respectful value has to do with the context in which the data originated, in which the data will be used and in which advanced data-processing activities occur, including in which decisions will be made. The way in which the original “context” or “use” is defined determines how broad a range of other uses can be considered “reasonable”. Advanced data processing activities affect many parties (including individuals to whom the data relates; organizations that

---

memorialized. An example is the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, [http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS\\_2\\_FINAL\\_Web.pdf](http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf).

95. Six Data Protection Principles, [https://www.pcpd.org.hk/english/data\\_privacy\\_law/ordinance\\_at\\_a\\_Glance/ordinance.html#1](https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html#1).

96. The Privacy Commissioner has issued the Code of Practice on the Identity Card and Other Personal Identifiers, [https://www.pcpd.org.hk/sc\\_chi/files/faq/picode\\_e.pdf](https://www.pcpd.org.hk/sc_chi/files/faq/picode_e.pdf), the Code of Practice on Consumer Credit Data, [https://www.pcpd.org.hk/english/data\\_privacy\\_law/code\\_of\\_practices/files/CCDCode\\_2013\\_e.pdf](https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/CCDCode_2013_e.pdf), and the Code of Practice on Human Resource Management, [https://www.pcpd.org.hk/english/data\\_privacy\\_law/code\\_of\\_practices/files/hrdesp\\_e.pdf](https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/hrdesp_e.pdf).



originate the data, collect the data, and use the data to make decisions; those that might regulate the data or data use) in many ways.

The Respectful value, which is consistent with Data Protection Principles 1, 3, 5 and 6 of the PDPO<sup>97</sup>, specifies:

- All parties that have interests in the data should be taken into consideration.<sup>98</sup>
- Organizations are accountable for conducting advanced data processing activities so that the expectations of the individuals to whom the data relate<sup>99</sup> and/or the individuals who are impacted by the data use are considered.<sup>100</sup>
- Decisions made and used about an individual and the decision-making process should be explainable and reasonable.<sup>101</sup>

---

97. “DPP1–Data Collection 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. Data subjects must be notified of the purpose and the classes of person to whom the data may be transferred. Data collected should be necessary but not excessive.

....

DPP3–Data Use Principle

Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject.. ...

DPP5–Openness Principle


A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.”

98. The Courts have often been tasked with the role of reconciling competing interests in this area. Eastweek Publisher v Privacy Commissioner [2000] HKC 692, <https://www.hongkongcaselaw.com/eastweek-publisher-ltd-and-another-v-privacy-commissioner-for-personal-data/> (the court balanced personal data privacy and the freedom of expression in respect of data collection by the media); Chan Yim Wah Wallace v New World First Ferry Services Limited [2015] HKEC 762, <https://www.hongkongcaselaw.com/chan-yim-wah-wallace-v-new-world-first-ferry-services-ltd/>, (the court balanced public interests in preserving confidentiality and interests of open justice in respect of confidential documents); Cinepoly Records Company Limited & Ors v Hong Kong Broadband Network Limited [2006] HKLRD 255, Cinepoly Records Company Limited & Ors v Hong Kong Broadband Network (a similar question arose in a third-party discovery application of personal data).

99. Data Protection Principle 1 requires that the means of collecting data must be lawful and fair, and the data collected must not be excessive regarding the purpose(s) of collection. Data Protection Principle 3 requires obtaining prescribed consent of the data subject before using data for a purpose other than that for which the data was collected or for a directly related purpose. “Prescribed consent” means “express consent of the person given voluntarily.”

100. HKSAR v Chan Kau Tai [2006] 1 HKLRD, <https://www.hongkongcaselaw.com/hksar-v-chan-kau-tai/>; Yiu Wing Ching John v ONC Lawyers [2017] HKEC 1453 (whether an individual has a reasonable expectation of privacy depends on the circumstances; where a reasonable expectation of privacy has arisen, the individual would have a right of privacy and the organization may be accountable for the contravention of that right).

101. Data Protection Principle 5 provides for the individual’s right to ascertain the organization’s personal data policies and practices and be informed of the kind of personal data held by it and the main purposes for which the data is used. The Privacy Commissioner encourages organizations to establish Personal Information Collection Statements and Privacy Policy Statements and has issued a Guidance Note, [https://www.pcpd.org.hk/english/publications/files/GN\\_picspps\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf).

