Data Protection of Biometric Data and Genetic Data

John Paul M. Gaba[★]
Joan Janneth M. Estremadura[★★]

★ '02 LL.B., University of the Philippines College of Law. The Author is a Partner at Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW), specializing in intellectual property, cyberspace, e-commerce law, and data privacy and protection. He is a member of the Corps of Professors of the Philippine Judicial Academy (PHILJA) where he serves as a professor and lecturer on intellectual property, e-commerce and cyberspace law, and data privacy and protection, and sits as a member of PHILJA's Department of Court Technology. Currently, he teaches Intellectual Property Law, E-Commerce/Cyberspace Law, and Data Protection & Privacy at De La Salle University College of Law.

★★ '15 J.D., *with honors*, Ateneo de Manila University School of Law. The Author is an Associate of the Intellectual Property Department at Angara Abello Concepcion Regala & Cruz Law Offices (ACCRALAW). She has written several Opinions in BusinessWorld, one of which is entitled *Robo-rights: Artificial intelligence machines' right to own copyright over works* (Joan Estremadura, *Robo-rights: Artificial intelligence machines' right to own copyright over works*, BUSINESSWORLD, Dec. 3, 2019, *available at* https://www.bworldonline.com/robo-rights-artificial-intelligence-machines-right-to-own-copyright-over-works (last accessed Feb. 29, 2020)). She was also the moderator for *The Future is Mobile Seminar* held at the at De La Salle University College of Law in 2017.

Cite as 64 ATENEO L.J. 949 (2020).

I. OVERVIEW OF DATA PRIVACY AND PROTECTION LAWS

A. General Data Protection Regulation (GDPR) and its Scope

Recent years have seen the emergence of data privacy and protection laws across the globe.[1] This was brought about by the European Union's (E.U.) adoption in April 2016 and full implementation in May 2018 of the General Data Protection Regulation,[2] or more commonly known as the GDPR. The implementation of the GDPR was in recognition of, and in response to, the rapid technological developments and globalization, which have brought new challenges for the protection of an individual's personal data as technology facilitated the ease of collection and sharing of such information between entities which may be located in different jurisdictions.[3] While the E.U. has welcomed such technological advancements, it has also put in place and required "a strong and more coherent data protection framework" that will allow individuals to have ultimate control of their own personal data, without having to unduly restrict the flow of information.[4]

The impact of the implementation of the GDPR was felt worldwide as it applies to all individuals who are citizens of the E.U. regardless of where the processing of information takes place,[5] to any individual or natural person (of any nationality or descent) found within the E.U. regardless of

1. *See* Graham Greenleaf, Global Data Privacy Laws 2019: 132 National Laws & Many Bills, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 (last accessed Feb. 29, 2020).
2. Commission Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].
3. *Id.* whereas cl. 6.
4. *Id.* whereas cl. 7.
5. *Id.* art. 3 (1).

whether the processing takes place within the E.U.,[6] or to an institution or company which is found in the E.U. regardless if it is established outside the union, and even though the processing of information may be outside the territorial jurisdiction of the E.U.[7]

Considering the scope of the GDPR, its application cuts across borders, and, as such, various countries[8] amended their own data privacy laws to comply with the strict requirements of data protection provided thereunder. As will be discussed in this Article, the Philippines enacted in 2012 a comprehensive data privacy law[9] that followed the E.U. approach on data protection closely patterned after the E.U. Data Protection Directive of 1995, the predecessor of the current GDPR.[10]

B. Subject Matter of Protection Under the GDPR

A common misconception is that the GDPR covers and protects all kinds of information. The GDPR only pertains to the processing of personal data relating to individuals or natural persons. It does not relate to the protection

6. *Id.* art. 3 (2).

7. *Id.*

8. As an example, since April 2016, Japan, through the Personal Information Protection Commission, has been in discussion with the European Commission with a view to building the framework for mutual and smooth transfer of personal data between Japan and the European Union (EU). Personal Information Protection Information Commission Japan, The framework was implemented and came into force on 23 January 2019. Final agreement on building the framework for mutual and smooth transfer of personal data between Japan and the European Union, *available at* https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20180717 (last accessed Feb. 29, 2020) & Personal Information Protection Information Commission Japan, The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force, *available at* https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123 (last accessed Feb. 29, 2020).

9. An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

10. Philippine Data Privacy Law is Signed into Law, *available at* https://www.hldataprotection.com/2012/08/articles/international-eu-privacy/philippine-data-privacy-law-is-signed-into-law (last accessed Feb. 29, 2020).

of other information like trade secrets which are subject to a different set of laws and rules; nor does it cover the protection of information of corporations or other juridical entities (except for the personal information of the representatives or officers of such entities, for example).

Personal data is defined under Article 4 (1) of the GDPR as

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural[,] or social identity of that natural person.[11]

It refers to any information, or a set of such information taken together, which may be used to identify a natural person or an individual. The GDPR does not distinguish the form which the data or information takes, as it protects personal data both in written or digital format, so long as the data is part of a filing system or database.[12]

As defined in the GDPR, personal data has two tiers: (1) personal data and (2) a special category of personal data.[13] The special category of data, previously known as sensitive personal information in old privacy laws, relates to a specific nature of information which pertains to the individual's "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, ... genetic data, biometric data ... , data concerning health[,] or data concerning a natural person's sex life or sexual orientation."[14] Under the GDPR, processing of such special category of personal data is prohibited, unless the conditions under Article 9 of the GDPR are met which include, among others, explicit consent of the data subject and the necessity of protecting such information (commonly referred to as "valid legal basis for processing").[15]

The term *processing* of personal data also has a specific definition under the GDPR. It is defined in Article 4 (2) of the GDPR as

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or

11. GDPR, *supra* note 2, art. 4 (1).

12. *Id.* art. 2 (1).

13. *See* GDPR, *supra* note 2, art. 4 (1).

14. GDPR, *supra* note 2, art. 9 (1).

15. *Id.* art. 9 (1) & (2).

> alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure[,] or destruction.[16]

This definition covers a broad spectrum of activities, which technically encompasses any action done or involving personal data.

The broad coverage of the term *processing* has also affected the jurisdictional effect of the GDPR. As mentioned, the scope of the GDPR is already broad (e.g., an institution with presence in the E.U. or an individual found in the E.U., regardless of nationality or residency). Combine such scope with the nature of the activity involved and the scale of affected entities becomes even more extensive.