- 
- Individuals should be provided with appropriate and meaningful engagement and control over advanced data processing activities that impact them.<sup>102</sup> Individuals should always have the ability to make inquiries, to obtain relevant explanations and, if necessary, to appeal decisions regarding the advanced data processing activities that impact them.<sup>103</sup>

### ***Beneficial***

The Beneficial value has to do not only with benefits but also with risks. Advanced data-processing activities should provide benefits and values to users of the product or service, whether at the individual level or at a higher level, such as groups of individuals and even society.

The Beneficial value, which is consistent with the reduction of risk concept expressed in Data Protection Principle 4 of the PDPO,<sup>103</sup> specifies:

- Where advanced data-processing activities have a potential impact on individuals, the benefits should be defined, potential risks of the advanced data processing activity should be identified, and their severity should be assessed.
- Where advanced data-processing activities do not impact individuals, risks should be identified, and their materiality should be assessed.
- Once all risks are identified, appropriate ways to mitigate those risks should be implemented.

Any residual risks after mitigation should be identified and balanced against benefits.<sup>104</sup>

---

102. The PDPO provides individuals with specific, albeit limited, rights in respect of their data or control over how their data may be processed. Data Protection Principle 1 requires the data subject be informed before personal data is collected of: whether it is obligatory or voluntary to supply the data and where obligatory the consequences for failing to supply the data; the purposes for which the personal data are to be used and the classes of persons to whom the personal data may be transferred; the right to request access to and correction of the personal data. Data Protection Principle 3 requires that the individuals' prescribed consent be obtained for using their data for a new purpose. Data Protection Principle 5 provides for the individual's right to ascertain the organization's personal data policies and practices. Data Protection Principle 6 provides for the individuals' right to access or request correction of their data. Lastly, PDPO Parts 6 and 6A require specific consent for use or transfer of data in matching procedures or for direct marketing.

103. "DPP4–Data Security Principle

A data user needs to take practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use."

104. Although not required by Data Protection Principle 4, balancing risks and benefits under the Beneficial value is similar to the proportionality test applied to determine whether a legislative provision or conduct amounts to an interference with, or restriction of a constitutional right which is not absolute, that can be justified. *Hysan Development Co. Ltd. v. Town Planning Bd.*, FACV 21, 2015, <https://www.hongkongcaselaw.com/hysan->

## *Fair*

The Fair value has to do with the concept that advanced data-processing activities, including decision-making, are impartial and not solely for self-interested purposes. The Fair value, which is consistent with Data Protection Principles 1(2), 2(1) and 3 of the PDPO<sup>105</sup>, specifies:

- Advanced data-processing activities must avoid actions that seem inappropriate or might be considered offensive or causing distress or humiliation or might be seen as generating unequal treatment or illegal discrimination.<sup>106</sup>
- The accuracy and relevancy of algorithms and models used in decision-making should be regularly reviewed to reduce errors and uncertainty and should be evaluated for inappropriate bias and illegal discrimination.<sup>107</sup>
- Data-intensive activities should be minimized to effectively meet the data processing objectives.
- Advanced data-processing activities should be consistent with the ethical values of the organization.

In order to help implement the Enhanced Elements and the Values, a Model EDIA and a Process Oversight Model have been drafted.<sup>108</sup>

---

[development-co-ltd-and-others-v-town-planning-board-2/](#) . In order to make this determination, a four-step inquiry must be conducted:

1. Does the infringement or restriction pursue a legitimate societal aim?
2. Is the infringement or restriction rationally connected with that legitimate aim?
3. Is the infringement or restriction no more than necessary to accomplish that legitimate aim?
4. Has a reasonable balance been struck between the societal benefits of the encroachment and the inroads made into the constitutionally protected rights of the individual, asking in particular whether pursuit of the societal interest results in an unacceptably harsh burden on the individual?

105. "DPP1—Data Collection 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. Data subjects 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.

"DPP2—Accuracy & Retention Principle

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfill the purpose for which it is used.

"DPP3—Data Use Principle

Personal Data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent with a new purpose is obtained from the data subject."

106. Under Data Protection Principle 1, the personal data must be collected by means which are lawful and fair in the circumstances of the case, and the data collected must not be excessive having regard to the purposes. Under Data Protection Principle 3, prescribed consent must be obtained for new uses.