C. Principles of Data Protection Under the GDPR

The GDPR adheres to the following core principles with regard to processing personal data, namely: (1) lawfulness, fairness, and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability.[17]

The first principle (lawfulness, fairness, and transparency) requires that personal data be processed lawfully and fairly.[18] The GDPR also requires that the personal data is collected for specific and legitimate purposes and not further processed in a manner that is incompatible with such declared purposes (purpose limitation).[19] The processing of the data must also be "adequate, relevant[,] and limited to what is necessary in relation to the purposes for which they are processed (data minimization)."[20]

The personal data to be processed must also be accurate and updated (accuracy).[21] The GDPR requires that every reasonable step is taken to ensure that inaccurate personal data are either erased or rectified without delay.[22] Personal data, however, must be kept for a reasonable length of time, in accordance with the purpose of processing of such data (storage

16. *Id.* art. 4 (2).

17. *Id.* art. 5.

18. *Id.* art. 5 (1) (a).

19. *Id.* art. 5 (1) (b).

20. GDPR, *supra* note 2, art. 5 (1) (c).

21. *Id.* art. 5 (1) (d).

22. *Id.*

limitation).[23] The GDPR, however, provides for certain exceptions with regard to the storage of data and provides that information may be kept "for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes[,] or statistical purposes in accordance with Article 89 (1) [of the GDPR]."[24]

The sixth principle (integrity and confidentiality) mandates implementing or using appropriate technical or organizational measures to ensure that personal data are processed securely, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.[25]

The GDPR adds one more principle which is not present in the past data privacy laws of the E.U., and that is the seventh principle of accountability. It requires that the controller[26] be responsible for, and be able to demonstrate compliance with, all the above-mentioned principles.[27]

D. Data Privacy Law of the Philippines

Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012 (DPA) was signed into law on 15 August 2012 and took effect 15 days thereafter.[28] The Implementing Rules and Regulations of the Data Privacy Act (DPA-IRR) was promulgated four years after, or on 24 August 2016.[29]

The present DPA and DPA-IRR are largely derived from the E.U.'s privacy laws, and, thus, generally reflective of the principles and restrictions found in the GDPR.

---

23. *Id.* art. 5 (1) (e).

24. *Id.*

25. *Id.* art. 5 (1) (f).

26. A "controller" is defined in Article 4 (7) of the GDPR as "the natural or legal person, public authority, agency[,] or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." GDPR, *supra* note 2, art. 4 (7).This is synonymous with the concept of "personal information controller" under the Data Privacy Act of 2012. *See* Data Privacy Act of 2012, § 3 (h).

27. GDPR, *supra* note 2, art. 5 (2).

28. Data Privacy Act of 2012, § 45.

29. Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).

Similar to the GDPR, the DPA is founded on the policy of protecting the fundamental human right to privacy, while, at the same time, ensuring the free flow of information to promote innovation and growth.[30] At this point, it bears stressing that pursuant to the E.U. approach, the Philippines has adopted a privacy law primarily protecting one's individual human right to privacy, which has now gained acceptance and recognition as having application to one's personal information. Hence, the traditional notion that privacy protects persons — and not places — now extends to a person's underlying right to privacy over one's own personal data.

The scope of the coverage of the DPA and the DPA-IRR is also broad as they apply to:

(1) the processing of personal information of a Filipino citizen or a resident of the Philippines regardless of his location;[31]

(2) the processing of personal information done in the Philippines;[32] or

(3) any natural and juridical person involved in personal information processing who, although not found or established in the Philippines, uses equipment that are located in the Philippines, or those who maintain an office, branch, or agency in the Philippines.[33]

The scope of the Philippines' data privacy law is conceptually similar to that of the GDPR as it also has the attribute of extraterritoriality.[34]

---

30. Data Privacy Act of 2012, § 2.

31. Rules and Regulations Implementing the Data Privacy Act of 2012, § 4 (b).

32. *Id*. rule II, § 4 (c).

33. *Id*. rule II, § 4 (d).

34. Section 6 of the Data Privacy Act of 2012 provides —

> SEC. 6. *Extraterritorial Application*. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:
>
> (a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;
>
> (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
>
> (1) A contract is entered in the Philippines;

Expressly, the DPA rests on general principles of privacy which are: transparency, legitimate purpose, and proportionality.[35] The DPA-IRR expounds on these principles. The principle of transparency requires that an individual, called the *data subject*, must be aware of the following:

(1) "the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved[;]"[36]

(2) "the identity of personal information controller[;]"[37] and

(3) "his or her rights as a data subject, and how [such rights] can be exercised."[38]

In addition, "information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language."[39]

With regard to the principle of legitimate purpose, the DPA-IRR provides that "[t]he processing of information [must] be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy."[40] This is also similar to the GDPR's purpose limitation principle.

---

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

Data Privacy Act of 2012, § 6.

35. *Id.* § 11.

36. Rules and Regulations Implementing the Data Privacy Act of 2012, rule IV, § 17 (a).

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.* § 18 (b).

Finally, under the DPA-IRR, the principle of proportionality provides that "[t]he processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose."[41] This ensures that unnecessary collection and storage of personal information may be avoided, considering that the means employed to collect and process these information will be measured and evaluated against the declared purpose.

The DPA also clearly defines two tiers of information, namely, *personal information* and *sensitive personal information*.

Under the DPA, *personal information* is defined as "any information[,] whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[42] The definition in local law is reflective of the definition provided under the GDPR as it pertains to any information which, taken individually or together, will enable the *reasonable* identification of an individual.

The DPA also provides for a special category of data which is classified as *sensitive personal information*. This type of information includes:

(1) "an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;"[43]

(2) "health, education, genetic or sexual life of a person[;]"[44]

(3) "any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;"[45]

(4) any information "[i]ssued by the government peculiar to an individual which includes, but not limited to, social security

41. *Id.* § 18 (c).

42. Data Privacy Act of 2012, § 3 (g) & Rules and Regulations Implementing the Data Privacy Act of 2012, rule I (l).

43. Data Privacy Act of 2012, § 3 (l) (1) & Rules and Regulations Implementing the Data Privacy Act of 2012, rule I, § 3 (t) (1).

44. Data Privacy Act of 2012, § 3 (l) (2) & Rules and Regulations Implementing the Data Privacy Act of 2012, rule I, § 3 (t) (2).

45. *Id.*

numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;"[46] and

(5) those "[s]pecifically stablished by an executive order or an act of Congress to be kept classified."[47]

Notably, while the DPA and the DPA-IRR provide for the protection of information on the health and genetic information of a person, which may, arguably, subsume his or her genetic code, the GDPR provides a separate category and definition for the term *genetic data*[48] as opposed to what it describes as *data concerning health*.[49]

The question now is: will the absence of a specific express definition in Philippine laws and regulations of biometrics and genetic code as a particular category of data have an impact on an individual's right to privacy and, on a larger scale, affect the quality of life of a person?

II. BIOMETRIC DATA AND GENETIC CODE AND PRIVACY LAWS

A. Overview of Biometric Data and Genetic Data

With the variety of data and information available for consumption and the rapid pace data are transferred through various means (primarily through digital and mobile-enabled technology), privacy and data protection laws are constantly evolving and adapting to these innovations.

Under the GDPR, *biometric data* and *genetic data* are among those classified under the *special category of data*,[50] recognizing that, nowadays, these provide new means of identifying an individual. It goes beyond the name, address, birth date, contact number, and what is normally perceived and classified as *personal information*. The GDPR expressly recognizes that an individual's digital data including metadata, IP address (if taken together with some other personal information), location data, e-mail address, and social media identity are personal information.

46. Data Privacy Act of 2012, § 3 (l) (3) & Rules and Regulations Implementing the Data Privacy Act of 2012, rule I, § 3 (t) (3).

47. Data Privacy Act of 2012, § 3 (l) (4) & Rules and Regulations Implementing the Data Privacy Act of 2012, rule I, § 3 (t) (4).

48. GDPR, *supra* note 2, art. 4 (13).

49. *Id.* art. 4 (15).

50. GDPR, *supra* note 2, art. 9 (1).

1. Data Relating to Health and Genetic Data

Unlike Philippine data privacy law and regulations, the GDPR expressly defines what constitutes *data concerning health*. It is defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[51] It is not merely a general reference to health, but specifically mentions both physical and mental health and tangential information relating thereto, such as the person's health care requirements which may reveal his or her health condition.

The DPA, on the other hand, makes a general mention on this type of information as anything *about an individual's health*. The GDPR goes on to separately describe what genetic data is and refers to it as "personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."[52] A similar definition is also found in the GDPR's Recitals, and further expounds by providing examples, namely, "chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained."[53]

Notwithstanding the seeming lack of sophistication in the definition found in the DPA and DPA-IRR, it can be argued that Philippine privacy law and regulations still consider as sensitive personal information all health-related information which include one's genetic data, the genes being the essential building and identification blocks of any life form.[54]

2. Biometric Characteristics and Biometric Data

A person's biometric characteristics are distinctive, measurable characteristics which can be transformed as a template to identify and describe an individual.[55] It combines computer vision with knowledge of human

51. *Id.* art. 4 (15).

52. *Id.* art. 4 (13).

53. *Id.* whereas cl. 34.

54. Data Privacy Act of 2012, § 3 (l) (2).

55. Anil Jain, et al., Biometric Identification, *available at* http://helios.et.put.poznan.pl/~dgajew/download/PUT/SEMESTR_10/IO/FACE_RECOGNITION/BiometricsACM.pdf (last accessed Feb. 29, 2020).

physiology and behavior.[56] Generally, this includes, but is not limited to, a person's fingerprint, palm veins, facial features, or a person's DNA.

The GDPR provides for a separate definition for *biometric data*. It has been defined as "personal data resulting from specific technical processing relating to the physical, physiological[,] or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[57]

The World Intellectual Property Organization (WIPO) also described *biometrics* as information dealing with the recognition of people based on his or her physiological characteristics, such as face, fingerprint, vascular pattern or iris, including a person's behavioral traits, such as gait or speech.[58]

The definition of *biometric data* under the GDPR, however, has grown to include not just the physiological characteristic of a person like his or her fingerprints, facial features including irises or retinas, but now also includes an individual's behavioral traits or characteristics.[59] The inclusion thereof in the definition of what constitutes personal information reshaped the conduct of business of several multi-national companies which are required to comply with the GDPR's requirements. The GDPR aims to regulate the use of these special category of data for commercial purposes, such as targeted advertising and unsolicited contact (i.e., spamming).

B. Current Regime that Governs Protection of Biometric Data and Genetic Code Under the GDPR

Article 6 of the GDPR[60] provides that processing of personal information (i.e., those not considered falling under the *special category of data*) is lawful when any one of the following factors are met:

> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

56. Hsiu-Ren Chien, *Protection of Biometric Data and Genetic Code in Taiwan: Privacy and Patent Rights*, Presentation made during the Asian Patents Attorneys Association 2019 Conference (Nov. 10, 2019).

57. GDPR, *supra* note 2, art. 4 (14).

58. WORLD INTELLECTUAL PROPERTY ORGANIZATION, WIPO TECHNOLOGY TRENDS 2019 ARTIFICIAL INTELLIGENCE 147 (2019).

59. GDPR, *supra* note 2, whereas cl. 71.

60. *Id.* art. 6.

(b) processing is necessary for the performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [or]

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[61]

From the above, it is apparent that, even without the consent of the individual or data subject, personal information (i.e., those not considered falling under the *special category of data*) may be processed if any of the conditions under paragraphs (b) to (f) is present.

The GDPR, however, provides a stricter requirement for processing of information defined as the special category of data under Article 9, which includes genetic and biometric data.[62] It provides a more restrictive language and states that generally, processing of personal information considered as special category of data is prohibited, unless any of the following conditions are met:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

61. *Id.*

62. *Id.* art. 9 (1).

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defen[s]e of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to [a] contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes[,] or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific

> measures to safeguard the fundamental rights and the interests of the data subject.[63]

While Article 9 provides for more exceptions to the lawful processing of these special category of data, the conditions are more stringent and specific such as allowing local legislation to allow data subjects to put an absolute prohibition on processing this special category of data.

In summary, Article 9 of the GDPR provides that before a special category of data may be processed, there must be the existence of either one of the two primary conditions: explicit consent by the data subject or a legitimate interest to process the same.[64]

The *legitimate interests* requirement contemplated by this provision is two-fold. *First*, the data controller needs to process the information for purposes of its legitimate interests or for the interest of a third party to whom information is disclosed. These interests may include the overarching interest of public health and safety. *Second*, once the purpose or interests have been established, these interests must be balanced against the interests of the individual concerned.

The *balancing of interest* is one of the tests to determine the propriety of any government action which tends to affect or limit the exercise of a fundamental human right, which in this case is the right to privacy, and tangentially, the right to health. In this case, the test is also used to determine the propriety of an action or measure a private organization or entity as it relates to processing the special category of data under the GDPR.

Article 30 of the GDPR also provides that a controller[65] and/or processor,[66] where applicable, must maintain records of the processing activity which include the following information: (1) the purpose of processing the information; (2) the description of the categories of data subjects and categories of personal data; (3) the recipients of personal data including if such recipient is in a third country (outside the E.U.) or an international organization; (4) time limits for erasures; and (5) a general description of the technical and organizational security measures of the controller, among others.[67]

---

63. *Id.* art. 9 (2).

64. *Id.*

65. To reiterate, a *controller* is defined in Article 4 (7) of the GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." This is synonymous with the concept of "personal information

The provision on record-keeping generally applies to an enterprise or organization employing less than 250 persons.[68] The GDPR, however, provides for certain conditions when record-keeping is mandatory despite an organization or entity not employing the required 250 threshold. This is when:

(1) the nature of the processing of personal information is likely to cause "risk to the rights and freedom of data subjects[;]"[69]

(2) "the processing is not occasional[;]"[70] or

(3) "the processing includes special categories of data as referred to in Article 9 (1) or personal data relating to criminal convictions and offences referred to in Article 10 [of the GDPR]."[71]

This exception again establishes a different standard for handling and processing for the special category of data (which include biometric and genetic data) compared to processing other personal information.