107. Data Protection Principle 2(1) requires that all practicable steps be taken to ensure that personal data are accurate having regard to the purpose for which the data are being or are to be used.

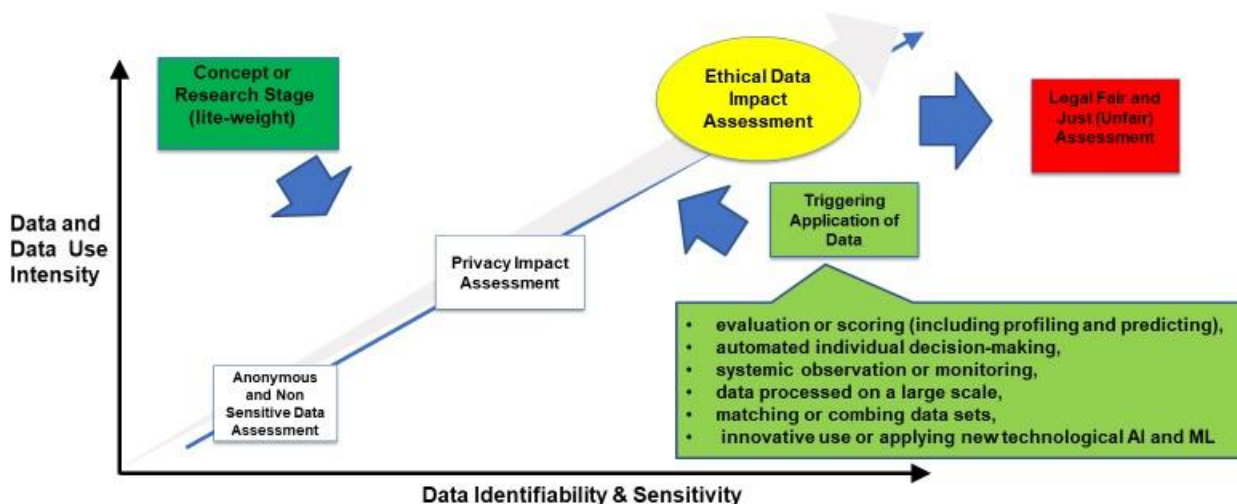
108. The Model EDIA and the Process Oversight Model are being provided under Section 8(1) of the PDPO. See note 74 *supra*.



## XII. [The Model EDIA](#)

A triage process determines the type of assessment necessary for advanced data-processing activities.

### Assessment Choice for Ethical Data Stewardship




6

If data processing is very similar to processing that has been done in the past, no additional assessment may be necessary provided that the appropriate assessment has been conducted already. If the processing is less complex, a more simplified Privacy Impact Assessment (PIA) may be more appropriate. At the concept stage of a data processing activity, a light-weight version of a PIA might be appropriate to identify issues early in the development life-cycle. As data uses get more complex and/or are less obvious to the parties, a more rigorous PIA is likely required. Finally, where the uses are most complex, under either a third party or an in-house solution, an assessment that weighs the risks and benefits may be required. It is in these latter situations that an EDIA may be more appropriate in addition to a PIA (if the EDIA does not include all the elements of a PIA).

An EDIA is a process that looks at the full range of rights and interests of all parties in a data-processing activity to achieve an outcome when advanced data analytics may impact people in a significant manner or when data-enabled decisions are being made without the intervention of people. An EDIA assists an organization in looking at the rights and interests impacted by the data collection, use and disclosure in data-driven activities.

In order to determine whether an EDIA may be necessary, the organization should consider, before the activity begins and when there are any changes which affect the scope of the activity,



whether the data-processing activity involves advanced analytics such as evaluation or scoring (including profiling and predicting), automated individual decision-making, systemic observation or monitoring, data processed on a large scale, matching or combing data sets, innovative use or applying new technological or organizational solutions (such as AI and ML). If the data-processing activity may have an impact on an individual or on a group of individuals that may not be anticipated or easily known, then an organization should consider whether an EDIA should be done either at the concept stage or at the service/product/analytical development stage or at both stages. If the organization determines that an EDIA is not appropriate for the data-processing activity, then only a PIA may need to be completed.<sup>109</sup>

The Model EDIA consists of four sections:

- I. Purpose of the activity,
- II. A full understanding of the data, its use and parties involved,
- III. Impact to parties and in particular individuals, and
- IV. Whether an appropriate balance of benefits and mitigated risks supports the data-processing activity.