1. Specific Requirement for the Protection of Clinical Data and Medical Records

At the onset, the GDPR states that personal data must be secured, including the special category of data, and that the controller and the processor shall implement measures to ensure a level of security appropriate to the risk, including, when appropriate, the pseudonymization and encryption thereof.[72]

---

controller" under the DPA. GDPR, *supra* note 2, art. 4 (7) & Data Privacy Act of 2012, § 3 (h).

66. The term *processor* is defined in Article 4 (8) of the GDPR as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." This is synonymous with the concept of "personal information processor" under the DPA. GDPR, *supra* note 2, art. 4 (8) & Data Privacy Act of 2012, § 3 (i).

67. GDPR, *supra* note 2, art. 30 (1).

68. *Id.* art. 30 (5).

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.* art. 32 (1).

Pseudonymization has been defined in the GDPR as the

> processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[73]

Pseudonymization does not take the personal data outside the ambit of personal information, as the same may still be used to identify an individual if taken together with other information which may not be readily available or had been separately secured.[74]

While pseudonymization is not the required technical measure to be implemented for the protection of personal data, the GDPR used such term therein, together with the term *encryption*, to refer to an appropriate form of security measure to reduce risks to the data subjects and to help controllers and processors meet their data protection obligations.[75]

Pseudonymization, however, is not the same as *anonymization*. The Recitals of the GDPR provide that pseudonymization will not apply to data or information which has already been anonymized as personal information which has undergone pseudonymization — which could be attributed to a natural person by the use of additional information — should still be considered as information on an identifiable natural person.[76] Meanwhile, *anonymization* is when the information "does not relate to an identified or identifiable natural person or to personal data and rendered anonymous in such a manner that the data subject is not or no longer identifiable."[77] Thus, personal information which undergo anonymization is no longer considered personal data as identification of the natural person or individual is irreversibly prevented.

The importance of such difference between anonymization and pseudonymization is crucial in handling clinical data as the difference between the two measures is essential in determining whether consent of

73. GDPR, *supra* note 2, art. 4 (5).

74. *See* Jessica Bell, et al., *Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative dataresearch in the UK*, 34 COMPUTER L. AND SECURITY REV. 222, 233 (2018).

75. GDPR, *supra* note 2, whereas cl. 28.

76. *Id.* whereas cl. 26.

77. *Id.*

data subjects is required for Data Sharing Agreements (DSA) between two different entities or organizations involving sharing or transfer of clinical trial data. If what is merely implemented is pseudonymization of the data, then explicit consent of the data subject is necessary before a DSA may be implemented.[78] However, if the clinical trial data has been anonymized, then the data will no longer be considered personal information and, thus, is taken away from the ambit of coverage of the GDPR.[79] Consent of the data subject may no longer be necessary. It must be emphasized, however, and as will be discussed in detail later, complete anonymization of clinical trial data is almost impossible to achieve.[80]

Moreover, as against medical records, the "right to be forgotten" does not readily apply. Generally, a data subject has the right to request the erasure of his or her personal data, which include medical records.[81] The right to be forgotten, however, is not absolute as the GDPR provides that the data subject may not request the erasure of his or her personal data if the processing is necessary "for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9 (2) as well as Article 9 (3)." [82] This right may also not be exercised if the processing of information relates to "archiving purposes in the public interest, scientific or historical research purposes[,] or statistical purposes in accordance with Article 89 (1) insofar as the right to [erasure] is likely to render impossible or seriously impair the achievement of the objectives of [the] processing [of information]."[83]

78. Jan Linquist, Data science under GDPR with pseudonymization in the data pipeline, *available at* https://www.dativa.com/blogs/data-science-gdpr-pseudonymization-data-pipeline (last accessed Feb. 29, 2020).

79. Khaled El Emam & Mike Hintze, Does anonymization or de-identification require consent under the GDPR?, *available at* https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr (last accessed Feb. 29, 2020).

80. *See* Alex Hern, 'Anonymised' data can never be totally anonymous, says study, *available at* https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds (last accessed Feb. 29, 2020).

81. GDPR, *supra* note 2, art. 17 (1).

82. *Id.* art. 17 (3) (c).

83. *Id.* art. 17 (3) (d).

III. IMPACT OF THE CURRENT REGIME TO THE RIGHT TO PRIVACY AND DEVELOPMENT

In the age of rapid technological development, the importance of biometric and genetic data cannot be denied.

Genetic data, while defined as including the physiological or mental health of a person, goes beyond the simple and straightforward health records as it includes a collection of information obtained from a series of tests and analysis of an individual's genetic make-up to reveal various information, including, among others, his or her ancestry and assessment for risks of acquiring genetic diseases.[84] Such has been instrumental in research and finding treatments for rare genetic diseases. This is evidenced by the establishment of various biobanks in different countries such as the United States (U.S.), Canada, United Kingdom, Austria, and Finland, among others.[85]

Biometric data, meanwhile, is often used by companies to deliver fast and efficient services to consumers.[86] As an example, mobile phone companies, such as Samsung Group and Apple Technology Company, use biometric data for a user to easily access his or her mobile devices through fingerprint, iris, or retina scans.[87] More recently, financial institutions such as banks started utilizing the same biometric data to allow users to access their mobile applications to facilitate banking transactions.[88] In December 2018, Taiwan's Taishin Bank's automated teller machines started using facial

84. *See* Julian Segert, Understanding Ownership and Privacy of Genetic Data, *available at* http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data (last accessed Feb. 29, 2020).

85. Heidi Beate Bentzen, et al., *Data in question: A survey of European biobank professionals on ethical, legal and societal challenges of biobank research*, PLOS ONE, Volume No. 19, at 5.

86. *See* Entrepreneur, Are Your Customers Ready for Biometrics?, *available at* https://www.entrepreneur.com/article/57086 (last accessed Feb. 29, 2020).

87. *See* Heather Kelly, *Fingerprints and face scans are the future of smartphones. These holdouts refuse to use them.*, WASH. POST., Nov. 15, 2019, *available at* https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them (last accessed Feb. 29, 2020).

88. *See* Danny Thakkar, Adoption of Biometrics in Banking and Financial Service Industry, *available at* https://www.bayometric.com/biometrics-in-banking-and-finance (last accessed Feb. 29, 2020).

recognition technology to enable its customers to withdraw money.[89] A first-time customer will only need to insert the debit card, do a face registration, and set a password for the registered face.[90] After which, subsequent transactions do not require a debit card but only the customer's face and face password.[91]

These developments are coupled with the rapid increase of patent applications relating to biometrics filed with various intellectual property offices worldwide. Patents relating to computer vision, i.e., image scanning done by artificial intelligence or machines, grew by an average of 23% annually between the years 2011 and 2016.[92] Patents relating to biometrics, subsumed under computer vision, have grown by an average of 30% since 2013, surpassing all other computer vision sub-categories.[93] Samsung Group and Sony Corporation are the top patent filers with regard to biometrics technology.[94]

While technological advancements are undeniably crucial in improving a person's quality of life, especially in the field of health and medicine, these developments happen at a rapid pace that the propriety, and even the morality, of such advancements are put in question.

A. From Internet of Things (IoT) to Internet of Bodies (IoB)

With the technological developments related to and brought about by the Internet of Things (IoT) and Big Data, it is expected that the fourth industrial revolution will occur.

IoT has been defined as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[95] In addition, "[t]hrough the exploitation of

89. Taishin Holdings, Taishin Holdings 2018 Annual Report (A Financial Report Published by Taishin Holdings for 2018) at 80, *available* at https://www.taishinholdings.com.tw/upload/F38060100/fs_20190513154721_file3.pdf (last accessed Feb. 29, 2020).

90. *Id.*

91. *Id.*

92. WORLD INTELLECTUAL PROPERTY ORGANIZATION, *supra* note 58, at 46.

93. *Id.*

94. *See* WORLD INTELLECTUAL PROPERTY ORGANIZATION, *supra* note 58, at 66.

95. International Telecommunication Union, Overview of Internet of Things (A Recommendation Published by the International Telecommunication Union)

identification, data capture, processing[,] and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, [while] ensuring that security and privacy requirements are fulfilled."[96] Simply put, it is an interconnection of all things and the ability to transfer data through a network without requiring human-to-human or human-to-computer interaction. These things are "object[s] of the physical world (physical things) or the information world (virtual world), which are capable of being identified and integrated into communication networks."[97]

As defined, "[p]hysical things exist in the physical world and are capable of being sensed, actuated, and connected. Examples of physical things include the surrounding environment, industrial robots, goods[,] and electrical equipment."[98] Meanwhile, "[v]irtual things exist in the information world and are capable of being stored, processed, and accessed. Examples of virtual things include multimedia content and application software."[99]

IoT enables technology to process information. When considered from the perspective of *data*, the IoT related technologies acquire various data called *Big Data*, manage data collected via networks, analyze and learn Big Data using artificial intelligence or other related technology, and utilize data while finding out new values and services.[100] It may be said that the degree of innovation these technologies may develop is directly proportional to the number and quality of information these technologies process. While these result in improvement of services, they also pose a risk to individuals considering the nature and number of information collected by these *things*, especially those relating to personal information and even information classified as special category of data.

---

at 1, *available at* http://handle.itu.int/11.1002/1000/11559 (last accessed Feb. 29, 2020).

96. *Id.*

97. *Id.*

98. *Id.* at 3.

99. *Id.*

100. Japan Patent Office, Examination Guidelines Pertinent to IoT Related Technologies (Guidelines made by the Examination Standards Office, Administrative Affairs Division, Japan Patent Office) at 15, *available at* https://www.jpo.go.jp/e/news/public/previous/document/181009_ai_shinsa_e/01.pdf (last accessed Feb. 29, 2020).

With the wealth of information now available, the term *Internet of Bodies* (IoB) has evolved. As mentioned, data, whether public or private, is the driving force of development in the concept of IoT. In the process of feeding data to machines or devices, especially in the context of medical breakthroughs, natural persons or individuals unwittingly surrender to networks, giving these networks access to a human's body, including the bodies' genomes and minds.[101] In addition, "[n]etworks of biosensors and algorithms will capture and analyze an ever more refined record of [a human's] biometrics, vital signs, emotions and behaviors"[102] — this set of networks is now called the IoB.[103]

IoB is defined as when human bodies, including information related thereto and their functions, are becoming connected to, and sometimes reliant upon, software, hardware, and the Internet for portions of their *default* functionality.[104] The incorporation of the human body to a network or a technology may be as simple as wearing devices to monitor a person's health, e.g., a Fitbit or a smart watch that has an installed sports or health application,[105] or may be in the form of consuming a *digital pill*, "a medication embedded with a sensor that can tell doctors whether, and when, patients take their medicines."[106] While consent of the patients is still required before such digital pill is consumed, this consent allows the patient's "doctors and up to four other people, including family members, to receive electronic data showing the date and time pills are ingested."[107] A smart phone app will let a patient block recipients anytime he or she changes his or her mind.[108]

---

101. *See* WORLD INTELLECTUAL PROPERTY ORGANIZATION, *supra* note 58, at 132.

102. WORLD INTELLECTUAL PROPERTY ORGANIZATION, *supra* note 58, at 132.

103. *Id.*

104. Andrea M. Matwyshyn, *The Internet of Bodies*, 61 WILLIAM & MARY L. REV. 77, 86 (2019).

105. *See* Why Fitbit, *available at* https://www.fitbit.com/ph/whyfitbit (last accessed Feb. 29, 2020).

106. Pam Belluck, *First Digital Pill Approved to Worries About Biomedical 'Big Brother'*, N.Y. TIMES, Nov. 13, 2017, *available at* https://www.nytimes.com/2017/11/13/health/digital-pill-fda.html (last accessed Feb. 29, 2020).

107. *Id.*

108. *Id.*

Moreover, apart from the monitoring purpose of these devices, it is highly probable that these devices collect data from the human body,[109] which may include biometric and genetic data.

B. Consent Under the GDPR, a Waiver of the Right to Privacy

Under the GDPR, explicit consent acts like a partial waiver of the person's right to privacy. Simply using a device or service or accessing a site or a server, however, does not necessarily mount to explicit consent contemplated by the GDPR.

The GDPR requires that the consent, apart from being voluntarily and freely given,[110] is given through a "a clear affirmative act establishing a freely given, specific, informed[,] and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her."[111] While the GDPR does not require that a consent be in a particular form, the GDPR's Recitals provide that the consent may be given through a written statement, including by electronic means, or an oral statement.[112] Consent may be given through "ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates ... the data subject's acceptance of the proposed processing of his or her personal data."[113] Thus, under the GDPR, silence, pre-ticked boxes, or inactivity do not constitute explicit consent.[114]

In light of this unequivocal manifestation of consent requirement under the GDPR, there has been a shift among companies as to how they operate their respective businesses, whether they be operating online, engaged in the manufacture of devices which access and obtain information from the human bodies, or otherwise. It is now common to have software or applications which notify the users of the Terms & Conditions (T&C), which includes provisions on privacy measures — clearly in compliance with

109. *See* Bernard Marr, What Is The Internet Of Bodies? And How Is It Changing Our World?, *available at* https://www.forbes.com/sites/bernardmarr/2019/12/06/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/#5e3108f668b7 (last accessed Feb. 29, 2020).