The very nature of an ethical and values-based assessment requires a careful consideration of the data activity benefits as well as the risks to individuals and society, considering the interests of all the parties who may be part of the activity. While open, structured questions can help, a way to organize the ultimate decision as to whether to proceed can be evaluated by using a well-established risk modeling process where the outcome of the analysis (significance, likelihood and effectiveness of controls) is depicted in a “net benefit/risk heat map.” The Model EDIA is an example of this approach.

Successful implementation of an EDIA assumes and depends on the full implementation of the Enhanced Elements and, in particular, on highly qualified and competent, accountable roles and responsibilities with appropriate separation of duties. For example, EDIAs could be conducted by the privacy group, engineers in the business, a combination of several parts of the organization. The structure of the overall Model EDIA and the questions in each section are illustrative, and the Model EDIA should be adapted as appropriate for each organization and/or industry. Completion of the EDIA constitutes the evidence that the EDIA was conducted.

The EDIA is broader in scope than the typical PIA. For example, all data are considered in an EDIA and not just personal data. Therefore, all aspects of the EDIA include data in the aggregate, nonidentifiable form that may be outside the scope of the PDPO and many other privacy and data-protection laws. However, to the extent the EDIA can be used to consider and appropriately mitigate the impact of a personal data practice, the EDIA process may supplement (or be woven into) the organization’s PIA process. In this regard, the EDIA process may enhance and augment an organization’s privacy management program and compliance with its legal obligations under the PDPO or similar regulatory frameworks.

---

109. An example of a PIA can be found in the August 2018 edition of the Hong Kong Accountability Guidance pp. 49-53. The Office of the Privacy Commissioner for Personal Data, Hong Kong, conducted a Privacy Compliance Assessment Report on the Smart Identity Card System (SMARTICS). <https://www.immd.gov.hk/pdf/PCARReport.pdf>.



An EDIA does not replace a PIA; it is designed to be used in conjunction with PIAs; it is not a complete PIA. Organizations may incorporate the EDIA in whole or in part into their own unique processes and programs so as to supplement or evolve with their PIA processes. Just as completion of a PIA is not equivalent to compliance with the requirements of the PDPO, neither is completion of an EDIA. However, completion of a PIA and an EDIA is a demonstration of an organization's good faith attempts to comply with the PDPO and other regulatory driven accountability requirements.

As a Model EDIA, other relevant authorities and/or regulatory bodies may provide input into its content and format. The goal of the EDIA is to encourage ICT innovation and competition by demonstrating that an organization has considered the interests of all parties before deciding to pursue an advanced data-processing activity.

### XIII. [The Process Oversight Model](#)

Assessments conducted solely by the parts of an organization implementing intensive data activities may raise issues of trustworthiness. Where the oversight of the assessment and accountability process is done by the organization itself (versus the accountability or regulatory agency), then the oversight should be conducted pursuant to a commonized framework.<sup>110</sup> Until such an approach is established, the Process Oversight Model looks at how an organization has translated organizational ethical values into principles and policies and into an "ethics by design" program. It considers how well-established internal review processes, such as EDIAs and effective individual accountability systems, have been implemented. It presumes the oversight process is independent from the assessment process. For example, it could be a function performed by an internal audit group or an internal control function. It may be likened to an assessment of "controls and controls effectiveness" by the internal audit group.

For example, the internal audit group usually is established by the Audit Committee of the Board of Directors or the highest level of the governing body. The Chief Audit Executive reports functionally to the Board, and the internal audit function is independent and objective. The scope of internal audit's responsibilities encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organization's governance, risk management, and internal controls.<sup>111</sup> The Process Oversight Model can be thought of as analogous to a set of control definitions against which the capability and effectiveness of the organization's assessment process is tested. A set of control parameters across functional assessment domains is established and then, through a set of audits, the effectiveness of the relative controls is tested. While this oversight could be performed by internal audit, it could also be accomplished by way of an assessment or test conducted by an external resource (e.g. a consulting firm). This sort of audit and testing work is similar to work already performed by these external firms in other domain areas.

---

110. See IAF Oversight Report pp. 18-24.

111. The Institute of Internal Auditors, "Model Internal Audit Activity Charter," May, 2013. <https://global.theiia.org/standards-guidance/public%20documents/modelcharter.pdf>.