110. GDPR, *supra* note 2, whereas cl. 43.

111. *Id.* whereas cl. 32.

112. *Id.*

113. *Id.*

114. *Id.*

the GDPR's principle of transparency and consistent with informing the data subject as to how his or her personal information will be processed.[115]

While the GDPR requires that information on personal data processing be explained in "a concise, transparent, intelligible[,] and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child,"[116] more often than not, the T&C users normally encounter are crafted in lengthy and complicated language, which most (if not all) users find difficult and too tedious and cumbersome to read completely.

The complexity of such T&C notwithstanding, it is arguable that once a person provides his or her consent thereto covering, for example, the use of a device which gives access to information about one's human body, including traits and behaviors, such person has relinquished a part of his or her privacy to the entities which developed the device or contraption, and consequently, to third parties who were granted access to such information under a valid DSA or any other similar valid agreement.

Using the foregoing setup, it appears that a person must be willing to waive or surrender a part of his or her privacy in exchange for an improvement in one aspect of his life — at the very least, enjoy a convenience promised to be offered by a particular product or service. The GDPR emphasizes the value of proportionality of the nature and number of data collected to the stated purpose for the processing of such personal information;[117] however, the measure of such proportionality cannot be readily ascertained, as the same is governed by the *balancing of interest* test between the person's right to privacy and the legitimate interest of the organization or entity. While the GDPR obligates each E.U. Member State to provide for independent public authorities who will monitor compliance with the GDPR,[118] the concept of *proportionality to the legitimate purpose* may still be subject to varied interpretation by an arbiter who will measure whether the conduct or measure of processing information is commensurate to the stated purpose or interests, in a proceeding either in an administrative body in charge of protecting a person's privacy, or ultimately, the courts in a full-blown legal proceeding.

---

115. *Id.* art. 12 (1).

116. GDPR, *supra* note 2, art. 12 (1).

117. *Id.* whereas cl. 49.

118. *Id.* art. 51 (1).

Simply put, when a person does not consent to the processing of his or her personal information, he or she may not be able to fully enjoy the value and full capabilities of such product, device, or even service. Such enterprise or organization may justify the denial of access, under the guise that it needs the data subject's consent to process information for its stated purpose or for a legitimate interest, the propriety of which may or may not be proportional to the stated purpose.

Thus, while the GDPR's main thrust is to have a person possess the ultimate control of his or her personal information, the question is: given the current realities, does an individual really have effective and meaningful control of his or her personal data, including biometric and genetic data?

C. Commercialization of Biometric Data: The Behavior for Sale

With the relinquishment of a part of a person's privacy through explicit consent, the collection of information acquired from various individuals are now considered high-value commodities especially for businesses. Before the implementation of GDPR, companies in the U.S. have collected information and profiled millions of Americans.[119] This knowledge may include a customer's purchasing pattern and tendencies and other behavioral patterns relating to how the individual consumers decide to make his or her purchases. Armed with such knowledge, businesses that know a lot about their customers may improve their efficiencies in marketing, distribution, and product development.[120] This knowledge inarguably leads to the delivery of less expensive and more useful products and services.[121] Again, in this scenario, consumers are largely trading privacy for a more efficient marketplace, and it appears that the benefits of such trade is more appealing than the loss of some personal privacy rights.[122]

As an example, the term *cookies* in web browsing is generally referred to as "small text files that websites place on [a user's] device as [he or she is] browsing."[123] These are processed and stored in the web browser. While initially regarded as harmless, as these are easily deleted, the same are

119. Craig D. Tindall, *Argus Rules: The Commercialization of Personal Information,* 2003 U. ILL. J.L. TECH. & POL'Y 181, 182-83 (2003).

120. *Id.*

121. *Id.*

122. *Id.*

123. Richie Koch, Cookies, the GDPR, and the ePrivacy Directive, *available at* https://gdpr.eu/cookies (last accessed Feb. 29, 2020).

included in the scope of information that GDPR regulates.[124] Cookies can store a wealth of data, enough to potentially identify an individual, and are the primary tools that advertisers use to track a user's online activity so that they can target the user with highly specific ads.[125] Thus, businesses and their technology may now be able to trace human activity, analyze such activity, create a pattern from the human activity, and in turn, create a business opportunity from such pattern.[126]

Thus, establishments with online presence require its online users to consent to its T&C, including its Cookies Policy, to have continuous and unimpeded access to their respective websites as required under the GDPR. The same is true for other platforms which have now become significant in the digital age, such as search engines, e-mail service providers, and online shopping platforms, among others.

The GDPR provides for safeguards from what it considers as *profiling* — a form of "automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to [analyze] or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, [behavior], location[,] or movements."[127] These safeguards against *profiling* include:

(1) a person's right to be informed that he or she is subject of a profiling and the accompanying consequences of the same;[128] and

(2) the right to object to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.[129]

124. *Id.*

125. *Id.*

126. Yusuke Ichikawa, Japan Patent Attorneys Association, *Recent Developments of Protection and Effective Use on Biometric Data in Japans*, Presentation made during the Asian Patents Attorneys Association 2019 Conference (Nov. 10, 2019).

127. GDPR, *supra* note 2, art. 4 (4).

128. *Id.* art. 13 (2) (f).

129. *Id.* art. 22 (1).

It must be noted that the GDPR only provides for the right to be informed of such profiling, [130] and object to the same, on certain instances. [131] There is nothing stopping organizations, for example, a company engaged in the business of collecting information obtained from *cookies* to *transfer* such information to another entity once the data subject consents to the *processing* of such information. This information may include a person's behavioral pattern in relation to his or her consumer practices, which is considered *biometric data* under the GDPR.

While the GDPR requires that the individual or data subject be informed of the purpose of collection and the further processing of information by another party or controller, [132] there is also nothing stopping these businesses from selling such information to other entities who may be in need of the same, under the guise of a valid and legitimate DSA, which is formally compliant with the GDPR, and to which the data subject has also explicitly consented to. [133]

D. Weaponization of Biometric Data: The Big Brother Effect

Apart from being a high-value commodity, biometric data is increasingly gaining an impact in the quality of life of individuals.

More recently, China implemented a policy of *social credit system* akin to a dystopian approach of the existence of a *big brother* which monitors each and every action of an individual. [134] In China's social credit system, a person is monitored and evaluated by Sesame Credit, a company ran by the online shopping platform giant Alibaba. [135] China, whose local legislation does not provide for protection of biometric information, allegedly collects biometric information through various means such as from applications for passports, identification cards, bank accounts, and through internet connections. [136]

130. *Id.* art. 13(2) (f).