The Process Oversight Model consists of seven sections:

- I. Accountability for the oversight process,
- II. Translation of organization values into principles and policies,
- III. Translation of organizational values into an “ethics by design” program,
- IV. Use of the EDIA,
- V. Review according to an internal process,
- VI. Accountability to the individual, and
- VII. Transparency of process.

The questions in each section of the Process Oversight Model are illustrative and should be adapted as appropriate for each organization to oversee the trustworthiness of its assessment process.<sup>112</sup> The Process Oversight Model is designed to address the ethics part of data stewardship and assumes other internal oversight processes exist to address core elements of privacy programs.

The oversight process does not have authority over the conduct of individual EDIAs but does have authority over the conduct of the overall EDIA process as well as key elements of Enhanced Accountability. When conducting an EDIA, the participants are expected to evaluate the activity to the best of their ability. When overseeing the EDIA process, the overseers (e.g. the internal audit group) are evaluating the integrity with which EDIAs were conducted. If EDIAs repeatedly (not occasionally) are inaccurate in balancing risks and benefits, then perhaps the process is not operating correctly (not that individual EDIAs were conducted incorrectly).

Evidence of oversight is important. The Process Oversight Model provides rigor to the assessment process and demonstrates that oversight of the EDIA process has occurred. Whether this oversight occurs internally, for example by the internal audit group, or externally, for example by a consulting firm, it is necessary that documentation exists that demonstrates how the oversight was conducted and that, in fact, it was conducted. The completion of the Process Oversight Model provides the evidence that the administration of suitable controls was conducted.

The oversight process should measure whether the EDIA process is being conducted with honesty and whether it recognizes the full range of interests of all parties in order to demonstrate that the interests of the organization were not placed in front of the interests of other parties.<sup>113</sup> The organization should stand ready to demonstrate its assessment governance process and individual assessments to regulators with appropriate authority.<sup>114</sup> The Process Oversight Model provides guidance regarding how such oversight should be conducted and documentation that the oversight actually occurred.

---

112. An assessment of the process is designed to be different than a secondary assessment of a specific data intensive activity.

113. IAF Oversight Report, p.21.

114. Id. pp. 23-24.





As process-oversight models evolve, there may be input and guidance from other relevant authorities and/or regulatory bodies. Such input and guidance will increase the trustworthiness of the EDIA process.

#### XIV. Conclusion

To the extent individuals provide the data that creates the information that creates the insights upon which advanced data processing activities, such as AI and ML, depend, organizations are encouraged to develop an assessment process for ascertaining that advanced processing of data pertaining to people is conducted ethically.<sup>115</sup> Only the organizations themselves know how they are going to process the personal and other data, and after conducting an EDIA, the organizations are able to determine the benefits and risks to individuals' rights and interests as a result of the processing and the appropriate steps to mitigate any risks.<sup>116</sup> Using an oversight process, which is independent from the assessment process itself, is a critical component of Enhanced Accountability and increases the trustworthiness of the EDIA process. Trust in the EDIA process will result in trust in advanced data processing activities and will enable organizations to continue to use data to drive the ICT economy.

---

115. The concept of assessment by an organization is prevalent in the context of employee monitoring. In the PCPD's "The Privacy Guidelines: Monitoring and Personal Data Privacy at Work," December 2004, [https://www.pcpd.org.hk/english/publications/files/monguide\\_e.pdf](https://www.pcpd.org.hk/english/publications/files/monguide_e.pdf), the Privacy Commissioner recommends that prior to the commencement of any employee monitoring, employers should undertake an assessment process referred to as the 3As: Assessment, Alternatives, and Accountability, including an assessment of the risks and benefits of the monitoring. Accountability includes development of an employee monitoring policy and disclosure of that policy to the employees.

116. Wong Article, p.19.

## Appendix A

### *Business Participants – Hong Kong Project*

- Cathay Pacific Airways Limited
- China Taiping Insurance (HK) Company Limited
- Dentons Hong Kong LLP
- The Hong Kong Association of Banks
- Hong Kong Federation of Insurers
  - AIA International Ltd
  - Prudential Hong Kong Limited
- Hong Kong Science & Technology Parks Corporation
- Microsoft
- MRT Corporation Limited
- Naspers Ltd
- Octopus Cards Limited
- PWC Hong Kong
- Transunion
- WTT HK Limited