131. *Id.* art. 22 (1).

132. *Id.* art. 13.

133. *See* GDPR, *supra* note 2, arts. 28-36.

134. Nicole Kobie, The complicated truth about China's social credit system, *available at* https://www.wired.co.uk/article/china-social-credit-system-explained (last accessed Feb. 29, 2020).

135. Charlie Campbell, How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens, *available at* https://time.com/collection/davos-2019/5502592/china-social-credit-score (last accessed Feb. 29, 2020).

136. Billie Thomson, China ranks top of the world's 'Big Brother' states for its 'extensive' and 'invasive' use of biometric data belonging to citizens and tourists,

There are even reports that some "factories, state-owned enterprises, and the military have started monitoring the brain activities of employees by means using mind-reading hats to spot workplace rage, anxiety[,] or depression."[137] Moreover, mobile phone users are now required to have facial scans to ensure that all mobile devices are directly linked to identified users.[138] This is coupled with the installation of a mass surveillance network, composed of hundreds of millions of street cameras, which is tagged as the "world's most powerful facial-recognition system"[139] and "aims to identify China's 1.4 billion citizens within three seconds."[140]

From the collection of such biometric data, Sesame Credit evaluates an individual through a broad range of behaviors, both financial and social, which are underwritten by an invisible web of Big Data.[141] The point system goes beyond evaluating whether a person timely pays his or her loans, but also takes into consideration whether such person has done a good deed like donating blood or a bad deed which may range from quarreling with a neighbor to speaking ill against the government.[142] The social credit score generated by the system not only determines the mortgage rate of a person, but has gone beyond to evaluate a person's degree of access to basic utilities, like transportation and healthcare services.[143] Even U.S. Vice President Mike Pence described the system as "an Orwellian system premised on controlling virtually every facet of human life."[144]

On a more alarming note, it appears that this dystopian future is not only happening in China, but in other countries as well, such as Germany[145] and Russia,[146] among others. Moreover, the prevalence of Chinese firms involved in the collection and processing of personal information of a vast number of data subjects[147] may also be a source of alarm.

---

available at https://www.dailymail.co.uk/news/article-7760657/China-No-1-Big-Brother-state-invasive-use-biometric-data.html (last accessed Feb. 29, 2020).

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. Campbell, *supra* note 135.

142. *Id.*

143. *Id.*

144. *Id.*

145. Germany has a universal credit rating system known as a Schufa operated by a private company that assesses the creditworthiness of about three-quarters of all

E. Protection of Genetic Data vis-à-vis the Public Health Interest

1. Effect on Biobanks

The Organisation for Economic Co-operation and Development (OECD) defines a *biobank* as "a collection of biological material and the associated data and information stored in an organized system, for a population or a

Germans and over five million companies in the country. A person who intends to rent a house or loan money is required to produce their Schufa rating in Germany. Additionally, factors like "geo-scoring" can also lower a person's grade if he or she happen to live in a low-rent neighborhood, or even if a lot of his or her neighbors have bad credit ratings. Moreover, there are certain insurance companies which lower their premiums if a person consents to sharing his or her FitBit data. Cathrin Schaer, Germany edges toward Chinese-style rating of citizens, *available at* https://www.handelsblatt.com/today/politics/big-data-vs-big-brother-germany-edges-toward-chinese-style-rating-of-citizens/23581140.html?ticket=ST-37744584-92mM7R74uTwSG4zRGJen-ap1 (last accessed Feb. 29, 2020).

146. There is a move by the Russian government to have 80% of its population, or four out of five Russians, get and build a digital profile by 2025. This digital profile will be composed of an individual's personal successes and failures as part of the government's plans to digitize the economy. Similar to China's social credit system, an algorithm will rate the trustworthiness of citizens based on an individual score determined by credit history, personal characteristics, behavior and interpersonal relationships. 80% of Russians Will Have State-Gathered 'Digital Profiles' by 2025, Official Says, *available at* https://www.themoscowtimes.com/2018/09/28/80-percent-russians-will-have-state-gathered-digital-profiles-by-2025-official-says-a63027 (last accessed Feb. 29, 2020).

147. As an example, Venezuela recently implemented its national ID system called the *carnet de la patria*, or *fatherland card*. The ID transmits data about cardholders to computer servers which, according to employees of the card system and screenshots of user data reviewed by Reuters, include birthdays, family information, employment and income, property owned, medical history, state benefits received, presence on social media, membership of a political party, and whether a person voted. This national ID system is being handled by ZTE, a Chinese corporation. Angus Berwick, Venezuela is rolling out a new ID card manufactured in China that can track, reward, and punish citizens, *available at* https://www.businessinsider.com/venezuela-id-card-tracks-citizens-like-china-2018-11 (last accessed Feb. 29, 2020).

large subset of a population."[148] It consists mainly of two different parts: *first*, "the biological material that is collected, processed, and stored for a long time[;]" [149] and *second*, "[t]he database, including information about demographical and clinical data for each sample and also associated with the bank inventory with the following main activities[:] biospecimen collection, processing, storage or inventory, and distribution of biological material."[150]

The increasing importance of *Big Data* in clinical research done by these biobanks cannot be denied, especially in this day and age when there are emerging and mutating rare diseases, and even the re-emergence of those diseases which have been thought to be eradicated. Thus, cross-border data sharing between these biobanks becomes essential in research. Clinical data is often collected in one or more countries and processed in another country before being transmitted and integrated in global clinical trial databases.

Under the GDPR, informed consent by the data subject may address privacy issues in research.[151] Meanwhile, under medical ethical standards, "[i]nformed consent consists of three basic components: adequate information, voluntariness, and competence."[152] Similar to the requirements of the GDPR, "prior to consenting, a participant should be informed of the goal of his participation and research, possible risks and adverse effects, and the possibility to refuse or withdraw from research at any time."[153]

More recently, however, the discussion on informed consent has focused on the problem of whether consent has to be termed as "general or broad." [154] The European Medicines Authority (EMEA) proposed the terminology and nomenclature that was adopted by the International

148. Judita Kinkorová, *Biobanks in the era of personalized medicine: objectives, challenges, and innovation*, EPMA J., Volume No. 7, Issue No. 1, at 2 (2016) (citing Organisation for Economic Co-operation and Development, Glossary of Statistical Terms, *available at* http://stats.oecd.org/glossary/detail.asp?ID=7220 (last accessed Feb. 29, 2020).

149. *Id.* (citing Stefan-Alexandru Artene, et al., *Biobanking in a constantly developing medical world*, SCI. WORLD J. Volume No. 2013, at 1).

150. *Id.*

151. GDPR, *supra* note 2, Article 9 (1).

152. Kinkorová, *supra* note 148, at 9.

153. *Id.*

154. *Id.* (citing Anne Cambon Thomsen, et al., *Trends in ethical and legal frameworks for the use of human biobanks*, 30 EUR. RESPIRATORY J. 373, 373–82 (2007)).

Conference on Harmonization of Technical Requirements,[155] which in basic terms provide as follows —

> [I]dentified data and samples are labeled with personal identifiers such as name or identification numbers; coded data and samples are labeled with at least one specific code and do not carry any personal identifiers; and anonymized data and samples are initially single or double coded, but the link between the subjects' identifiers and the unique code(s) is subsequently deleted. Once the link has been deleted, it is no longer possible to trace the data and samples back to individual subjects through the coding key(s).[156]

Moreover, one of the concerns brought about by the regulators with respect to genetic data is whether there are sufficient and secured platforms which may be used to collect, process, and store clinical data which is compliant with the rigid requirements of the GDPR.[157] As pointed out earlier, genetic data, to be completely taken out of the requirements of the GDPR, as described by the EMEA, must be anonymized and not be merely pseudonymized.[158] Thus, such terms (i.e., anonymization and pseudonymization) should be carefully distinguished and used in clinical trial protocols, as only anonymization of data will ensure that the data is no longer considered personal data.

The challenge now is how to completely anonymize genetic data. For instance,

> [w]hen conducting genomics research, two essential values of science research need to be balanced [—] the need to share data broadly to maximize its utility for ongoing scientific exploration, and the need to protect research participants' privacy. Achieving the right balance is particularly challenging for genomic data since each person's DNA

155. Kinkorová, *supra* note 148, at 9 (citing International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Definitions for Genomic Biomarkers, Pharmacogenomics, Pharmacogenetics, Genomic Data and Sample Coding Categories at ⋆3, *available at* https://pharmexcil.com/uploadfile/ufiles/1152876357_E15_Step4.pdf (last accessed Feb. 29, 2020)).

156. Kinkorová, *supra* note 148, at 9.

157. Pawel Piotrowicz, Venner Shipley, *Privacy and Data Protection in Europe*, Presentation during the Asian Patents Attorney's Association 2019 Conference (Nov. 10, 2019).

158. GDPR, *supra* note 2, whereas cl. 26.

> sequence is very unique (with the exception of identical twins), and[,] therefore, a DNA sample can never be truly technically anonymized.[159]

Thus, in this case, for entities engaged in the sharing of clinical data involving an identifiable person's genetic data, or a pseudonymized clinical data, entities must ensure that any sharing of these type of information must be done through a contract or a valid DSA, with both parties strictly implementing the reasonable and appropriate security measures as contemplated by the relevant agreement and the applicable privacy laws and regulations.[160]

F. Commercialization of Genetic Data: Consumer Genetic Testing

In recent years, society has witnessed software applications or programs take the place of specially trained genetic counselors and perform the tests to determine the existence of genetic disease-related variants.[161] Meanwhile, other websites allow an individual to trace his or her relatives or ancestry.[162]

While these applications or programs may be used voluntarily or with an individual's consent, the amount of information collected by these platforms are immeasurable and highly valuable.[163] As an example, whenever a person makes the choice to publicize his or her own data, he or she inadvertently also publicizes data pertaining to his or her relatives, as related individuals share portions of their genetic code.[164] Such practice implicitly creates a public database containing the genetic data of uninformed data subjects (in the example given, his or her relatives). This poses an issue with regard to how such practice impinges upon a person's right to privacy.

---

159. National Human Genome Research Institute, Privacy in Genomics, *available at* https://www.genome.gov/about-genomics/policy-issues/Privacy (last accessed Feb. 29, 2020).

160. Piotrowicz, *supra* note 157 at 157.

161. Segert, *supra* note 84.

162. *Id.* This refers to the website *GEDmatch*, which helped a law enforcement agency solve the decades-old Golden State Killer cold case. "Since that case was solved in April, a total of 25 cases have been solved using public genealogy databases that can be queried without a warrant [—] a practice that is actively encouraged by GEDmatch." *Id.*

163. *Id.*

164. *Id.*

IV. THE PHILIPPINE CONTEXT

The DPA and the DPA-IRR boast of a complete strictest of stringent requirements for the protection of personal data as the same are patterned after the E.U. model on personal data privacy protection, and, thus, are reflective of the GDPR. However, as already pointed out, although not containing any express reference to *biometric data* and *genetic data*, Philippine privacy law and regulations can be considered adequate to cover these types of data, as they clearly define *sensitive personal information* to include any information "about one's health, ... genetic, or sexual life of a person."[165]

With respect to a person's behavior as constituting biometric data under the GDPR, it is notable that the DPA-IRR expressly defines the concept of *profiling*. It is defined therein as

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location[,] or movements.[166]

The definition provided in the DPA-IRR (though not found in the DPA) is reflective of the definition provided in Article 4 (4) of the GDPR.[167]

Similar to the GDPR, the DPA-IRR require that a data subject be informed of the fact that he is being profiled and the purpose for such profiling.[168] A data subject may also object to such profiling.[169]

Based on above-referenced provisions related to *profiling* found in the DPA-IRR and how the DPA defines *personal information*, it can be argued that our local privacy law and regulations also extend to and cover biometric data.

Moreover, with respect to genetic data, local or indigenous applications have been developed, such as AIDE, which provide DNA testing and will be able to generate reports about the a user's genetic risks for diseases such as cancer, his or her personality, gender and behavioral traits, and even his or

165. Data Privacy Act of 2012, § 3 (l) (2).

166. Rules and Regulations Implementing the Data Privacy Act of 2012, § 3 (p).

167. GDPR, *supra* note 2, art. 4 (4).

168. Rules and Regulations Implementing the Data Privacy Act of 2012, § (19) (2) & § 34 (a) (1).

169. *Id.* § 34 (b).

her ancestry.[170] Thus, while the present DPA already prescribes the safeguards for the protection of one's personal information pertaining to his or her health, similar to the challenges faced in other jurisdictions, the question is whether there are also safeguards to protect the privacy of individuals whose personal data (primarily health information) have been implicitly divulged by another person (in this example, by the relative).

While many individuals continue to grapple with understanding their rights as data subjects under the current privacy law and regulations, along with companies exerting efforts to align their operations with the legal requirements, challenges continue to come in as rapid advances in digital and information technology constantly reshape and redefine current conceptions and practices no one has imagined a few years ago. Who would have thought that one's retina, voice, or facial features can replace the traditional ID card with name and photo as a usual way of identification (and even as a code to gaining access to one's digital gadget or mobile phone)? With persons gaining the convenience provided by these revolutionary ideas and technology, it unfortunately came at the expense of people giving up certain human rights and liberties — their family's privacy included.

170. *See* Aide, DNA Analysis, *available at* https://www.aide-app.com/dna (last accessed Feb. 29, 2020).